

# **A Self-Sovereign Identity for financially inclusive Cash-based Assistance**

The potential satisfaction of Customer Due Diligence in Malawi and Kenya

Jan Meyling (*i6170487*)

Supervisor: Dr. Zina Nimeh

M.Sc. Public Policy and Human Development

*September 2017 Cohort*

United Nations University – MERIT &

Maastricht Graduate School of Governance

Date submitted: 10.04.2019

Word Count (main text): 21,698

**Maastricht Graduate School of Governance (MGSoG)**



i. Declaration of Academic Integrity

I, Jan Michael Lukas Meyling, hereby declare with relation to my master's thesis:

***A Self-Sovereign Identity for financially inclusive Cash-based Assistance***

that:

- I am aware of and have understood the rules and regulations stipulated in the Education and Examination Regulations (EER) regarding fraud and plagiarism;
- I am aware of the possible consequences and disciplinary measures in the case of fraud and plagiarism in my master's thesis;
- I have conducted myself in accordance with the Thesis Guidelines, Education and Examination Regulations and generally established standards of academic integrity in writing my master's thesis
- I have carefully marked and referenced all direct quotes and references all indirect quotes included in my master's thesis;
- My master's thesis is an original result of my own work and does not include the work of others except in the case of direct and indirect quotes that are recognizable as such



10.04.2019, The Hague

## ii. Expression of Gratitude

I am extraordinarily thankful to so many amazing, brilliant and admirable individuals, that I must take care not to write a whole thesis just about them. Without you, none of this would have been possible.

From United Nations University, I would first and foremost like to thank my supervisor Dr. Zina Nimeh. As coordinator of the Social Protection Masters Specialization, she and her team of lecturers handed me important tools for pursuing my ideals of a more social and just global society. Not only being an expert in social protection, but equipped with viewpoints on social exclusion, poverty and inequality I highly admire, she could not only enrich this thesis from a certain angle, but also willingly went the extra mile to supervise me on a topic not necessarily geared towards her professional background.

From the Netherlands Red Cross Society/510, I want to thank my “unofficial” supervisor Maarten van der Veen in particular. I am more than grateful for you letting me be a part of this project, supporting me with your time and knowledge was vital to the process. I highly admire your horizontal leadership, your ability of conveying even the most abstract concepts in a few concise words, and how you serve as a role-model to the rest of the team. Your vision and brilliance will surely make 510 a well-known institute.

Moreover, I want to specifically thank Lars Stevens, Jonath Lijftgot, Orla Canavan and Marijke Panis for always having an open ear to my various questions and comments (or going bouldering with me).

Furthermore, from 510, I want to thank my good friend Bassel AlKhatib, I loved all our professional and somewhat lesser professional discussions, and I look forward to continuing so in the future!

Finally, I would like to thank the entire team, being part of it for several months was more than enriching. Working with so many idealistic volunteers, graduate students and staff that are trying to cautiously innovate the humanitarian sector while maintaining a strong focus on people in need, was a very refreshing experience.

From Kenya Red Cross Society, I would especially like to thank Ted Bolton, who continuously accompanied me along the research and spent a lot of time and effort to

link me to relevant stakeholders. The same applies to Gumbi Gumbi from the Malawi Red Cross Society.

Furthermore, I want to express my eternal gratitude to the respondents willing to take part in this research. Everyone of them is equipped with an unbelievable amount of intelligence and expertise. Even more importantly, with a highly admirable normative compass. This led to every single interview not only being very enriching from an academic point of view, but also highly re-assuring from an ethical perspective. Everybody was moreover so super nice and friendly during the interviews, that I felt highly comfortable the whole time.

Specifically, I want to thank Prof. Avner Levin from Ryerson University's Faculty of Law for explaining regulatory concepts to an un-trained person like me in the friendliest way imaginable, Wonderful Kunje from the Malawi Red Cross Society for all his contextual input while exactly being as he is named, Vincent Graf from the International Committee of the Red Cross for his dedication to support me, Kokoévi Sossouvi as independent consultant for being so amazingly considerate and supportive, Raul Zambrano, whose pioneer work "Unpacking the disruptive potential of blockchain technology for human development" for IDRC in 2017 is the reason, why I picked-up this research in the first place, Anna Kondakhchyan from (back then) Oxfam International for her unbelievably enriching input and Rajesh Bansal from the Bankable Frontiers Association, for giving a thesis-student some of his very scare time. Finally, I want to thank the other potential respondents indicating an interest to be interviewed but were not eventually, due to my time and scope constraints.

Constantly being surrounded and engaging with people so much more knowledgeable and experienced than me, makes me hope below thesis does not insult your intellect too much.

Lastly, but most importantly, I want to thank the persons who are the most valuable thing I have in my life: my family. Here, I want to firstly thank my "brother-from-another-mother" Andrew Simkus for proof-reading.

All my love and gratitude finally go to my brothers by blood Michael and Mathis, my lovely grandparents, uncles and aunts, my father Peter and my mother Berit. Without your constant and unconditional love and support, especially during the crazy times, I would never be where I am right now.

### iii. Technical Abstract

#### Starting Point

Cash is set to become the default mechanism of humanitarian assistance - when adequate. Technology is increasingly utilized to conduct payments and support the identification of recipients digitally.

#### Complication

Digital Financial Services (DFS), such as mobile money, risk excluding those lacking required access-factors and capabilities. This is especially the case for open mechanisms, which would allow for long-term impacts beyond humanitarian interventions via financial inclusion. Here, a key obstacle is the global ID challenge - individuals without officially recognized identity documents, yielding service providers' potential failure to comply with Know-Your-Customer (KYC-) regulations.

#### The Solution?

Not only governmental institutions, but also humanitarian agencies create identity systems. While most current humanitarian ID systems are proprietary and serve a sole functional purpose, this could change in the nearby future due to recent technological developments. A potential ID solution, able to grow into an efficient, trusted, interoperable system among various humanitarian actors, is seen in reach. If such an ID system would further be accepted by regulating bodies to access wider public and private services, a foundational solution to the global ID challenge could be found. This could, amongst others, alleviate one of the core obstacles to financial inclusion impacts of humanitarian interventions, an explicit goal within the humanitarian-development nexus.

#### Approach

The key question arising is, whether and how regulating bodies would accept a functional humanitarian ID serving a more foundational character. Context matters - this question is thus analysed through the lens of a humanitarian ID satisfying KYC-requirements for open-loop mobile-based payment systems in Kenya and Malawi. These two countries were selected by the Netherlands Red Cross Society (NLRC) and its "510" initiative, the provider of this research. The initiative is developing an open-source, end-to-end digital (Self-Sovereign) Identity (SSI) and cash system - and has

a vested interest in a more foundational character and broad adoption. To examine how and if a deployment could be accompanied by enhanced financial inclusion humanitarian, development, regulatory and DFS-experts with working knowledge of and in the contexts are interviewed.

### Results

In Kenya, current inclusion of un(der)-documented into the incumbent mobile money system seems to be possible based on a humanitarian agency absorbing recipient's individual Money Laundering/Financing Terrorism risks. An according agreement with the service provider could already yield a functional SSI serving some open-loop functionalities.

As this risk-based approach would still be occurring on humanitarian grounds, a long-term sustainable legal status will most likely only be based on formal governmental adoption, or at least, approval. This underscores the importance of successfully implementing a pilot showcasing the alleged advantages of an SSI.

A functional ID system, based on, inter alia, the merits of increased interoperability and efficiency, initially and incrementally adopted among various humanitarian actors, could then be formally adopted by the government or consensually coexist, serving as vehicle for foundational purposes.

In Malawi, regulators could be currently more flexible in accepting a more foundational purpose of a digital ID system early on. However, basic access factors, such as network connectivity or electricity, might undermine that potential in the medium-term. Furthermore, most of the country's residents already hold a legal ID enabling e-KYC compliance.

While recipients' Personal Identifiable Information (PII) held by service providers could potentially be significantly lowered, providing a legal SSI hence does not necessarily respond to the most urgent needs of people affected.

Finally, a humanitarian agency must carefully balance between the aim to support post-recovery periods and replacing public tasks, such as providing foundational ID infrastructures. It furthermore seems highly unlikely, that a sovereign state will give away political power in determining who can possess a legal ID.

A sustainable Self-Sovereign Identity (SSI) should thus, politically and ethically, involve the public sector as soon as possible – hence most likely not circumventing the need of including PII into currently centralizing governmental databases.

Supporting national identification efforts and lobbying for the inclusion into national ID structures vis-à-vis the yet excluded, while primarily focussing on the prospects a functional SSI potentially offers to humanitarian assistance itself should therefore be the current focus.

A too rigid focus on linking humanitarian assistance to long-term development otherwise risks parallel, undermining public ID structures and a deterrence from a humanitarian's core mandate – providing immediate disaster relief.

## Table of Contents

i.	Declaration of Academic Integrity .....	i
ii.	Expression of Gratitude .....	ii
iii.	Technical Abstract .....	iv
<b>1.</b>	<b>Starting Point</b> .....	<b>1</b>
1.1.	Chapter overview.....	1
1.2.	Humanitarian Assistance: from in-kind to cash.....	1
1.3.	The digitalization of cash-based assistance .....	2
1.4.	Digital cash-based assistance and financial inclusion .....	4
<b>2.</b>	<b>So, all good?</b> .....	<b>5</b>
2.1.	Chapter Overview.....	5
2.2.	Exclusion from financially inclusive e-transfer mechanisms.....	5
2.3.	Higher barriers to financially inclusive ( <i>open-loop</i> ) mechanisms .....	7
2.4.	The global ID challenge - a major financial inclusion barrier .....	8
<b>3.</b>	<b>The Solution?</b> .....	<b>10</b>
3.1.	Chapter Overview.....	10
3.2.	Supporting un-documented with (digital) humanitarian IDs .....	10
3.3.	The Silver Bullet? .....	12
3.4.	Reality Check: Fragmented functional systems, instrumental designs .....	13
3.5.	Foundational systems, infrastructural designs – A pathway to financial inclusion and beyond? .....	14
3.6.	Context matters .....	16
<b>4.</b>	<b>Use Case</b> .....	<b>17</b>
4.1.	Chapter overview.....	17
4.2.	Context of Malawi and Kenya.....	17
4.3.	KYC-satisfaction for DFS as analytical lens.....	17
4.4.	Focus on national, open-loop enabled DFS-systems .....	18
4.5.	Focus on open-loop mobile DFS-systems (if possible).....	18
4.6.	Focus on Self-Sovereign Identity as digital ID system .....	19
4.6.1.	Beyond traditional digital ID ecosystems .....	19
4.6.2.	Minimization and Pseudonymization.....	20
4.6.3.	Assertion and Trust.....	21
<b>5.</b>	<b>Research Question</b> .....	<b>22</b>
5.1.	Chapter Overview.....	22
5.2.	Synthesis to Research Question.....	22
5.3.	Operational Sub-Questions .....	23

<b>6. Methodology</b> .....	23
6.1. Chapter Overview.....	23
6.2. SQ i) – iv: Desk Study.....	23
6.2.1. General.....	23
6.2.2. SQ-specific Motivation and Approaches .....	24
6.2.3. Summary Desk Study Approach .....	26
6.3. SQ v – vii: Semi-structured Interviews.....	26
6.3.1. General.....	26
6.3.2. SQ-specific Motivation .....	27
<b>7. Desk Studies</b> .....	30
7.1. Chapter Overview.....	30
7.2. Desk Study Malawi - Summary .....	30
7.2.1. Political, Economic, Social, Technological Environment.....	30
7.2.2. Law/Regulation .....	31
7.2.3. International Humanitarian Organisations .....	31
7.3. Desk Study Kenya - Summary .....	32
7.3.1. Political, Economic, Social, Technological Environment.....	32
7.3.2. Law/Regulation .....	33
7.3.3. International Humanitarian Organisations .....	33
<b>8. Semi-Structured Interviews</b> .....	34
8.1. Chapter Overview.....	34
8.2. Initial Contact - Reaching out to potential respondents .....	34
8.2.1. Institutional stakeholders in Malawi and Kenya .....	34
8.2.2. Independent Experts .....	35
8.3. Developing the Interview Guidelines .....	36
8.4. After the Initial Contact.....	40
8.4.1. General.....	40
8.4.2. Reactions of potential Respondents .....	40
8.4.3. List of Respondents.....	40
8.5. Conducting the Interviews .....	41
8.6. Pre-liminary Analysis.....	42
<b>9. Analysis</b> .....	43
9.1. Chapter Overview.....	43
9.2. Could a humanitarian-backed ID satisfy KYC-requirements to yield inclusion into open-loop mobile DFS?.....	43
9.2.1. Verification of asserted Identity Claims.....	43

9.2.2.	Producing KYC-compliant ID credentials .....	44
9.3.	Can a Self-Sovereign Identity yield open-loop inclusion?.....	48
9.3.1.	Governmental Approval.....	48
9.3.2.	Convincing decision makers .....	48
9.3.3.	Creating a use-case .....	49
9.3.4.	Functional deployment as initial step .....	50
9.3.5.	Scaling up.....	51
9.3.6.	Interoperability with public systems.....	51
9.3.7.	Technical teething problems.....	52
9.4.	Is providing a humanitarian, foundational ID desirable in these contexts? .....	53
9.4.1.	Filling the gap.....	53
9.4.2.	Humanitarian Development Nexus .....	54
9.4.3.	Functional vs. foundational SSI.....	61
<b>10.</b>	<b>Conclusion</b> .....	<b>62</b>
10.1.	Chapter Overview.....	62
10.2.	Conclusion.....	62
10.3.	Recommendations for further research .....	64
10.4.	Limitations .....	66
10.4.1.	Introduction.....	66
10.4.2.	Methodology and Research Process .....	66
10.4.3.	Ethical Considerations.....	68
<b>Appendix</b>	.....	<b>I</b>
Appendix 1: Glossary .....	.....	<b>I</b>
Appendix 2: E-transfer Mechanisms .....	.....	<b>XLIII</b>
Appendix 3: Elaboration Figure 1 .....	.....	<b>XLIV</b>
Appendix 4: Benefits and drawbacks of e-transfer mechanisms.....	.....	<b>XLVII</b>
Appendix 5: Complete Desk Study Malawi.....	.....	<b>XLIX</b>
Political Environment .....	.....	<b>XLIX</b>
Economic Environment.....	.....	<b>LI</b>
Social Environment.....	.....	<b>LIV</b>
Technological Environment.....	.....	<b>LVI</b>
Regulatory Environment.....	.....	<b>LVII</b>
International Humanitarian Organisations .....	.....	<b>LXI</b>
Appendix 6: Complete Desk Study Kenya.....	.....	<b>LXIII</b>
Political Environment .....	.....	<b>LXIII</b>
Economic Environment.....	.....	<b>LXVIII</b>

Social Environment.....	LXX
Technological Environment.....	LXXIII
Regulatory Environment.....	LXXIV
International Humanitarian Organisations .....	LXXIX
Appendix 7: All Interview Questionnaires – Malawian Institutions .....	LXXXII
Appendix 8: All Interview Questionnaires – Kenyan Institutions.....	LXXXVIII
Appendix 9: Example of Cover Letter to Institutions in the Contexts .....	XCVI
Appendix 10: Example of Mail to Independent.....	XCVIII
Appendix 11: Summary Interviews.....	XCIX
Appendix 12: Full Interviews.....	CXXIV
Appendix 13: Anonymized Cover Letter & Informed Consent .....	CCXIX
<b>References</b> .....	CCXXIII

## 1. Starting Point

### 1.1. Chapter overview

The first chapter briefly outlines current trends in [humanitarian assistance](#)<sup>1</sup> and how these trends could be leveraged to increase linkages between humanitarian interventions - as immediate response to a [disaster](#) - and longer-term development impacts.

### 1.2. Humanitarian Assistance: from in-kind to cash

Transfer [modalities](#) of [humanitarian assistance](#) are changing.

Shifting paradigms in [protracted crises](#) response and the necessity to manage restricted resources in an effective and efficient manner, has increasingly made cash-based assistance ([CBA](#)) a part of the humanitarian tool-kit (Smith et. al, 2018; Global System for Mobile Communications Association [GSMA], 2017b; World Bank, 2016).

Increasingly gaining significance as a [disaster](#) response after the 2004 Tsunami in India<sup>2</sup>, the share of [CBA](#)-interventions to total [humanitarian assistance](#) boosted from 1% in 2004 to 10% in 2016, then totalling an estimated 2.6\$ (Smith et. al, 2018).<sup>3</sup>

Underlying reasons for the gradual shift to cash are improved accountability and transparency, reduced leakage and complexity, as well as increased speed and flexibility of [disaster](#) responses to the supply side (World Bank, 2016; Oxfam, 2016; ODI, 2015). A substantive amount of studies further underscores an on average higher

---

<sup>1</sup> Given the vast use of terms and concepts potentially demanding a definition for a reader not working in the sphere, and to not interrupt the reading-flow, relevant terms and concepts will be explained in the glossary (Appendix 1). According terms and concepts defined or explained in the glossary are cross-referenced to respective entry. A reader with software enabling cross-references/hyperlinks can simply “click” on the marked terms to be forwarded.

<sup>2</sup> Although often regarded as “innovation”, cash in form of assistance already dates to the 19<sup>th</sup> century, for example when the Red Cross (RC) responded to the Franco-Prussian war in 1870-1871, or as response to a famine in India (Bailey and Harvey, 2015). The first review of humanitarian [cash transfer programming](#) by international humanitarian agencies was published in 2001 (Bailey and Harvey, 2015a).

<sup>3</sup> Previously, there used to basically be a sole focus on [in-kind assistance](#) in humanitarian interventions.

cost-[efficiency](#)<sup>4</sup> when compared to [in-kind](#) alternatives (World Bank, 2016). On the demand side, evidence suggests a tendency of recipients preferring [CBA](#) to [in-kind](#) assistance.<sup>5</sup> It is believed to increase choice and control of spending for the people affected (PA)<sup>6</sup>, local markets and systems are supported, long-term recovery is enhanced (World Bank, 2016; Overseas Development Institute [ODI], 2015). Implicitly, supply sides' [efficiency](#) gains can furthermore yield improved benefit coverage (Metcalf-Hough et. al, 2018).

Accordingly, while the overall share of [CBA](#) is still low, a report to the United Nation's (2016; p. 31) former Secretary-General suggests that [CBA](#) "should be the preferred and default method of support", and the biggest donors and humanitarian agencies agreed on a rapid scale-up of cash-based interventions (Metcalf-Hough et. al, 2018).

Nonetheless, delivering [CBA](#) analogously is still seen as far away from being an optimal solution by some. Considering the need for rapidity in [disaster](#) response, depending on the context, delivering physical cash to the vulnerable groups can be a slow and lesser scalable process, costly due to international transfers, and comes along with security issues for humanitarian staff and PA (510, 2018).

### 1.3. The digitalization of cash-based assistance

Major trends in politics,<sup>7</sup> the concentration of people in urban settings, and increased market integration have created a more conducive environment for cash (World Bank, 2016), but also technological advancement (Cohen and Salaun, 2017). An often-cited

---

<sup>4</sup> While it is disputed, whether the [effectiveness](#) of cash is higher than [in-kind](#) assistance, the [efficiency](#) is generally in favour of cash. [Cash transfers](#) seem more [efficient](#) to deliver than [in-kind modalities](#), suggesting it might be more [cost-effective](#) on average. However, results should be interpreted with caution, as delivery is just one dimension of cost assessment, and overall costs depend on the scale of interventions, crisis context, procurement practices etc. (World Bank, 2016).

<sup>5</sup> Although it is difficult to generalize on individual's preferences, [in-kind](#) transfers tend to be preferred in the context of high or volatile prices, or complete absence of functioning local markets (World Bank 2016; Sabates-Wheeler and Devereux, 2010), while a higher recipient's utility with cash is normally assumed (World Bank, 2016).

<sup>6</sup> This term and its singular "human affected" are used interchangeably with "recipient" and "end-user" in this thesis, the term "beneficiary" is avoided.

<sup>7</sup> For example, between 2010 and 2013, the number of African countries with unconditional cash transfers doubled (World Bank, 2016). Today, almost every country in Sub-Saharan Africa has some kind of [cash transfer](#) programme (Davis et. al, 2016)

reason in that sense is the rapid increase of [mobile phone penetration](#)<sup>8</sup> and Point of Sale ([PoS](#)) devices. With 70% of the bottom welfare quintile<sup>9</sup> in developing countries<sup>10</sup> possessing a mobile phone<sup>11</sup>, targeting even remote areas with e-assistance is seen as viable (World Bank, 2016).

Hence, not solely an incremental shift towards [CBA](#), but also towards its digital distribution as [e-transfers](#) can be observed, increasingly involving, inter alia, banks, payment providers and [mobile network operators](#) (Bemo et. al, 2017; ODI, 2015).

Transferring [CBA](#) with technological tools yields a huge potential for further increases in security, [efficiency](#), speed and transparency, convenience, traceability, reduced administrative and transaction costs and logistics (Kondakhchyan et. al, 2018; Bailey, 2017; Sossouvi, 2013).

To the recipients, it further potentially facilitates value-added services through [financial](#) and [social safety net](#) access beyond the humanitarian intervention, for post-[disaster](#) recovery (Bemo et. al, 2017; Blake et. al, 2016; World Bank, 2016; Global Innovation Exchange, 2016; Grossman and Nelson, 2014; Sossouvi, 2013).

---

<sup>8</sup> Particular attention must be given to the term [mobile phone penetration](#), as it does not refer to how many people possess a mobile in a country. Rather, it is an indicator describing the number of registered [SIM](#) cards/mobile phones to a country's total population. While penetration rates therefore might very well exceed 100% (International Telecommunication Union, 2018) due to some individuals possessing e.g. more than one SIM-card (GSMA, 2017a), it is not a good indicator for how many people of a country are actually included into the systems. Therefore, [unique mobile subscriber](#) data might yield a better, yet not perfect, proxy to retrieve information on how many people of a country are included. Looking into [unique mobile subscriber](#) penetration rates, e.g. Sub-Saharan Africa, with 43% in 2016, is expected to increase to 51% in 2020, remaining the region most left behind (George et. al 2016). Intuitively, World Bank's (2016) claim of 7 out of 10 of the bottom wealth quintiles in developing countries actually possessing a mobile phone, seems thus not to be very reasonable.

<sup>9</sup> Refers to either consumption or income, depending on the country (World Bank, 2016a).

<sup>10</sup> In this thesis, the term "developing" country refers to countries not possessing the average or higher per capita GDP of OECD countries, without aiming at imposing a normative hierarchy or categorization.

<sup>11</sup> Technology connectivity and penetration are however highly uneven across and within countries, often leaving the poorest and most vulnerable left behind (World Bank, 2016, Minges, 2012), especially in Least Developed Countries (LDCs) (International Telecommunication Union, 2018). For example, women in Sub-Saharan Africa were 17% less likely to possess a mobile in 2016 (GSMA, 2017a). Concerning mobile internet connection, the disparities are even more severe, with two thirds of the region still expected to be offline by 2020 (GSMA, 2017a).

#### 1.4. Digital cash-based assistance and financial inclusion

Especially the increased potential of [financial inclusion](#)<sup>12</sup> by the deployment of technology for e-[CBA](#) is emphasized in the literature (Bemo et. al, 2017; Cracknell and Atluri, 2017; Fabre and Aggiss, 2017; Global Innovation Exchange, 2016; Grossman and Nelson, 2014; Sossouvi, 2013) as having a “transformative” character to its recipients. If [financial inclusion](#) beyond a humanitarian intervention would take place due to an [e-transfer](#), target populations could not only access [humanitarian assistance](#) during crises, but also build resilience to better manage risk and shocks in the future (Bemo et. al, 2017; Fabre and Aggiss, 2017).

On a broad level, concerns about long-term impacts of [humanitarian assistance](#) can be situated in a re-surfaced discussion around a “[humanitarian-development nexus](#)”. Stemming from increased occurrence of [protracted crisis](#), seeking linkages between (short-term) humanitarian and (long-term) development efforts has gained attraction in recent years (United Nations Office for the Coordination of Humanitarian Affairs [UN-OCHA], 2017). In that sense, is not only cash-delivery itself considered as an important corner stone to bridge the nexus’ divide, but also the provision of financial services (El-Zoghbi, 2017; El-Zoghbi et. al, 2017).

Providing e-[CBA](#)-recipients with a basic transaction account that can be leveraged for a more robust [financial inclusion](#) however requires certain “rules of the game”, to ensure a fair and sustainable use of digital payments as [mechanisms](#) (Global Innovation Exchange, 2016).

Major humanitarian organisations accordingly agreed on the [Barcelona Principles for Digital Payments in Humanitarian Response](#) (Global Innovation Exchange, 2016). These principles, amongst others, suggest making use of existing national/local digital payment systems where feasible, preferably those offering potentials for wider

---

<sup>12</sup> Recipients however still might stick to more traditional/informal [financial service providers](#) after the interventions due to various reasons, such as familiarity with informal [mechanisms](#), or withdrawing the whole assistance at once to meet pressing consumption needs (Bailey, 2017). Hence, one cannot assume increased [financial inclusion](#) just by formally offering access to financial services via technology. However, even if increasing access to [digital financial services](#) (DFS) is neither an appropriate goal nor a priority of the interventions, humanitarian organizations still should use digital delivery systems where they offer the most efficient, accessible and transparent way to deliver [CBA](#) (Bailey, 2017). Thus, while [CBA](#) as response to emergencies should not be regarded as a primary tool for [financial inclusion](#) the opportunity to do so should be kept in mind (Fabre and Aggiss, 2017).

[financial inclusion](#) of recipients during a humanitarian response (Global Innovation Exchange, 2016).

## 2. So, all good?

### 2.1. Chapter Overview

The second chapter describes current challenges to [financially inclusive humanitarian assistance](#) using [e-transfer mechanisms](#) for a hypothetical human affected. Firstly, on a more general level and subsequently more narrowly tied a specific obstacle.

### 2.2. Exclusion from financially inclusive e-transfer mechanisms

There are some unneglectable advantages of delivering [CBA](#) digitally. However, shifting from analogue delivery to [e-transfer mechanisms](#) is not necessarily geared towards improving experiences for all types of recipients (Kondakhchyan et. al, 2018).

In alignment with one of the main principles of [humanitarian assistance](#), [Impartiality](#) (UN-OCHA, 2008),<sup>13</sup> also meaning that any [CBA](#)-delivery should be non-exclusive to [marginalized populations](#), the use of technology can be problematic.

As [e-transfers](#) necessarily involve (see Appendix 2) the utilization of [Information and Communication Technology \(ICT\)](#) in the delivery chain, [digital divides](#), oftentimes mirroring analogue inequalities (Zambrano, 2017), can undermine a fully (financially) inclusive system (Sossouvi, 2013).

More sophisticated payment [mechanisms](#), such as [mobile money](#), demand substantive access to hardware, infrastructure and [identity documents](#) (GSMA, 2017; Bailey, 2017; Gigler, 2015; Sossouvi, 2013). Input-factors, that are not always in the hands of [marginalized](#) recipients.<sup>13</sup>

Besides a lack in access, the characteristics of underlying technologies for [e-transfers](#) may prevent an adequate technology utilization, for example, if individuals are illiterate (Zambrano, 2017; GSMA, 2017; Bailey, 2017; Gigler, 2015; Grossman and Nelson, 2014; Sossouvi, 2013).

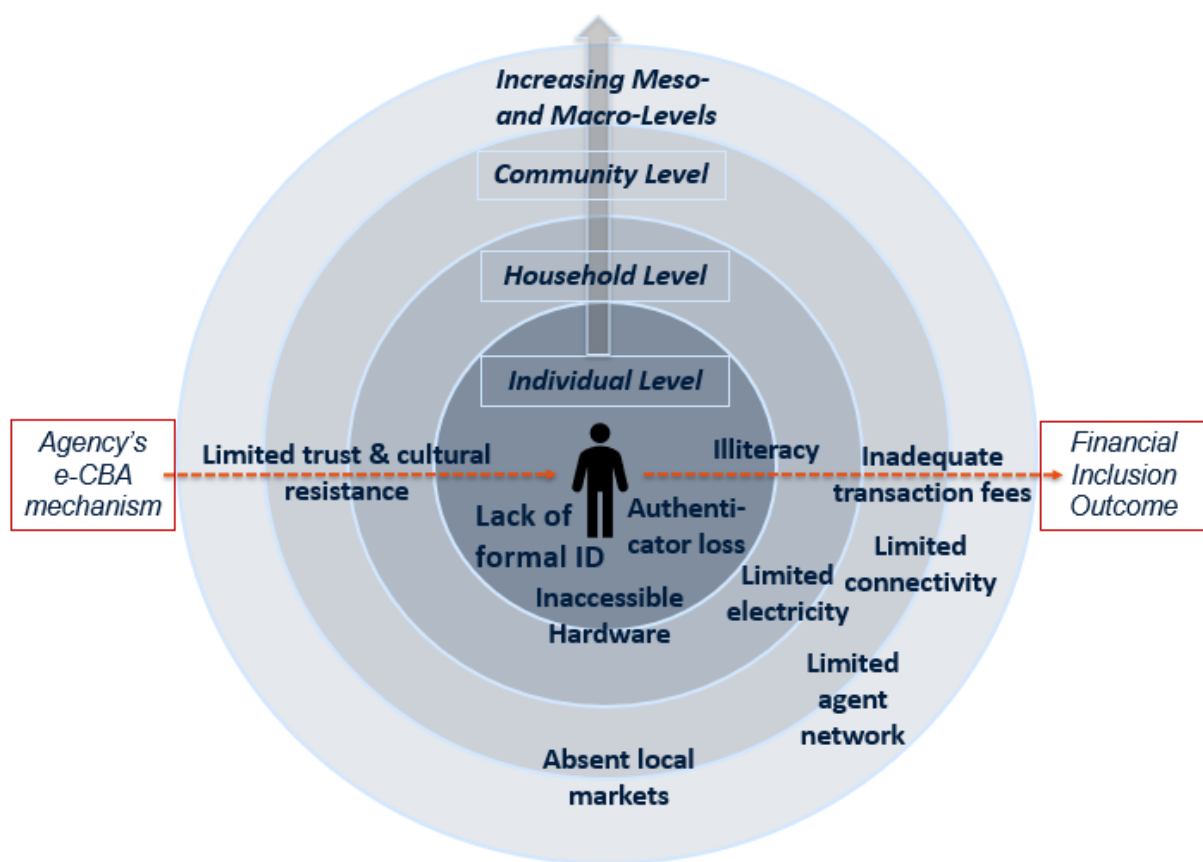
---

<sup>13</sup> It should be mentioned however, that involving intermediaries (such as [mobile money agents](#) etc.) possessing the required inputs could (partially) overcome these obstacles (Zambrano, 2017), but this potentially creates other issues, such as data protection concerns to the human affected by the involvement of third parties (Privacy International, 2018).

Furthermore, an incautious deployment of technology without strong data-protection could pose threats to positive outcomes of an intervention, if for example persecuted minorities experience further stigmatization due to the deployment (United States Agency for International Development [USAID], 2017; Nyst et al. 2016).

Figure 1 thus provides a non-exhaustive overview<sup>14</sup> summarising some in the literature identified factors potentially preventing *marginalized populations* from being gainfully *financially included* by e-CBA systems. Appendix 3 elaborates figure 1.

Figure 1: Framework for financially non-inclusive e-CBA



Source: Author's own contribution

Breaking down these considerations to a more operational level, Appendix 3 describes currently existing types of *e-transfers mechanisms* and their minimum equipment-

<sup>14</sup> Kindly note, that this non-exhaustive framework aims not to be complete but solely provides some potential exclusion and inclusion determinants found in the literature (see Appendix 3). These existence and relevance of the determinants will vary depending on the specific *e-transfer* mechanism, the specific context and the specific individual. The placement of the determinants on and between different micro- and meso-levels in figure 1 thus is merely suggestive.

requirements to the recipient and involved [agents/vendors](#). Appendix 4 provides, applying the in Appendix 2 laid out dimensions of access and appropriateness, a non-exhaustive overview about some drawbacks and benefits to the human affected per e-[CBA mechanism](#) in general.

There are potential obstacles for [marginalized](#) groups to be included in any humanitarian [e-transfer](#) scheme, as can be seen in Appendix 4, which carefully need to be considered before the intervention.

### 2.3. Higher barriers to financially inclusive ([open-loop](#)) mechanisms

More sophisticated [mechanisms](#), which can enable recipients to participate in [open-loop](#) payment systems as demanded by the [Barcelona Principles](#)<sup>15</sup>, grant the largest freedom of choice (Bemo et. al, 2017; Ford, 2017; Cornish, 2016) and potentials for long-term impacts via [financial inclusion](#) (GSMA, 2017; Zimmerman et. al, 2016), but also pose the most hindrances to a fully inclusive system in terms of required access-inputs and capabilities.

[Open-loop mobile money](#) systems<sup>16</sup> are particularly lobbied for by the supply side (Osafo-Kwaako, 2018; Bemo et. al, 2017), since mobiles are distributed globally and are functionally most adaptable (Grossman and Nelson, 2014), this could significantly reduce the cost of setting up [PoS-devices](#) or [ATMs](#) (Sossouvi, 2013).

Despite the potential of leveraging the increasingly conducive environment for digital payments and linking them to commercially provided financial services, many practical challenges might remain, as figure 1 indicated.

Facing a disaster, the priority of reaching human affected with [humanitarian assistance](#) as fast as possible, particularly in (digitally) nascent markets<sup>17</sup>, utilizing digital payment

---

<sup>15</sup> Due to ambiguous definitions of [open-loop](#) systems in the literature, the definition found in the [Barcelona Principles](#) will be primarily utilized for this thesis. In that context, [open-loop](#) payment systems refer to “payment systems that enable recipients to store value, withdraw cash, purchase items, or perform a variety of other transactions” (Global Innovation Exchange, 2016, p. 3). The common norm of seeing [open-loop](#) as necessarily interoperable among various payment-channels hence becomes secondary.

<sup>16</sup> Many [DFS](#) have been launched as [closed-loop](#) systems operating on an individual [mobile network operator](#) (MNO) service (Brand Engel and Scher, 2014.). According to Brand Engel and Scher (2014), a [closed-loop](#) system limits the ability of customers to transact with peers using a different [MNO](#) service.

<sup>17</sup> For example, when the user base or the [agent](#)-system is not well established (Zimmerman and Martin, 2016).

mechanisms might cause unacceptable delays (Zimmerman and Martin, 2016). Hence, digital payments, if adopted at all, are often disbursed through [closed-loop](#) systems (Zimmerman and Martin, 2016).

These systems are usually created abroad and for short-term use, without connecting users to an account enabling to store, send and receive funds beyond the humanitarian response (Zimmerman and Martin, 2016).

For example, (digital) [cash vouchers](#) are a common tool for immediate relief, but generally designed with features prohibiting further financial access (Zimmerman et. al, 2016).

Therefore, humanitarian agencies oftentimes are not able to sufficiently satisfy the according [Barcelona Principle](#).

#### 2.4. The global ID challenge - a major financial inclusion barrier

One of the most severe problems (Bemo et. al, 2017) for accessing an [open-loop](#) system, such as a [mobile money e-wallet](#), is of regulatory nature:

Figure 1 mentioned the lack of official [identity documents](#) (IDs). This is preventing a fulfilment of Know You Customer ([KYC](#))-regulations.

[KYC](#) generally refers to the information that regulators require regulated [financial service providers](#) to perform [due diligence](#) on their customers and nature of their transactions,<sup>18</sup> to discourage financial products being used for Money Laundering (ML) or other crimes , such as Terrorism Financing (TF) (CaLP, 2017 and GSMA, 2017, Levin et. al, 2015).

As part of the Digital Financial Service ([DFS](#)) providers, [mobile money](#) providers are required to conduct [KYC](#) checks when opening customer accounts, in line with national regulations and global [AML/CTF](#) standards (GSMA, 2017).

In most countries, it is not possible to register an individual for these services without an acceptable form of photo identification issued by national authorities (GSMA, 2017; Bemo et. al, 2017).

---

<sup>18</sup> [KYC](#)-standards usually regulate entities, not individuals (Levin et. al, 2015). In this thesis, [KYC](#) is oftentimes used as umbrella-term broadly referring to the hindrance to subscribe to ([DFS](#)) due to [AML/CTF](#) laws preventing sufficient [CDD](#) for un(der-)documented.

However, globally, above one billion individuals lack [legal identification](#) (Juden and Pisa, 2017), and [financial service providers](#) would normally fail to comply with [KYC](#)-regulations, if they were to enrol these undocumented individuals (Bemo et. al, 2017).

Humanitarian organisations are not included under the list of financial and quasi-financial entities that must comply with [KYC](#)-rules. However, any entity, with which the agency would partner with to deliver [CBA](#) would be subject to [KYC](#)-standards (Levin et. al, 2015).

While not every kind of [e-transfer](#) (see Appendix 4) requires people affected holding a legally issued ID document, [open-loop](#) systems enabling [financial inclusion](#), such as [mobile money](#), usually do (GSMA, 2017). Although also mobile [e-wallet](#) systems can be designed with restrictions providing greater control and fund visibility (GSMA, 2017b), this does not align with the motivating principle behind e-[CBA](#) - empowering recipients to make their own decisions (Bemo et. al, 2017) and achieving long-lasting impacts (Global Innovation Exchange, 2016).

Hence, if humanitarian organisations were to stick to the [Barcelona Principles](#) and aim to include a human affected into [open-loop](#) payment systems for sustainable [financial inclusion](#), [KYC](#)-regulations generally will need to be complied with (Ford, 2017; GSMA, 2017b; USAID, 2017).<sup>19</sup>

Eventually, in the case of un-documented human affected, humanitarian organisations are usually forced to stick to less [efficient](#), [closed-loop](#) e-[CBA mechanisms](#) (GSMA,

---

<sup>19</sup> In the humanitarian context, PA usually does not approach the service provider to establish a temporary or permanent relationship, the humanitarian institution contracts the service provider. There is thus a business relationship between the agency and the service provider, not between the human affected and the service provider. The agency usually provides the funds, and the selected service provider facilitates the distribution of those to the human affected. The nature and purpose of these transactions and the correlating source of funds are thus already known. The humanitarian agency usually provides the service provider with a case number that is assigned to each human affected. The information that links the case number and the identity of the beneficiary is retained by the humanitarian organization. If cash was for example distributed through [mobile money](#), the phone and the [SIM](#) card were taken out in the humanitarian organization's name and not the end user's name. The responsibility of identifying and verifying the human affected is placed on the humanitarian agency, but not necessarily for the purpose of complying with [KYC](#)-standards, but for registering e.g. refugees and providing them with [CBA](#) (Levin et. al, 2015), without a longer-term provision of e.g. an account to store value. Thus, a further [financial inclusion](#) of the recipient usually cannot take place, if he or she is bound to a [closed-loop](#) payment system (International Rescue Committee, 2016; Bemo et. al, 2017).

2017b; Zimmerman and Martin, 2016), including restrictions on deposits, withdrawals and transfers to mitigate [ML](#) risks (Cracknell and Atluri, 2017).

Therefore, humanitarian agencies potentially fail to yield the envisioned positive impacts on response and resiliency efforts via [financial inclusion](#), until the critical issue of [KYC](#)-compliance for un-documented is addressed (Bemo et. al, 2017).

Beyond the institutional goals of the [Barcelona Principles](#), the global ID-challenge is far more problematic than just the failure to satisfy [due diligence](#) requirements, as un(der)-documented populations are per se excluded from many public services, such as voting, access to health care, education etc. (World Bank and GSMA, 2016).

This problem disproportionately impacts women and children in Africa and Asia (World Bank and GSMA, 2016) in rural regions with the highest burden of extreme poverty (USAID, 2017); and, even more severely, displaced populations (GSMA 2017b; Juden and Pisa, 2017).

Although providing [legal identification](#) to everyone thus is an explicit target of the Sustainable Development Goals (United Nations Department of Economic and Social Affairs [UN-DESA], 2015)<sup>20</sup>, wide identification gaps remain.

### 3. The Solution?

#### 3.1. Chapter Overview

Following chapter outlines a potential solution to previously described obstacle to [financially inclusive humanitarian assistance](#) using [e-transfer mechanisms](#) – the global ID-challenge and why this potential solution needs further research.

#### 3.2. Supporting un-documented with (digital) humanitarian IDs

Governmental bodies are not the only ones issuing [identity documents](#).

Other institutions, such as private companies, but also humanitarian agencies, create ID systems to enrol, validate and authenticate their users (USAID, 2017; World Bank and GSMA, 2016).<sup>21</sup> Such ID systems often rely on [ID tokens](#) - physical objects (e.g.,

---

<sup>20</sup> “By 2030, provide legal identity for all, including birth registration” (UN-DESA, 2015, SDG 16.9).

<sup>21</sup> For a short overview on classifications of currently existing ID-systems, refer to Appendix 1 – glossary, term “[Digital Identity Systems](#)”.

a card), or information pieces (e.g., a [PIN](#)) that are utilized to support identity claims (USAID, 2017).

Especially, in a context where the public sector lacks the capacity to provide official documentation, humanitarian institutions and their IDs play a vital, and sometimes, sole role (GSMA, 2017b). According to GSMA (2017b), this is particularly the case in Least Developed Countries (LDCs).

For humanitarian organisations, [digital ID systems](#) have gained more and more adoption, for example due to lower duplication and thus fraud, lowered costs and reduced time spent on registration and authentication,<sup>22</sup> when compared to analogue alternatives (USAID, 2017; Price, 2008).

For example, after introducing fingerprint verification in a Kenyan refugee camp, within 6 months, the World Food Programme ([WFP], 2016) claimed monthly savings of \$1.5 million and a 20 percent reduction in refugee numbers (due to lowered duplication).

Furthermore, improved updatability of data and data-driven programming, the possibility of streamlining humanitarian and social services, simplified monitoring and reporting processes are potentials of [digital IDs](#), as well as increased transparency by linking people to transactions in unique entries (USAID, 2017) are alleged advantages.

For the people affected, these potentials can yield improved time-[efficiency](#) of receiving assistance, as well as improved adequacy/coverage due to improved [value for money](#) (Chifabfa, 2014; Scott, 2014; Kopinak, 2013).

Hence, digital technology is increasingly used to collect, process, and store data to enhance the integrity of ID systems (USAID, 2017).

Inherently, aligning with the general trend towards [e-transfers](#), [digital identity systems](#) are a complementing feature of e-[CBA](#) delivery (Ford, 2017) - digital payment systems can be leveraged to enable [digital identification](#) and vice versa (Zimmerman, 2017).

---

<sup>22</sup> For a brief explanation of the registration, issuance and authentication processes, refer to Appendix 1 – glossary, term “[Digital Identity Systems](#)”.

Given technological advances in, for example, [biometrics](#), combined with the extensive use of mobile devices<sup>23</sup> in developing countries, [digital IDs](#) allegedly offer a transformative and efficient solution to the global ID challenge (UNHCR, 2018; USAID, 2017; World Bank and GSMA, 2016).

Consequently, if a [digital Identity](#) for humanitarian purposes could outlive the time-limited intervention and link holders to more constant public services, due to e.g. [KYC](#)-satisfaction (GSMA, 2018; USAID, 2017; Zimmerman and Martin, 2016); the chance for better risk management and recovery during extended humanitarian crises or post-[disaster](#) recovery periods (USAID, 2017; Blake et. al, 2016) would be enhanced.

### 3.3. The Silver Bullet?

Although there is a consensus in literature, that humanitarian institutions benefit from [digital identity systems](#), people affected might not. Threats arising from the utilization of a [digital ID system](#) may for example entail a centralization of data in digital data bases increasing privacy threats, in-transparent or in-consensual data (“over”)-collection, data-abuse or lack of data-privacy (e.g. by linkable identifiers, lack of blinding information, lack of pseudonymisation), or the impossibility to withdraw consent (Nyst et. al, 2016).

Intuitively, any in-consensual data leakage of [Personally Identifiable Information](#) (PII), is especially problematic in a context of discriminatory and exclusionary practices or violence directed towards a as homogenously considered group of individuals (USAID, 2017; Levin et. al, 2015).

Accordingly, does Sossouvi (2013) conclude, that however attractive an option for [e-transfers](#) is, if humanitarian agencies cannot guarantee the protection of sensitive PA’s data, [e-transfers](#) should not be considered.

However, have most humanitarian organisations not yet incorporated [privacy-by-design](#) principles into their data management systems, no standard or recognized

---

<sup>23</sup> Mobile phones have become an increasingly significant part of identity system infrastructure and are likely to be part of all emerging technology trends, such as [blockchain](#)-backed IDs, [algorithmic IDs](#) and [biometrics](#). (USAID, 2017). For example, can mobile phones serve as a platform for fingerprint, voice or facial recognition or other factors of authentication, such as [PINs](#) or passwords; they are thus capable of multi-factor authentication. By itself, a mobile phone can further serve as an ID, if it contains a with an [MNO](#) registered [SIM](#) card (USAID, 2017).

humanitarian data protection policies guide humanitarian agencies to protect the data privacy of the human affected (USAID, 2017; Levin et. al, 2015).

Moreover, sectors such as banking or telecommunications are usually strictly governed and provide their infrastructure only upon acceptance of their conditions (Privacy International, 2018), such as [KYC](#)-compliance. These private companies are increasingly intermediaries for the humanitarian sphere and its target groups (Pirlot de Corbion et. al, 2018).

Relating to [KYC](#), Levin et. al (2015) attest, that humanitarian agencies strongly rely on the service providers responsible for performing [due diligence](#) in defining the purpose of the data collection, utilization and disclosure, with these definitions then operating as the de-facto data privacy policy.

In the age of digital identities, the collected and processed data for [KYC](#) purposes is more and more circulated among various private and governmental intermediaries and therefore subject to exponential fraud, data-leakages and mis-use, out of the control and sight of the individuals (GSMA, 2018; Tobin and Reed, 2017; Levin et. al, 2015).

Thus, even if a humanitarian organisation internally adheres to high data protection standards, involving intermediaries in its delivery chain and letting them perform [KYC](#), can have vast negative consequences to the human affected.

### 3.4. Reality Check: Fragmented functional systems, instrumental designs

Apart from various risks to the human affected arising from the use of [digital IDs](#) itself, are humanitarian ID systems currently mostly fragmented (USAID, 2017), and most identity management systems centralized (World Economic Forum, 2018; Tobin and Reed, 2017)

Current common practice in the sphere of [humanitarian assistance](#) thus is that an agency issues a functional ID to its target group. A functional ID system is designed for serving a specific purpose, in this case, receiving [humanitarian assistance](#) (USAID, 2017).

Commonly serving the sole purpose of accessing humanitarian relief, the humanitarian schemes are not being recognised as form of ID meeting, for example, [KYC](#)-standards for accessing financial services (GSMA, 2017b; USAID, 2017).

Notwithstanding, comparable with physical infrastructure, a [digital ID system](#)'s utility and compatibility with existing local systems are crucial to its long-term sustainability (USAID, 2017).

Treating humanitarian ID systems as fulfilling a sole, functional purpose, further usually yields “instrumental” designs. Instrumental designs are highly contextualized, rely on unique standards and/or proprietary technology (USAID, 2017).

This results in the ID-systems not only being singularly functional but further incompatible among the various actors in the humanitarian sphere, with the usability limited to a single intervention (USAID, 2017).

For example, if a recipient of [humanitarian assistance](#) would receive [CBA](#) from WFP and a Red Cross Society, he or she commonly could not use the [ID credentials](#) of the Red Cross Society to authenticate for WFP's [CBA](#) or vice versa.

This situation can partly be attributed to ID providers' tendency to prioritize their own [efficiency](#) goals over the needs and experiences of ID users. The narrow focus on institutional and donor's aims consequently creates to sector-specific, siloed ID systems, which are “locked in” with specific [vendors](#) (USAID, 2017). This led, in turn, to vast inefficiencies to the agencies, but also for the individuals, as he or she is required to carry various functional, limited-purpose, IDs (USAID, 2017).

And even if inter-agency information sharing was possible, non-transparent policies and information utilization might undermine what is in the best of the recipients' interests (Levin et. al, 2015).

### 3.5. Foundational systems, infrastructural designs – A pathway to financial inclusion and beyond?

Other than functional systems, allow foundational ID systems for multiple functional purposes and follow the intention to provide identification as a public good (USAID, 2017).

Normally, national governments serve as providers of foundational ID systems (USAID, 2017). These (normally physical) identity cards issued by the public sector tend to be widely recognized as a “legal” form of identity (Lynch, 2017).

Foundational ID systems tend to be built with an “infrastructural” design. Infrastructural design approaches view ID systems as core infrastructure to support other systems

and activities and thus can be compatible with local systems (Lynch, 2017; USAID, 2017).

Functional IDs in general can also serve multiple purposes though. For example, a driver's license can be accepted not only for operating an automobile but be used as ID for activities unrelated to driving (USAID, 2017), for example, verifying one's age for an age-restricted service.

In the sphere of [humanitarian assistance](#), the refugee [identity](#) card issued by UNHCR might provide a good example of a functional ID serving a more foundational character.

Normally, this ID supports the operations of the UNHCR, but especially in states, where governmental ID systems are weak or absent, or a refugee population living out of the scope of formal identity systems is hosted, this ID card can enable to access wider public and financial services (GSMA, 2017b; USAID, 2017).

For example, in Malawi, refugees living in Dzaleka refugee camp recently were eligible to open a bank account with their UNCHR-issued refugee ID card (Hansen, 2018; Msiska and Ghelli, 2018).

Such an ID system thus could potentially be leveraged for [KYC](#)-alignment (GSMA, 2018; USAID, 2017; Zimmerman and Martin, 2016).

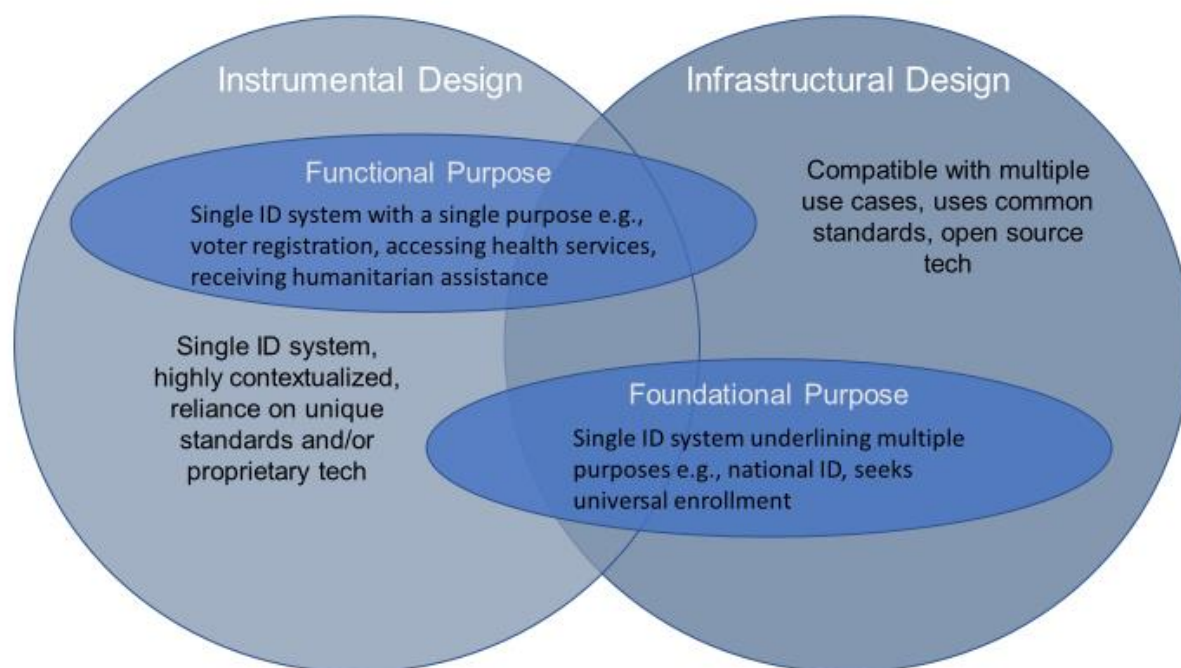
This implies, that a functional ID system of a humanitarian organisation can serve a more foundational purpose, especially if an infrastructural design allows for its interoperability among stakeholders (USAID, 2017), such as entities involved in [KYC](#)-procedures (GSMA, 2018).

While the urgency of humanitarian interventions may preclude waiting for a (governmental) foundational ID system that is currently weak or absent, a functional ID system thus should not only strive towards re-purposability, but even potential "backward integration" into a future foundational system (USAID, 2017).

As such an ID system would then increasingly be linked to a broader segment of services, its value would increase, thus reinforcing continued participation and growth of and in the system, eventually creating a foundational system (USAID, 2017).

Figure 2 relates the overlapping definitory space of functional and foundational systems and instrumental and infrastructural approaches.

Figure 2: Foundational & functional systems, infrastructural & instrumental designs



Based on USAID (2017)

Finally, one may conclude, that either a humanitarian agency's deployment of a foundational system, or a functional system incrementally upgrading or being integrated into a foundational system could overcome the lack of [legal IDs](#).

### 3.6. Context matters

While governments usually play a large role in foundational (digital) identity systems, (non-) governmental participation depends on context-specific needs and capacities, existing identity infrastructure and services and so forth (World Bank and GSMA, 2016).

Similarly, the manner in which identification supported by a humanitarian organisation yields a more foundational purpose, such as an alignment with [KYC](#)-standards, depend specifically on the country, its regulation, potentially conflicting (humanitarian) requirements, such as individual data protection<sup>24</sup>, nature of service providers and

<sup>24</sup> Relating to the concerns of data protection, it is for example advised to explicitly incorporate personal information protection principles into humanitarian [KYC](#)-guidelines and minimize personal information and their use as much as possible (Levin et. al, 2015).

other intermediaries, applicable legislation of donor countries, and so on (GSMA, 2018; Levin et. al, 2015).

Therefore, the question, under which circumstances an ID system supported by a humanitarian agency could yield a government or service provider to accept a more foundational purpose, is highly contextual.

## 4. Use Case

### 4.1. Chapter overview

The next chapter provides context, scope and specific ID-system providing the use-case to investigate above potential solution to the global ID challenge for [financially inclusive humanitarian assistance](#) using [e-transfer mechanisms](#).

### 4.2. Context of Malawi and Kenya

To make a use case, this thesis shall focus on two distinct countries: Malawi and Kenya.

These countries were chosen in collaboration with The Netherlands Red Cross (NLRC)'s 510 initiative. 510 currently plans to perform e-[CBA](#) interventions in these countries by integrating [blockchain](#)-technology in its "121-system", with, among others, a scalable and interoperable [Self-Sovereign Identity](#). While the main aim is to improve [humanitarian assistance](#) for both ends, the initiative has a vested interest in the 121-system fulfilling a more legal purpose and gaining broad (intersectoral) adoption.

### 4.3. KYC-satisfaction for DFS as analytical lens

Given the global ID-challenge, inter alia, potentially preventing [open-loop](#) e-[CBA](#) when adhering to the humanitarian principle of [Impartiality](#), a humanitarian digital ID's potential for satisfying [KYC](#) provides the narrower analytical lens for the underlying broader question of whether a non-governmental ID can achieve a more foundational character in both contexts.

Intuitively, if a government would formally accept that kind of ID to align with [KYC](#)-standards, the effects on trust would be immense, yielding potential acceptance of the ID for other public services (Cracknell and Aluri, 2017) and thus, a more foundational character besides the functional purpose of [humanitarian assistance](#).

Due to the correlated trends towards digital [CBA](#) and [identification](#) within the humanitarian sphere and the system's specific characteristics, [KYC](#) for [DFS](#) shall specifically be regarded.

#### 4.4. Focus on national, open-loop enabled DFS-systems

In alignment with the [Barcelona Principles](#) and as recommended by Bemo et. al (2017), World Bank (2016) and ODI (2015), the subsequent context analysis shall furthermore focus on already existing national/local [open-loop DFS](#) systems.

As indicated in previous sections, [open-loop-mechanisms](#) are subject to stricter [KYC](#)-regulation when compared to [closed-loop](#) alternatives on the one hand (Ford, 2017), but allegedly provide wider benefits to the human affected on the other (Bemo et. al, 2017). An [open-loop KYC](#)-satisfaction thus can yield a higher utility and a stronger proxy of trust - and therefore, a higher propensity to become foundational (USAID, 2017).

#### 4.5. Focus on open-loop mobile DFS-systems (if possible)

While the question of how a humanitarian ID can satisfy [KYC](#)-requirements for [open-loop DFS](#) is not explicitly tied to a specific [mechanism](#), mobile-based [DFS](#) shall be specifically regarded, if present and dominant in the contexts.

That decision was made due to the following reasons:

Firstly, as with investigated ID-system, mobile phones are an increasingly crucial piece of [digital identity system](#) infrastructure<sup>25</sup> (Clark and Gelb, 2013) and likely to be part of all emerging technology trends, such as [blockchain](#)-backed IDs (USAID, 2017). Secondly, as previous sections indicated, could the wide mobile-penetration in developing contexts be leveraged to leap-frog traditional [DFS](#) and identity systems. Thirdly, in respect to [KYC](#), subscribing to a [mobile money](#) account is normally easier than opening a bank account (GSMA, 2017).

---

<sup>25</sup> Mobile phones for example serve as a platform for fingerprint, voice or facial recognition or other factors of authentication, such as [PINs](#) or passwords; they are thus capable of multi-factor authentication. Can a mobile phone can further serve as an ID, if it contains a with an [MNO](#) registered [SIM](#) card by itself (USAID, 2017).

## 4.6. Focus on Self-Sovereign Identity as digital ID system

### 4.6.1. Beyond traditional digital ID ecosystems

The question of legal acceptance does not only depend on contextual factors, but also on the specific identity system a humanitarian agency intends to use (USAID, 2017).

Promising to overcome some threats and caveats arising from traditional digital identity management systems, [SSI](#) have recently gained attention. Due to the emergence of [blockchain](#) technology, or more broadly, [Distributed Ledger Technology](#), the concept of [SSI](#) is becoming more popular, as [blockchain](#) technology may finally provide the required enabling software-architecture (GSMA, 2018; Stevens, 2018; Juden and Pisa, 2017; USAID, 2017), given their, inter alia, decentralised nature and utilization of asymmetric cryptography (GSMA,2018; Zambrano, 2018).

Providing ownership to its holder, to decide with whom to share which data, while the technological characteristics allegedly enable a strong individual privacy and data-protection without compromising the trust into and the transparency of the system (Zambrano, 2018; Lewis, 2017; USAID, 2017; Tobin and Reed, 2017; Allen, 2016), [SSI](#) is a potential gamechanger of humanity's relationship with the concept of [identity](#) and its management systems.

Aligning with the 510-initiative, a [Self-Sovereign Identity](#) (SSI) thus will specifically be regarded. While still being in development, the final end-product of regarded ID-system may not only incorporate [privacy-by-design](#) principles, but, given entity's humanitarian background, [humanitarian information management principles](#) (Stevens, 2018).

Relating to [KYC](#), does the [ID2020 Alliance](#) (2017) initiative attest user-owned and controlled [digital identities](#) to not only promise improved user-experiences, but also hold, amongst others, promises of a drastic reduction of [Personal Identifiable Information](#) (PII) held and overall costs associated with [KYC](#)-procedures by and for [FSPs](#). Relating this to the concerns of data protection, as Levin et. al, (2015) suggest, explicitly incorporating personal information protection principles into humanitarian [KYC](#) guidelines and minimizing personal information and their use as much as possible could thus be enhanced.

However, as if the question of regulator's acceptance of humanitarian IDs for legal purposes was not already complicated (and sensitive) enough, the abstract concept of [SSI](#), its high entry barriers, technological complexity and immaturity (Zambrano, 2018) add a considerable intricacy to the research.<sup>26</sup>

Generally, as Zambrano (2017) attested, [blockchain](#) applications are hurrying ahead local policies and regulations, and particularly non-industrialized countries are struggling to catch up. Relevant decision-makers' previous knowledge or engagement with both concept and technology can thus not be assumed, nor that a [SSI](#) utilizing [blockchain](#) is best positioned to increase identity inclusion in complex development contexts (Zambrano, 2018). However, as end-user adoption will depend on additional benefits the technology may provide (Zambrano, 2018a) and its application to development contexts (Zambrano, 2018b), an argument for investigating its potentials for enhanced [KYC](#)-satisfaction could be assumed.

On a narrower level, relating to [KYC](#), two aspects of an [SSI](#) utilizing [blockchain](#) as underlying software architecture will be relevant to the research in further detail.

#### 4.6.2. Minimization and Pseudonymization

One of the key features an [SSI](#) adheres to, the minimization of identity claims (Allen, 2016), can be achieved with [blockchain](#)'s cryptographic tools yielding pseudonymization (Zambrano, 2018), while using the distributed trust, transparency and immutability of the ledger (Zambrano, 2018), to ensure a service provider, that an individual already has undergone full [KYC](#)-checks validated by another authority (GSMA, 2018).

This means, that by using asymmetric cryptography, while still making it simple to verify, that a certain transaction can be attributed to a certain individual or entity (GSMA, 2018), a [KYC](#)-check could formally be complied with, without a service

---

<sup>26</sup> Kindly note, that technological characteristics of [Self-Sovereign Identity](#) and [Distributed Ledger Technology](#) in general, and from these characteristics arising prospects for [humanitarian assistance](#) and human development are depicted in a harshly simplified and reduced form in this paper, which is rather pursuing a narrow scope on aspects relevant to [KYC](#)-regulation. For a comprehensive (potential) system design, refer to Sevens' (2018) substantive work.

provider actually accessing and holding all [PII](#) retrieved during enrolment, when undergoing authentication for a service (USAID, 2017).

This abstract possibility however potentially conflicts with traditional [KYC](#)-standards applicable to individual customers, demanding the service provider establishing the relationship to obtain and verify individual data, such as the name, temporary/permanent address and nationality, as laid out in the Financial Action Task Force's ([FATF] 2012-2018)-recommendations.<sup>27</sup>

Coming back to Zambrano (2017), one hence cannot assume this possibility yet being considered by relevant institutions in Malawi and Kenya.

#### 4.6.3. Assertion and Trust

Above possibility of [KYC](#)-checks with reduced [PII](#)-revelation brings up another issue - the question of trust.

Accretionary ID models such as some [blockchain](#)-backed IDs hypothetically allow for individuals to self-assert identity claims with little or no supporting information, and build up that identity over time through interactions with other entities (USAID, 2017). Even without accretionary characteristics, the broadly common feature of [blockchain](#)-backed IDs is that individuals directly create and manage their identities (Zambrano, 2018). Due to a so far absent universal definition of [SSI](#) (Allen, 2016), it is disputed in literature, whether it necessarily needs to be self-asserted. Windley (2016) defines an [SSI](#) as necessarily being self-asserted, while some see it differently (GSMA, 2018; van der Veen et. al, 2018).<sup>28</sup>

Either way, self-assertion normally is insufficient for [KYC](#)-requirements (USAID, 2017). A layperson's example: A bank is most likely unwilling to accept your self-asserted identity from your Facebook-account to open a deposit account.

Thus, whether self-asserted or with the support of another party, eventually, self-reported claims will need to be verified (Windley, 2016) by a trusted authority (GSMA, 2018).

---

<sup>27</sup> Refer to: FATF's (2012-2018, pp.59) interpretative note to recommendation 10 ([CDD](#)) C. 5 a&b.

<sup>28</sup> In the humanitarian context, it would oftentimes make sense, to e.g. have an assistance worker supporting an e.g. illiterate individual in the process of self-registering (van der Veen et. al, 2018), while still giving the individual the control and access in and to the ID scheme in the broader sense.

If a humanitarian organisation provides an ID to a human affected, the relevant governmental bodies, or the service providers performing [CDD](#), must trust the credibility of identity claims and its verifier sufficiently to accept it for [KYC](#)-purposes. In government-led and joint-led ID schemes, the trust is usually achieved by public representatives being involved in the enrolment, issuance and [credentialization](#) processes (GSMA, 2017b). However, in humanitarian settings, it might be desirable for an agency, to serve as sole third-party verifier of identity claims, for example, a context of minority-persecution, or simply, due to practical reasons, for example, in a camp-context.

The question of which entities can assert and verify identity claims for a legal ID is certainly not a new question. While an [SSI](#), once completely developed and well understood, might influence a regulators' acceptance of a sole humanitarian verification, the arising question fundamentally is about more than trust; it is about the sovereignty of a nation in politically determining, who can provide [legal IDs](#) and to whom (World Bank and GSMA, 2016).

## 5. Research Question

### 5.1. Chapter Overview

This chapter summarizes previously made considerations and the specific use-case to yield this thesis' research question. Subsequently, the research question is broken-down into several sub-questions for guiding the research.

### 5.2. Synthesis to Research Question

The question, whether a humanitarian ID could serve more foundational purposes, is examined through the analytical lens of satisfying [KYC](#)-requirements in the contexts of Malawi and Kenya. Aligning with the trends towards the digitization of IDs and [CBA](#) delivery and increased mobile-backed interventions, a [digital ID](#) for satisfying [KYC](#) for [CBA](#)-delivery via [mobile money](#) is regarded. The aim of yielding [financial inclusion](#) **beyond** the intervention yields the focus on [open-loop](#) mobile systems. Ideally, the potential [KYC](#)-satisfaction would still enable [privacy-by-design](#) principles of a potential [SSI](#), thus the overall research question:

**How can a [Self-Sovereign Identity](#) deployed for humanitarian [cash transfers](#) satisfy [Know Your Customer](#)-requirements for mobile [open-loop](#)-payment systems in Malawi and Kenya?**

### 5.3. Operational Sub-Questions

To answer that question, it is broken down into the following operational Sub-Questions (SQs):

- i) How can the current political, economic, social and technological environment of the contexts in relation to [DFS](#) and [identity](#) be characterized?
- ii) What are minimum [KYC](#)-requirements to participate in an [open-loop](#) system in Malawi and Kenya for an individual?
- iii) Are [open-loop](#) payment systems in Malawi and Kenya currently utilized by humanitarian actors?
- iv) What are the minimum requirements for humanitarian organizations to meet [KYC](#)-standards for [open-loop](#) cash programmes in Kenya and Malawi?
- v) Could a humanitarian-backed ID satisfy [KYC](#)-requirements to yield inclusion into [open-loop](#) mobile [DFS](#)?
- vi) If so, can a [Self-Sovereign Identity](#) yield [open-loop](#) inclusion as well?
- vii) Is providing a humanitarian, foundational ID desirable in these contexts?

## 6. Methodology

### 6.1. Chapter Overview

To answer the research question, the operational Sub-Questions (SQs) are used to guide the research step-by-step. Broadly, this thesis' research methodology can be categorized into two different approaches, one being desk studies, one being semi-structured interviews.

Subsequently, the underlying motivation for the specific SQs and further, the methodological approaches for the desk study-based SQs are displayed.

### 6.2. SQ i) – iv: Desk Study

#### 6.2.1. General

For both contexts, desk studies to gather secondary data will be performed. All relevant information retrieved will be used to inform subsequent interview questionnaires.

## 6.2.2. SQ-specific Motivation and Approaches

*6.2.2.1. SQ i): How can the current political, economic, social and technological environment of the contexts in relation to DFS and identity systems be characterized?*

### **Motivation**

To get a clearer picture about both contexts on the national scale relating to the subject matter.

### **Approach**

For structuring answers, a PEST-Matrix<sup>29</sup> as analysis framework is loosely applied, with particular focus on public identity management systems in the political dimension.

*6.2.2.2. SQ ii) What are minimum KYC-requirements to participate in an open-loop system in Malawi and Kenya for an individual?*

### **Motivation**

A desk-study considering governmental and service provider (e.g. [MNOs](#)) regulation and bills relating to [KYC](#)-standards for [open-loop mobile money](#), if SQi) proves [mobile money](#) to be relevant in the contexts, will be conducted. After clarification of the minimum requirements to an individual (SQ iii), the inference, what these minimum [KYC](#)-standards mean to un(der)-documented individuals, can be drawn.

### **Approach**

The recent regulations and bills by relevant regulators and service providers will be analysed.

*6.2.2.3. SQ iii): Are open-loop payment systems in Malawi and Kenya currently utilized by humanitarian actors?*

### **Motivation**

The motivation for SQ ii) is twofold. One is identifying in (e-)[CBA](#)-interventions involved humanitarian stakeholders to inform about potential interviewees for answering subsequent SQs. The other is to target the ones specifically experienced with [open-loop](#). In case of absent programmes using [open-loop](#), such as [mobile money](#), current

---

<sup>29</sup> A PEST-Matrix is a framework commonly analysing political, economic, socio-cultural and technological macro-environmental factors relevant for strategic management (Sammut-Bonici, 2015).

hindrances relating to according [KYC](#)-regulations can be inquired in interviews taking place for later SQs.

### **Approach**

The focus of this SQ will lie on larger, multi-national organisations to increase the likelihood of potential insightful information.

As the problem statement pointed out, target groups of the humanitarian interventions might not necessarily possess required access or capability-factors for making meaningful use of an individually-owned [SSI](#) involving [ICT](#). This will be considered, when researching for previous humanitarian interventions.

Attention will further be given to distinguish between [closed](#)- and [open-loop](#) solutions, as the actors might utilize both, or a mixed form.

*6.2.2.4. SQ iv) What are the minimum requirements for humanitarian organizations to meet KYC-standards for open-loop cash programmes in Kenya and Malawi?*

### **Motivation**

While seemingly similar to SQ ii, SQ iv) stems from the motivation, that humanitarian actors, when performing an intervention, as creators of a business relationship with the service providers, oftentimes allow for easier – “tiered” individual [KYC](#)-regulations (Levin et. al, 2015). This normally happens if there is a humanitarian crisis (Levin et. al, 2015). There is a general tendency of the [KYC](#)-journey for unbanked starting with a simplified [KYC](#) and then a subsequent upgrading to full compliance by sequentially providing more [KYC](#)-related information (Cracknell and Aluri, 2017). Thus, the tiered [KYC](#) applicable to a humanitarian agency might provide an entry-point for [financial inclusion](#) of yet un(der)-documented in the contexts, e.g. given an [accretionary ID](#) model (USAID, 2017). Although this assumption must be confirmed or declined in later SQs, the desk studies already might provide insights to potential exemptions and tiered approaches, if a humanitarian agency is involved.

### **Approach**

Although retrieving exact agreements between humanitarian organisations and service providers/governments with desk studies assumingly might be difficult, investigating relevant interventions of the past might already reveal, whether some

kind of tiered or waived [KYC](#) for recipients of humanitarian [CBA](#) were applicable and whether the mechanism used was [open-loop](#) enabled or not.

### 6.2.3. Summary Desk Study Approach

The macro-national PEST-Analysis of SQ i) and the analytical (L)aw/ -lens of individual [open-loop KYC](#) of SQ ii) are complemented by information concerning relevant international humanitarian actors (I), their e-[CBA](#) interventions and potentially applicable lighter individual [KYC](#) in SQ iii) and SQ vi).

The overall analytical framework for the desk-studies thus broadly resembles a, to the SQs adapted, PESTLE-framework.<sup>30</sup>

*Figure 3: Analytical Framework for Desk-Studies*

Analytical Lens	PEST	L	I	
SQ	i)	ii)	iii)	iv)
Content	DFS & Identity Environment	Individual DFS-open-loop KYC	Humanitarian open-loop?	Humanitarian special status

## 6.3. SQ v – vii: Semi-structured Interviews

### 6.3.1. General

Retrieving all relevant and most current information of SQ i) to iv) solely with desk-studies cannot be assumed. Therefore, interviews with relevant stakeholders might offer an adequate approach to validate the desk studies and explore identified knowledge gaps. As the specificity of the Research Question relating to a non-governmental ID striving for a legal purpose in the contexts and the novelty and complexity of the concept of [SSI](#) underscore the further need for in-depth discussions combining contextual, regulatory, technological, political, social and ethical knowledge

<sup>30</sup> PESTLE is a PEST-Matrix extended by adding legal (L) and environmental (E) components (Sammut-Bonici, 2015). For the purpose of this thesis, (E) is replaced by (I), the relevant international humanitarian actors.

and considerations, "experts" and relevant institutional representatives will be reached out to and interviewed.

Therefore, semi-structured interviews will be conducted. This form of an interview is especially adequate when investigating complex issues, as questions can be asked in flexible order with less restrictions to potential answers when compared to structured interviews (Galletta, 2012). While still being based on a set of predefined and structured questions, the open character and flexibility allows for considerable reciprocity between participant and researcher. A space for the researcher is created to probe a participant's response for clarification, offering new meaning to and critical reflection of the topic (Galletta, 2012).

Offering an inductive approach, the main methodology applied for this thesis is hence qualitative in nature. Grounded data then provides the context for the interviewer's understanding of the topic of interest (Galletta, 2012).

### 6.3.2. SQ-specific Motivation

#### *6.3.2.1. SQ v) Could a humanitarian-backed ID satisfy KYC-requirements to yield inclusion into open-loop mobile DFS?*

##### **Motivation**

This question tackles the general issue of assertion and trust, as laid out previously.

Basically, this question investigates for the contexts,

- i) whether a service provider or regulating body would trust a humanitarian organisation sufficiently to accept the agency being the sole third-party verifier of (self-) asserted individual identity claims and to issue non-governmental [credentials](#) yielding [open-loop](#) payment system inclusion in these contexts, or
- ii) whether public officials would always need to be included in claim verification in a joint-led approach, or
- iii) whether according character of a humanitarian ID can (not) be achieved at all

This question is further set to tackle another issue:

Nations such as Jordan and Rwanda, have already revised [mobile money KYC](#)-regulations, allowing UN-issued identification as acceptable [KYC](#) for use in

[humanitarian assistance](#) (GSMA, 2017; Levin et. al, 2015). However, many countries have not designed more flexible [KYC](#)-regulations to provide open access to undocumented in case of a crisis, or beyond (USAID, 2017; GSMA, 2017; Bemo et. al, 2017; Levin et. al, 2015).<sup>31</sup>

In that sense, while some governments have shown willingness to modify and create tiered [KYC](#)-standards<sup>32</sup> **during** a humanitarian [disaster](#) (USAID, 2017; GSMA, 2017; Levin et. al, 2015), the inclusion into [open-loop](#) systems inherently aim at long-term impacts **beyond** the timeframe of the intervention<sup>33</sup> (Zimmerman et. al, 2016), and ideally already takes place **before** a humanitarian [disaster](#) occurs (Bemo et. al, 2017a; El-Zoghbi et. al, 2017; Blake et. al, 2016).<sup>34</sup>

Thus, a necessary pre-condition, that a humanitarian organisation's digital ID for [KYC](#)-alignment beyond the humanitarian intervention itself is accepted, comes into play.

---

<sup>31</sup> Especially an ID issued by humanitarian organisations for refugees is usually not accepted for [KYC](#)-purposes in most destination countries (USAID, 2017), e.g. due to diverging interests of refugee protection and governmental national security considerations (Jacobsen, 2017). For example, in above 120 countries, [MNOs](#) are subject to mandatory [SIM](#) registration obligations, requiring individuals to present official IDs before a [SIM](#) card and/or [mobile money](#) service can be activated. Identity documents issued by UNHCR or other nonstate actors are not accepted. In these circumstances, refugees must wait months, or even years, to obtain host-government-issued ID after being granted refugee status, to access services in their own name. In many of the world's top refugee-hosting countries, such as Kenya, this is currently the case (GSMA, 2017b).

<sup>32</sup> Creating a tiered-[KYC](#) system, with increasing customer [due diligence](#) requirements as volume, size and nature of the customers' payment transactions expand, can help to improve financial access. Examples of countries with varying approaches to tiered-[KYC](#) entail Mexico, Malawi, and India (Zimmerman, 2017).

<sup>33</sup> Unlike [closed-loop](#) systems, which, unless well-planned with a strategy to eventually integrate with or shift into open and shared payment systems channels, may be a diversion from the opportunities to leverage [DFS](#) for post-crisis response and resiliency building (Zimmerman et. al, 2016).

<sup>34</sup> Ideally, for improved [disaster](#) responsiveness, the inclusion of potential e-[CBA](#) recipients into the [open-loop](#) payment system takes place before a [disaster](#) occurs, incentivizing humanitarian ID uptake with a real, added-value for the potential human affected, e.g. by granting access to [mobile money](#), thus seems to be reasonable. According to Blake et. al (2016), pre-crisis preparedness includes facilitating private sector and humanitarian advocacy on key regulatory issues affecting humanitarian payments, including [KYC](#) and customer [due diligence](#) requirements.

So far, governments seem rather reluctant to do so<sup>35</sup> (GSMA, 2017b).

However, coming back to SQ iv, if a government was allowing to have a reduced [KYC](#) or even exemptions applicable to some un(der-) documented individuals deemed as “low risk”, there could be a potentially easier entry point for a humanitarian ID for satisfying [CDD](#) processes for [open-loop](#).

Hence, the question of long—term inclusion on the one hand, and the potential of using reduced [KYC](#) during a humanitarian response initially on the other, are investigated with that SQ.

*6.3.2.2. SQ vi) If so, can a (self-sovereign) digital ID yield open-loop inclusion as well?*

### **Motivation**

The abstract possibility specifically arising from an [SSI](#) utilizing [blockchain](#) - full [KYC](#)-compliance while maintaining pseudonymity, will be inquired. Therefore, answers to this SQ may reveal, whether minimised data not relatable to a specific individual are sufficient to align with official [AML/CTF](#) standards.

*6.3.2.3. SQ vii) Is providing a humanitarian, legal ID desirable in these contexts?*

### **Motivation**

While the research mostly asks questions about contextual feasibility, it also has vast ethical implications, especially given that providing this kind of multipurpose ID to individuals may go far beyond the common [mandate](#) of [humanitarian assistance](#) of providing relief as [disaster](#) response (Bailey and Harvey, 2015; Levin et. al, 2015; UN-OCHA, 2008).

As previous sections emphasized, there are a considerable number of factors potentially undermining a fully inclusive digital ID system utilizing [ICT](#). While the PEST-analysis performed for SQ i) most likely will reveal some of these relevant exclusion factors, the interviews are well positioned to validate and broaden acquired knowledge. Decades of, at least partially, failed development cooperation and tech-solutionism, urge to ask people affected and sovereign governments **before** deploying

---

<sup>35</sup> Beyond ID provision, potential solutions might entail creating specific humanitarian KYC standards, for e.g. refugee populations in collaboration with governments and international organizations, or ensuring that the humanitarian agencies, rather than the human affected, are treated as customers by service providers (Levin et. al, 2015).

a system aiming for sustainable development impacts and whether the system's alleged characteristics respond to the actual needs and demands "on the ground". Although people affected would accordingly be interviewed in the frame of this research, this was not deemed feasible, due to the remoteness of the research, scope, complexity, and time. To at least partially alleviate this, SQ vii) will be asked.

## 7. Desk Studies

### 7.1. Chapter Overview

The texts of the thesis summarize conducted desk studies. For the complete desk studies, refer to Appendix 5 and Appendix 6.

### 7.2. Desk Study Malawi - Summary

#### 7.2.1. Political, Economic, Social, Technological Environment

The political environment for [e-transfers](#) can be described as conducive.

Due to large scale efforts in 2017, Malawi went from an absent national ID system to (claimed) universal (digital) ID coverage with the help of [biometric](#) registration systems in 2017. Because of that, "bargaining power" concerning an alternative legal ID might be restricted. Claimed universal ID-coverage might however not reflect the reality, a substantial share of the population might still be un-documented. Furthermore, as the national ID seemingly is only issued to citizens, non-citizens might still suffer from e.g. financial exclusion. The national ID might exacerbate the problem for un-documented populations due to the (expected) upcoming stricter [KYC](#)-regulations (see below). If this sentiment is confirmed during the interviews, humanitarian agencies could thus consider supporting the national system to ensure that every inhabitant of Malawi, also those failing to provide officially recognized [credentials](#) (e.g. driving license, letter of chief), are included into the new ID-system. Identified public key informant is the National Registration Bureau.

[MNOs](#) provide most of the retail [DFS](#)-transactions. The dominant incumbents Airtel and Telekom Networks Malawi (TNM) provide mobile [open-loop](#) payment systems. Both are potential key informants. [Mobile banking](#), and thus, access to wider financial services, however, vastly lacks behind, especially in rural areas.

This is due to required social and technological factors might be insufficient to link mobile [wallets](#) to formal banking accounts.

These social and technological factors might further undermine inclusive humanitarian interventions utilizing some sort of [ICT](#). Amongst others, illiteracy, mistrust and lacking acceptance on the one hand, and low connectivity and a lack of electricity, [agent](#)/network coverage or mobile phone possession on the other, might pose considerable obstacles to reach [financial inclusion](#) with e-[CBA](#).

### 7.2.2. Law/Regulation

Before the national ID roll-out, ambiguous definitions in the regulations, the common practice of e.g. accepting chief-letters for [KYC](#) and tiered approaches not requiring official IDs, the need and bargaining power for a humanitarian, foundational ID could have been higher.

As the regulation seemingly still needs to tighten ID-requirements for [KYC](#), a potential entry point for deploying a foundational humanitarian ID could be given, though. This however would leave questions about the long-term sustainability of that approach, given the expected stricter regulations in the future.

Given claimed universality of the national ID, [KYC](#)-requirements are however expected to pose a negligible hindrance to financial inclusion/digital [CBA](#). Other above-mentioned exclusion-factors, such as illiteracy, seem to play a more dominant role.

Hence, while a humanitarian agency might “exploit” the currently still less strict regulations, advocating for the inclusion of non-citizens into the ID-system might therefore be another relevant working-area. Key-informant of the regulating bodies is the Reserve Bank of Malawi (RBM), as determinant of [agent-KYC](#).

### 7.2.3. International Humanitarian Organisations

Some humanitarian organisations have provided mobile-based [CBA](#), but potentially not on long-sustainable [open-loop](#) payment systems, and seemingly for the sole purpose of [disaster](#) response. How and what arrangements were reached based on humanitarian grounds, and whether [financial inclusion](#), especially of previously undocumented took place, remains unclear.

Refugees in Dzaleka camp however already seem to have access to formal banking services. They were able to register with a UNHCR-issued ID, upon governmental approval. As unlike in Kenya, the ID-system seems to be still more joint-led, this could

provide the pathway for a legally recognized [SSI](#) in Malawi. Which individual data had to be disclosed to the regulating bodies to yield [financial inclusion](#) of the refugees, remains open. UNHCR thus is regarded as key-informant from the humanitarian sphere, besides in e-[CBA](#) directly involved actors (Malawi Red Cross, WFP, USAID, Oxfam and Save the Children). The New Finance Bank, a unit of MyBucks, providing the banking services in Dzaleka Camp, is regarded as key-informant besides the others.

### 7.3. Desk Study Kenya - Summary

#### 7.3.1. Political, Economic, Social, Technological Environment

Highly conducive political, technological and private sector environment for [e-transfers](#). Lacking access to [DFS](#) is mostly attributed to insufficient income, absence of official IDs however plays an important role as well. Unlike in Malawi, lack of IDs is explicitly stated as reason of both individuals and humanitarian organisations for not utilizing [mobile money](#).

Despite current efforts to centralize current federated/semi-centralized ID system into one database, gaps are likely to remain, due to the [credential](#)-requirements of proving citizenship for obtaining the national ID. Supporting universal national ID coverage could thus be considered by humanitarian agencies.

The issuance of IDs for non-citizens furthermore has become increasingly restricted. Unlike in Malawi, an ID issued by UNHCR seems to be insufficient for digital/financial inclusion (see regulation below) nowadays.

Bargaining power for a foundational (humanitarian) ID alongside the governmental ID system might thus be restricted due to increased centralization efforts, and an increasing sole government-led approach towards refugee's and asylum seeker's ID [credentialization](#).

The governmental ID issuance efforts without complementing data protection policies call for an [SSI](#) following [PbD](#) principles, but might be undermined by the political economy demanding centralization of [PII](#), in form of [biometrics](#) etc. in one governmental database.

Socio-cultural and technological factors such as illiteracy connectivity seem to play a smaller role than in Malawi, yet still might pose considerable obstacles to inclusive e-[CBA](#) interventions.

### 7.3.2. Law/Regulation

Although Kenya was originally approaching [mobile money](#) with very light regulatory requirements, to align with the FATF<sup>36</sup> recommendations and linking mobile-[wallets](#) to banking accounts, [KYC](#)-standards now require an officially recognized ID document, from subscription to [SIM](#) cards to mobile-based [DFS](#). Accordingly, are un-documented citizens and non-citizens potentially financially and digitally excluded. Moreover, seem refugees and asylum seekers not holding the official governmental alien ID not be eligible for any mobile-based service.

In that sense, could the previously strong influence of mobile [DFS](#)-providers (specifically Safaricom) on according legislation be leveraged for future arrangements. Ideally, these agreements would not only be based on exemptions on humanitarian grounds. A humanitarian ID could then potentially provide long-term alleviation for both non- and citizens in terms of [KYC](#)-alignment.

However, the key service provider Safaricom seems to apply strict regulations for subscribing to a service, seemingly requiring IDs issued solely, or at least officially approved by the Kenyan government.

### 7.3.3. International Humanitarian Organisations

It remains ambiguous, whether humanitarian agencies were delivering [assistance](#) yielding long-term inclusion into an [open-loop](#) system so far, or whether the recipient's inclusion was given beforehand. How and what arrangements were reached based on humanitarian grounds, and whether [financial inclusion](#), especially of previously un-documented took place, remains unclear.

WFP is currently advocating for lower restrictions on delivering e-[CBA](#) to refugees. Their experiences, besides the vastly active UNHCR might hence be valuable.

---

<sup>36</sup> See glossary, term [KYC](#). Just as Malawi, Kenya is not a direct member of the FATF, but the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG), an associate member of the FATF (2019).

## 8. Semi-Structured Interviews

### 8.1. Chapter Overview

This chapter provides an overview about how the semi-structured interviews were set-up, prepared and conducted.

### 8.2. Initial Contact - Reaching out to potential respondents

#### 8.2.1. Institutional stakeholders in Malawi and Kenya

During the research, various relevant public, private, non-governmental and multilateral institutions as identified during the desk studies were reached out to. This included regulatory bodies directly involved in according [DFS](#)-regulation or broader [KYC](#)-regulation, or public bodies involved with the national identification system(s). Furthermore, were the relevant service providers (mostly based on their market-share), normally, [MNOs](#) and the identified international humanitarian agencies contacted.

Any institutional representative directly working in the contexts was approached officially over the channels of the Malawi Red Cross Society (MRCS), the Kenya Red Cross Society (KRCS), or the Netherlands Red Cross Society (NLRC). This mostly materialized in the initial contact over mail or phone being made by representatives of the relevant Red Cross Society. Most of the time, a formal cover letter, signed by the NLRC's 121-project & 510-initiative leader, a MRCS/KRCS representative, and this thesis' author, was attached to route the request. Appendix 9 displays an anonymized example of such a cover letter. A few times, after consultation with NLRC/MRCS/KRCS representatives, the initial contact was established over the author's NLRC mail account.

Figure 4: Contacted Institutional Stakeholders

Country	Kenya	Malawi
Institution		
<b>Public Identity Providers</b>	<ul style="list-style-type: none"> <li>- Ministry of Interior (general)</li> <li>- Refugee Affairs Secretariat</li> <li>- Department of Immigration Services</li> <li>- National Registration Bureau</li> <li>- Department of Civil Registration</li> </ul>	<ul style="list-style-type: none"> <li>- National Registration Bureau</li> </ul>
<b>Public KYC-regulators</b>	<ul style="list-style-type: none"> <li>- Central Bank of Kenya</li> <li>- Financial Intelligence Unit</li> </ul>	<ul style="list-style-type: none"> <li>- Reserve Bank Malawi</li> </ul>
<b>Service Providers</b>	<ul style="list-style-type: none"> <li>- Safaricom</li> </ul>	<ul style="list-style-type: none"> <li>- Telekom Network Malawi</li> <li>- Airtel</li> <li>- New Finance Bank</li> </ul>
<b>International Humanitarian Organisations</b>	<ul style="list-style-type: none"> <li>- UNHCR</li> <li>- WFP</li> <li>- IOM</li> </ul>	<ul style="list-style-type: none"> <li>- UNHCR</li> <li>- WFP</li> <li>- USAID</li> </ul>

### 8.2.2. Independent Experts

Given the complexity and novelty of technology and topic, and because previous relevant knowledge of contacted institutional stakeholders in the contexts could not necessarily be assumed, during the specific desk-studies and general literature identified “experts” on fragments of the topic were reached out to.

Thus, to enrich the thesis with a more general expertise of individuals thought of as possessing relevant technological, regulatory, contextual and humanitarian information relating to deploying an [SSI](#) striving for a more foundational purpose, the author contacted independent consultants, professors and institutional representatives not directly involved in the contexts. Appendix 10 provides an anonymized example of such an initial mail.

### 8.3. Developing the Interview Guidelines

Before and while reaching out to the potential respondents in both contexts, various interview-guidelines were developed, based on Galetta's (2012) suggestions and informed by the contextual desk-studies and the general literature around the topic. Figure 5 showcases the underlying motivation for developing the questionnaires for humanitarian agencies in Malawi. Appendix 7 and Appendix 8 provide all developed questionnaires for the institutional stakeholders in both contexts.

The interview guidelines for the independent experts were developed after a positive response indicating willingness to be interviewed, as based on the very specific area of expertise and previous work, this was deemed the only reasonable way. Broadly, SQ v-vii) were asked on a more general level and a lot of space was given to allow for respondent's elaboration.

Generally, the interview protocols were structured into three segments, aligning with Galetta (2012); the i) Opening Segment, ii) Middle Segment and iii) Concluding Segment, moving from more open-ended questions to more theoretical questions. Thus, while pursuing the open character of semi-structured interviews, considerable thought was given to the preparation of questions and their specific placement in the protocol, as semi-structured interviews can easily lead to abstract and off-topic answers (Galetta, 2012).

Figure 5: Showcased Interview Guidelines: Humanitarian Organisations in Malawi

<p><b>Opening Segment:</b> The questions in the first segment are suggested to be open-ended, creating space to the respondent to narrate her experience. While this elicits data which cannot be anticipated, the focus of the questions should still be carefully tied to the research (Galetta, 2012). Meaningful junctures in the interviewee’s narrative should be returned to later during the interview for increased in-depth exploration. Galetta (2012) describes the opening segment as the richest source of data, and the narrative of the participant is in place before more theoretically shaped questions are asked. As the interview progresses, the researcher is increasingly engaged in meaning-making with the participants.</p>	
<p>1) Which kind of marginalisation can you think of apply to your target groups posing obstacles to receiving electronic <a href="#">cash-based assistance</a>?</p>	
<p><b>Motivation</b> Informs about and confirms potential obstacles for inclusive <a href="#">ICT</a> deployment. Serves as open question to enter the interview and explore level of participant’s experience. Further set to establish a level of trust as demanded by Galetta (2012), by showing awareness about a too rigid “tech-solutionist” approach to <a href="#">humanitarian assistance</a> potentially undermining inclusivity.</p>	<p><b>Literature</b></p> <ul style="list-style-type: none"> <li>- Illiteracy, especially in rural areas</li> <li>- Transaction charges potentially inadequate to the poor</li> <li>- Poor or no connectivity, lack of electricity</li> <li>- Low <a href="#">agent</a> liquidity and accessibility, especially in rural areas</li> <li>- Mistrust/lack of acceptance</li> <li>- Refugee Status (ID?)</li> </ul>
<p>2) Your organisation utilizes/utilized some kind of <a href="#">e-transfer</a> during a humanitarian crisis.</p>	
<p>a. Which <a href="#">e-transfer</a> exactly?</p>	
<p><b>Motivation</b> Confirms literature and guides interview into direction of question 2b-f. Assumingly, the question will be already answered during question 1, if the respondent relates her experience to her agency’s interventions.</p>	<p><b>Literature</b> Bank cards, <a href="#">mobile vouchers</a>, and MRCS used <a href="#">mobile money</a> (Airtel).</p>
<p>b. What were your experiences with the <a href="#">mechanism</a> (in terms of PA satisfaction, efficiency increases etc.)?</p>	
<p><b>Motivation</b> Supposed to implicitly investigate Q. 1 from a different angle and prepare for Q. 2d-f.</p>	<p><b>Literature</b> Mixed results, especially for the earlier interventions, where <a href="#">e-transfers</a> seem to have been a rather sub-optimal approach.</p>
<p>c. Which intermediaries do/did you (have to) involve in the process?</p>	
<p><b>Motivation</b> Check for relevant service providers and prepares for question 2d.</p>	<p><b>Literature</b> Airtel, TNM, OIBM, and G4S Security.</p>
<p>d. Do you have the perception that the requirements of the involved service provider conflict with your <a href="#">mandate</a> as humanitarian organisation in any way? What exactly?</p>	

<p><b>Motivation</b> Prepares for Q. 6 by asserting, for example, special data protection needs. Check for further requirements a humanitarian-supported <a href="#">digital ID</a> would need to entail besides <a href="#">KYC</a>-satisfaction.</p>	<p><b>Literature</b> Not clear for particularly Malawi.</p>
<p>e. <i>Did your organisation reach a special agreement with regulators/service providers, is/was there a simplified/exemption to <a href="#">KYC</a>-standards applicable to your organisation and/or target group when using the <a href="#">e-transfer</a>?</i></p>	
<p><b>Motivation</b> Check and confirm tiered <a href="#">KYC</a> and/or exemptions applicable to humanitarian agencies. Prepares for Middle Segment and relates back to Q. 2c-d.</p>	<p><b>Literature</b> Malawi Red Cross did so with Airtel. Both <a href="#">MNOs</a> (Airtel&amp;TNM) seem to have (had) tiered approaches to un(der)-documented.</p>
<p><b>If Yes:</b></p> <ul style="list-style-type: none"> <li>- How did you reach it, and with whom (regulators/service providers)?</li> <li>- Which restrictions to the sending entity and receiving individual arise from the tired approach (e.g. <a href="#">closed-loop</a>)?</li> </ul>	<p><b>If No:</b></p> <ul style="list-style-type: none"> <li>- Do you think, it would be feasible to reach an agreement with regulators/service providers in the future?</li> <li>- How could such an agreement be reached and operationalized?</li> </ul>
<p>f. <i>Does/did the <a href="#">e-transfer mechanism</a>(s) therefore enable PA to store, receive and send cash during and beyond the humanitarian intervention?</i></p>	
<p><b>Motivation</b> Is utilizing an <a href="#">open-loop</a> payment system for <a href="#">humanitarian assistance</a> currently formally possible in the context, even for un-documented?</p>	<p><b>Literature</b> Not true for documented interventions. Due to <a href="#">financial inclusion</a> claim in Dzaleka camp, this could have recently changed.</p>
<p><b>If Yes:</b></p> <ul style="list-style-type: none"> <li>- How did align with <a href="#">KYC</a>-standards in case of un-documented (Q. 2e)?</li> <li>- Do you have robust data of increased <a href="#">financial inclusion</a> effects?</li> </ul>	<p><b>If No:</b></p> <ul style="list-style-type: none"> <li>- Is/was <a href="#">KYC</a> a reason, for example due to lack of official ID?</li> </ul>
<p>3) <i>Due to the substantive roll-out of the new national ID system since 2017, do you think future humanitarian interventions now can increasingly make use of payment systems such as <a href="#">mobile money</a>? Further, are you aware of any upcoming (<a href="#">KYC</a>-)regulations potentially impacting the choice of transfer <a href="#">modality</a> and <a href="#">mechanism</a>?</i></p>	
<p><b>Motivation</b> Accounting for the suspicion, that the new national ID on the one hand makes it easier to be <a href="#">financially included</a> for everyone who has it, and more difficult for everyone who does not. Wraps up questions 1 and 2 and leads towards Middle Segment.</p>	<p><b>Literature</b> First reports are enthusiastic about the new potentials for <a href="#">financial inclusion</a> arising due to the new ID system. No critical voices or concerns about some groups potentially being excluded were found so far.</p>

**Middle Segment:** In the Middle Segment, while drawing from the Opening Segment’s findings, questions of increased specificity should be asked (Galetta, 2012). After the broader questions of the first segment, questions of increased specificity can be more informed now as the participant has talked about her experience relating to the research topic. Hence, questions in the Middle Segment are now specifically tied to Sub-Questions v) to vii), after some degree of trust has been established between interviewer and the participant and some reciprocity has been attained.

4) *Some of the agencies’ target groups might not be eligible to receive a national ID. A currently discussed approach would be issuing [digital identities](#) as humanitarian agency, ideally not only supporting humanitarian [CBA](#)-delivery, but also enabling the recipient to access wider, public services. For example, financial services due to [KYC](#)-alignment, beyond the time-frame of a humanitarian intervention. Do you think, that this would be possible, e.g. if the humanitarian agency formally collects the required [KYC](#)-information?*

<p><b>Motivation</b> Would a regulating body/service provider generally accept a humanitarian ID sufficiently for e.g. long-term <a href="#">KYC</a>-alignment (SQ v)?</p>	<p><b>Literature</b> Assumingly, the refugees in Dzaleka camp are able to access financial services with a UNHCR-issued ID. This needs to be confirmed.</p>
--	---

5) *In some circumstances, when government-officials are absent, for example in a refugee camp, it might make sense that the registration and verification process for that kind of ID is solely supported by a humanitarian agency active in the community. Would that be possible?*

<p><b>Motivation</b> Can solely a humanitarian agency assert and verify identity claims (SQ v)?</p>	<p><b>Literature</b> Not clear.</p>
---	---

6) *Ideally, the [digital ID](#) would prevent in-consensual disclosure of (individualized) data, giving PA the ability to self-sovereignly manage which [PII](#) are disclosed to whom. Relating to [KYC](#), that could mean, that service providers would not necessarily be able to access [PII](#) during authentication for a service, a conflict to the traditional [KYC](#)-standards in Malawi. Rather, a service provider or regulating body would need to trust that the prior registration and verification of an individual by e.g. a humanitarian organisation was trustworthy enough. Do you think that is possible in Malawi?*

<p><b>Motivation</b> Could a <a href="#">SSI</a>, following <a href="#">privacy-by-design</a> principles, serve as sufficient ID for un-documented for long-term <a href="#">KYC</a>-alignment (SQ vi)?</p>	<p><b>Literature</b> Not researched.</p>
---	--

**Concluding Segment:** During the final segment, the opening narrative is revised, and important theoretical connections should be performed. Eventually, reaching closure should be aimed for (Galetta, 2012). The final segment thus offers an opportunity to return to points in the interviewee’s narrative which are still in need of exploration. Hence, the protocol should be designed with space in which ideas earlier expressed by the participant can be connected back to. In this way, the data that are grounded in lived experience and those addressing theory might converse. The movement from the first segments open questions to more in-depth/theoretical questions in the last segment illustrates the diversity available to this research method.

7) *After everything we have discussed so far, would you think it is desirable to deploy a humanitarian ID serving more foundational purposes? (SQ vii)*

8) *Do you have any final thoughts or recommendations for further research you want to add?*

## 8.4. After the Initial Contact

### 8.4.1. General

After the initial contact was established, more information on the research and underlying questions were provided (normally in the form of a research abstract), room was given to ask additional questions. If potential respondents signalled an interest to be part of the research, a time for conducting the interview was set up, a letter of informed consent (anonymized example in Appendix 12) was sent to be signed before the interview. Additionally, the letter's contents – the rights of the interviewee – were summarized in an additional mail.

### 8.4.2. Reactions of potential Respondents

Even with the Red Cross Societies as supporting “backers” of the research, establishing interviews with institutional representatives in the contexts proved to be very difficult, while on the other hand, independent experts oftentimes were more than eager to be part of the research. A common experience was, that institutional representatives, normally replying to the initial mail, were not eager to have an interview, after the underlying research and its questions were subsequently laid out in detail. Although one can only assume underlying reasons (besides a lack of interest and more urgent pressures at work), some potential explanations will be briefly mentioned in the “limitations” sub-section after the analysis.

### 8.4.3. List of Respondents

Figure 6 provides the list of respondents.<sup>37</sup>

---

<sup>37</sup> Note that positions of the respondents in figure 6 are depicted in simplified form and mostly are not legitimately representing the vast expertise of the respondents. For a more detailed description, refer to individual interviews in Appendix 11.

Figure 6: List of Respondents

Context	Name	Current Position
Malawi	Wonderful Kunje	Data Analyst at MRCS
Malawi & General	Rajesh Bansal	Regional Director - Bankable Frontiers Association
Kenya	Anonymous	Project Leader at anonym. humanitarian agency
Kenya & General	Anna Kondakhchyan	ICT & DFS Adviser at Oxfam
General, Malawi & Kenya	Raul Zambrano	International Development Consultant
General	Kokoévi Sossouvi	Independent Consultant on DFS & CBA
General	Prof. Avner Levin	Professor of Law
General	Vincent Graf Narbel	ICT Adviser at International Committee of the Red Cross

Unfortunately, although more interviews could have been conducted with several potential respondents indicating interest and willingness to share their insights, due to limited scope and time of the research, conducting further interviews had to be halted at some point.

### 8.5. Conducting the Interviews

Before the interviews, purpose and content of the research were outlined and the opportunity to ask additional questions was given. Most of the time, aligning with Galetta (2012) and this thesis' regulations, the letter of informed consent was signed before the interview took place. However, some respondents preferred to give their consent in oral form during the interview and then signed the letter after having received the written version of the summary and complete interview. All but one interview were conducted via Skype, one was conducted over Zoom. At every start of

an interview, aligning with Galetta (2012), was gratitude for the interviewee's participation expressed and purpose and content of the research repeated. The some core characteristics of a potential ID system were presented, space given to ask additional questions.

Furthermore, every was interviewee orally reminded of her or his rights as outlined in the letter of informed consent. Even if consent to record the interview for transcription purposes was given by signing the letter of informed consent beforehand, were interviewees explicitly asked to consent again before the recording was started. This led to a situation, where the interviewer felt one respondent not being overly comfortable with recording the interview, although having signed the letter of informed consent beforehand, yielding the decision to not record the interview after all.

Following Galetta (2012), during all interviews, tried the interviewer to adapt his language and format of the questions to the individual respondent, her or his position, experience and willingness to dedicate a certain amount of time to the interview. Furthermore, to ensure accuracy of interpretation and understanding of the interviewer, but also to give space for interviewees' elaboration, did the interviewer engage in clarification as much as possible. Every interview yielded considerable, multi-dimensional streams of data.

At the end of each interview, the interviewees were again reminded of their rights as laid out in the letter of informed consent and gratitude was expressed again.

All interviews were then transcribed (if consent for recording was given), summarized and sent to the respondents for (dis-)approval. The approved summaries and complete versions (if consent was given for the full versions, in two cases, that was not the case due to different reasons) displayed in Appendix 11 and 12 are subsequently analysed.

## 8.6. Pre-liminary Analysis

The summarized versions of the interview provided a first structure, pre-liminary analysis and meaning-making. The summarized and complete versions were subsequently sent to the respondents. This was done to ensure, that the pre-liminary meaning-making was adequately performed. The respondents' inputs and feedback were then structured according to the last three SQs, yielding the analysis below.

## 9. Analysis

### 9.1. Chapter Overview

This chapter provides the analysis of conducted semi-structured interviews, structured after the final three SQs and further adds some thoughts retrieved from previous literature.

### 9.2. Could a humanitarian-backed ID satisfy KYC-requirements to yield inclusion into open-loop mobile DFS?

#### 9.2.1. Verification of asserted Identity Claims

There is a common agreement among respondents tackling that issue, that identity claims need to be verified by some authoritative entity for yielding a legal foundation, aligning with the previously consulted literature.

While not neglecting the potential of initially self-asserting claims and needs on a [mechanism](#) utilizing [SSI](#), people affected hence would normally still be dependent on external verification for a legally compliant ID.

Therefore, some entity needs to ultimately hold the “truth” (Kondakhchyan) about claims made, even in a network of “distributed trust” (Graf), where, for example, some nodes would need to serve as verifiers.

Anonymous provides, implicitly aligning with Graf’s mention of several nodes serving as verifiers, a vision of a decentralized, interoperable system, in which certain standards and a code of conduct would apply to various humanitarian and civil society actors being authorized to include individuals into an identity system. A verification of an individual’s claims could be performed by several actors, before [identity credentials](#) are issued. This approach would thus not entail having a certain singular humanitarian agency being the sole executioner of an [identity](#).

Finally, a [blockchain](#)-enabled [digital identity](#) could achieve an environment support the decentralization of a certain self-assurance the way recipients represent and reveal themselves digitally, while some trusted external authority does not provide the identity information per se, but rather act as verifiers of the claims asserted by the individual (GSMA, 2018).

In Kenya, however, confirming the literature, Kondakhchyan states, that the government is restrictive in supporting the UNHCR-mandated refugee card to access

wider services beyond the camp-context, or merely allowing for out-of-camp mobility. The government thus might not necessarily aspire towards having refugee populations included into a system warranting access to wider services, potentially incentivizing further refugee influxes (Kondakhchyan), bypassing the government with fluid borders (Anonymous).

Thus, while one would most likely not need to include the government for in-camp-services, for out-of-camp services, it assumingly would (Kondakhchyan).

In Malawi, the case is less clear. Kunje, Bansal and Zambrano however provide some indications, that the government likely must be included in verifying identity claims for legal purposes as well.

Coming back to the literature, the question about sole humanitarian issuance of legal IDs fundamentally is about more than trust, it is about the sovereignty of a nation in politically determining, who can provide legal IDs and to whom.

Zambrano and Kondakhchyan eventually do not see it as feasible to have solely humanitarian organisations verifying of identity claims for a foundational purpose.

Altogether, this would imply a political economy against a humanitarian ID fulfilling a more foundational purpose nationwide - to at least some target groups.

## 9.2.2. Producing KYC-compliant ID credentials

### 9.2.2.1. Service Providers' Discretion

Does that conclusively mean, that humanitarian IDs could generally not permit access to more than [humanitarian assistance](#) out of the camp-context? Not necessarily.

Levin reaffirms that [KYC](#) regulates entities and not individuals. If a service provider would see [ML/TF](#) risks as adequately reduced, it could, depending on a case-to-case basis, eagerly accept a new form of identity as sufficient. Moreover, a humanitarian ID could include the same [identity](#) claims as an ID from a government (Levin).

For Kenya, Anonymous accordingly expresses optimism, that un(der-)documented might be included into Kenya's [M-Pesa](#) in the future, as according [MNO](#) was not strictly obliged by law to solely accept the national ID for [KYC](#)-compliance.<sup>38</sup> Hence, while not

---

<sup>38</sup> This aligns with the more recent regulation as investigated in the desk study for Kenya in Appendix 6, however not so much with IDs coming from the non-public sector.

necessarily politically desired, the law leaving space for some service provider's discretion could be leveraged as entry point for a more foundational humanitarian ID.

In the case of *Malawi*, as Levin indicates, based on the overall developmental status of the nation, the regulatory and political environment might be (even) more flexible concerning the question of *KYC*-compliance when compared to *Kenya*. This aligns with consulted literature (Appendix 5). Bansal correspondingly states, that *KYC*-regulation would still lag behind the national efforts to centralize previously more fragmented ID system.<sup>39</sup>

Kunje analogously implies, that accessing wider public services is still possible without national ID. Furthermore, could service providers accept a non-governmental digital ID for *KYC*-alignment, if sufficiently economically incentivized.

Conclusively, both contexts could potentially allow for a humanitarian ID implicitly serving broader functions, depending on successful advocacy of the humanitarian entity towards the relevant service providers.

In that sense, are both Kondakhchyan and Graf emphasize on the potentially good relationships and name Red Cross Societies have established in certain contexts.

#### *9.2.2.2. Reduced individual CDD as potential entry-point*

On the other hand, for *Kenya*, Anonymous states reaching *financial inclusion* by the service provider formally accepting a humanitarian ID is currently not possible.<sup>40</sup> While the humanitarian agency she or he is working for was able to reach an agreement to issue *SIM*-cards without the need to undergo full individual *CDD*, for accessing the *M-Pesa* system, people affected currently still need to provide governmental *ID credentials*.<sup>41</sup> Although people affected circumvent this regulation by e.g. sharing accounts (Anonymous), this obviously is not a sustainable, legally compliant solution.

However, as Levin, Sossouvi and Graf and point out to warrying extends, confirming the literature, humanitarian organisations generally achieve reduced *KYC* for recipients during, or in immediate recovery phases of a disaster.

---

<sup>39</sup> This aligns with according desk study.

<sup>40</sup> This aligns with conducted desk-study (Appendix 6).

<sup>41</sup> This aligns with conducted desk-study (Appendix 6).

This is generally because humanitarian transfers tend to be of relatively low value (Sossouvui) and the source of funds are known (Levin).

For Kenya, in Anonymous' eyes, a practicable approach for now hence would be to negotiate exemptions directly with the [MNO](#) of interest, based on humanitarian grounds. As the [MNO](#) was currently less accepting to use its discretion for a humanitarian ID formally complying with individual [CDD](#), this could prove to be a currently more feasible approach.

The humanitarian organisation could “absorb” the [KYC](#)-requirements of the individuals and thus be held accountable for potential adverse effects occurring due to people affected formally not undergoing full [CDD](#).

This however would mean, that a humanitarian ID would not be formally accepted by the service provider to satisfy individual [CDD](#)-obligations (Anonymous).

Rather, the humanitarian agency would take over the risks, either by restricting the [mechanism's](#) capabilities (Sossouvi, Levin), or by convincingly ensuring the internal humanitarian data management is good enough to reduce fraud etc. (Anonymous).

The first possibility, imposing restrictions, would more likely yield a [closed-loop](#) system. The latter possibility would potentially be more appealing if one wanted to deploy a humanitarian [SSI](#) functionally, while still serving a more foundational purpose.

This, again, would be dependent on the amount of trust an agency has established to absorb the risks accordingly (Anonymous).

Finally, if a service provider's discretion in determining which IDs are adequate for conducting [CDD](#) was not utilized accordingly, the common risk-based approaches humanitarian agencies can lobby for during a disaster could serve as an entry-point for humanitarian ID, then (at least implicitly) serving a more foundational purpose in relation to [KYC](#).

#### *9.2.2.3. Permanently reduced KYC-obligations*

As previously mentioned, “risk-based” approaches are common for humanitarian organisations – an agency establishing the business relationship (partially) taking over individual [CDD](#)-requirements and risks.

Levin and Kondakhchyan however state, that they are not aware of a context, in which simplified KYC would be permanently applicable. Using reduced requirements for the

long-term [financial inclusion](#) of recipients of [humanitarian assistance](#) then could prove as infeasible.<sup>42</sup>

Sossouvi, however, challenging above statement from Kondakhchyan and Levin, asserts, that normally, if the humanitarian agency was holding the business relationship, e.g. a mobile [wallet](#) with reduced [KYC](#), could become permanent. For that however, it must be actively used beyond the humanitarian intervention by its holder.

This implies the opportunity for some sort of long-term [financial inclusion](#) into an at least [closed-loop](#) or mixed system, even without individuals possessing a public ID.

Generally, though, according to Levin, in the long-run, the full [KYC](#) must be complied with. Compelling arguments for a simplified [KYC](#) thus would rather focus around a potential lack in identity infrastructure and the temporary urgency arising from a crisis. Tentatively, exemptions however could reasonably be lobbied for - e.g. in a refugee camp, where people might be dependent on a reduced [KYC](#) to access services on a longer-term basis - thus only for in-camp services.

Ideally, this would have been confirmed in the context of [Malawi](#) by interviewing UNHCR or the New Finance Bank providing banking services in Dzaleka camp, this was however not possible.

Finally, it remains ambiguous, whether reduced [KYC](#) and risk-absorption based on humanitarian grounds would present sustainable approaches to reach long-term [financial inclusion](#) beyond a humanitarian intervention, especially into an [open-loop](#) system - usually, as stated, demanding full individual [KYC](#)-compliance.

Furthermore, it remains open, whether one can circumvent political decisions who e.g. can be financially included and who not in a given context, by solely approaching the service providers and not the public sector.

Conclusively, this could mean, that in both contexts, yielding formal acceptance for individual [CDD](#)-satisfaction beyond the humanitarian scope, and thus a formal legal status for each individual ID, would only happen with the government's involvement.

---

<sup>42</sup> The possibility of using an accretionary model together with a reduced [KYC](#) as potential entry point for full [KYC](#)-compliance in the future was not fully asserted.

### 9.3. Can a Self-Sovereign Identity yield open-loop inclusion?

#### 9.3.1. Governmental Approval

The issue of potential governmental resistance towards solely humanitarian agencies performing identity claim-verification for legal purposes is also reflected in the likelihood of an [SSI](#) serving broader foundational purposes, if deployed by a non-governmental sector.

Most respondents hence do not regard it as likely to generally achieve legal, nationwide recognition of an [SSI](#) without the involvement and/or adoption of/by the government (Levin, Kondakhchyan, Sossouvi, Zambrano, Bansal, Anonymous, Graf). Vice versa, if a government would feel its sovereignty undermined, it could act adversely (Anonymous, Bansal, Kondakhchyan, Levin, Sossouvi).

Consequently, there a strong opinion against setting up parallel structures circumventing the public ones (Sossouvi, Bansal, Zambrano, Kondakhchyan, Levin).

For example, in [Malawi](#), as Bansal stresses, due the vast effort and spending for rolling-out the national ID, providing an [SSI](#) striving for a more foundational purpose as humanitarian agency would most likely be considered as duplication-effort.

And in [Kenya](#), not involving the government would be “inherently unsustainable” (Anonymous).

Governmental acceptance is thus considered as core hindrance (Bansal).

Accordingly, Sossouvi states, that the client for a **foundational** SSI should not be the humanitarian sector, but the government.

Thus, if a nation-wide, formally legal purpose was to be achieved, it potentially requires formal governmental approval or adoption.

#### 9.3.2. Convincing decision makers

The complexity and abstractness of both technology and concept however pose a considerable obstacle to provide a compelling argument, potentially making decision makers resistant to adoption, whether it is humanitarian agencies (Anonymous), governments, or service providers (Levin).

Graf, Levin and Zambrano hence accentuate the issue of explaining decision makers the alleged advantages in a tangible way, and Anonymous informs about the current

infeasibility to engage decision makers with the concept of an [SSI](#) in Kenya. A similar problem could be faced in [Malawi](#) (Zambrano).

As example in that sense, Levin states, confirming the literature, that encryption-techniques disguising the [identity](#) of an individual are conflicting traditional [AML/CTF](#) standards.

As the technology however could provide added value from an accounting perspective, Levin suggests an institution (public/private) could be accepting, once the ability to track transactions, without necessarily retrieving [PII](#), was sufficiently comprehended.

And according to Sossouvi, if a government would see an added value to its national structures when utilizing a more sophisticated ([SSI](#)-)system, it would be keen on implementing it. National states would have a vested interest in having all its citizens adequately identified, for e.g. efficient taxation.

Moreover, Anonymous points out, that decision-makers do not necessarily need to fully understand all underlying technology – if they can see and understand it works well (or better).

### 9.3.3. Creating a use-case

What does that mean for a humanitarian agency intending to deploy a more than functional [SSI](#)?

After Zambrano, there could be a possibility of trying to entice a desired change on the national level, with a pilot proving the alleged advantages of an [SSI](#) vis-à-vis to the incumbent national identity management systems.

Similarly, Anonymous, Bansal, Graf, Kondakhchyan, Levin and Zambrano touch upon the possibility of piloting for building a use-case to varying degrees, also both Kenya (Anonymous, Kondakhchyan) and [Malawi](#) (Bansal, Zambrano) specifically.

Finally, after Levin, a successful use-case in the humanitarian sphere, a “controlled experiment”, e.g. in one camp, could represent the first marginal step for scaling-up a pilot.

This would imply the importance of firstly implementing a successful pilot, before a broader adoption and formal legal character can be aimed for.

Being a proven path-way for innovation, picking the example of Kenya's M-Pesa, Kondakhchyan points out, that [M-Pesa](#) similarly would have been able to grow. However, engaging in discussions with the regulators as soon as possible would be indispensable for that.

A lot of initial "closed-door discussions" between [MNO](#) Safaricom, donors and the government would have created an accommodating regulatory space, allowing for the regulator to "step-back" and letting innovation thrive.

This could similarly apply to [SSI](#), given according high-level discussions.

#### 9.3.4. Functional deployment as initial step

Most respondents see challenges in deploying a system fulfilling foundational tasks running parallel to the public identity systems, as indicated before.

This could mean, that a pilot trying to show-case advantages coming from the humanitarian sphere will most likely firstly be used as functional ID system (Anonymous, Graf, Kondakhchyan). An [SSI](#) could still firstly be deployed as a functional ID, primarily pursuing the aim of improving internal humanitarian data management, while implicitly aspiring for a foundational character as implicit, secondary goal (Anonymous, Graf).

This would align with USAID (2017), stating that some foundational ID systems start off as solely functional.

Coming back to mentioned risk-based approaches, a humanitarian agency hence could use an [SSI](#) for "internally" absorbing individual [ML/TF](#) risks for the service provider (Anonymous).

Assumingly, this could already provide some of the functions of a [financially inclusive](#) system, however in the frame of providing [humanitarian assistance](#), again, leaving some ambiguity about the long-term sustainability of this approach.

This would also mean, that an [SSI](#) deployed by a humanitarian agency most likely will not immediately formally satisfy open-loop [KYC](#), as being dependent on initially unlikely governmental approval. However, given a strong-use case, as explained above, this formal acceptance could follow at some point.

Furthermore, providing a long-term plan for scaling-up, might make the regulator more accepting (Kondakhchyan).

### 9.3.5. Scaling up

The process of scaling-up from the pilot, then striving for a formal foundational purpose, would be, after Anonymous, two-folded.

For Kenya, firstly, the humanitarian agencies would need to use the system amongst each other.

Anonymous however emphasizes, that incrementally increasing adoption would most likely not occur based on the “ideals” an [SSI](#) follows, such as enhanced data ownership and control to the individual.

Anonymous, Bansal, Graf, Kondakhchyan, Levin, Sossouvi and Zambrano explicitly or implicitly state, that an [SSI](#) would need to satisfy conventional decision-maker metrics, such as increases in efficiency, transparency, accountability and a reduction of fraud and duplication for a successful use-case in the first place.

Kondakhchyan accordingly states the potential of improving [humanitarian assistance](#) delivery with a functional [SSI](#), by making it more interoperable, efficient and preventing the current functional systems’ fragmentation.

Then, after Anonymous, if enough humanitarian agencies would back the system, the regulating bodies could accept the ID system for formal [KYC](#)-compliance, based on its former inner-sectoral wide-spread adoption. To lesser extends, this sentiment is furthermore confirmed by Graf.

### 9.3.6. Interoperability with public systems

Incrementally pushing a wider adoption of the system, besides providing enhanced decision-maker metrics, demands a further crucial aspect: interoperability.<sup>43</sup>

The need for interoperability was brought up by all respondents to varying extends.

Public adoption of an [SSI](#) would need to include (Anonymous, Graf), but also go beyond inner-sectoral interoperability. As with infrastructural approaches in literature (USAID, 2017), the need was expressed for creating an interoperable system linking well to the public ones (Kondakhchyan, Sossouvi, Zambrano).

---

<sup>43</sup> Aligning with the adherence of an [SSI](#) (see glossary); as well as [open-loop](#) systems (Lepoutre and Oguntoye, 2018, Buckley et. al, 2015).

For Malawi, Kunje suggested, that interoperability between the national ID and a potential digital ID would also support MRCS's interventions.

Graf and Zambrano in that sense emphasize the need for contextual adaptation, as do Bansal in the specific case of Malawi, having local regulations in mind, and Kondakhchyan in the case of Kenya, concerning [user-centricity](#).

However, Graf points out, contextual adaption and dependency on case-to-case governmental approval might make standardization difficult. For example, a government could decide to ban a certain [SSI](#) at some point (Anonymous, Graf), or some communities could have a strong notion of a proxy gathering [humanitarian assistance](#) (Anonymous, Kunje, Graf), for example, a grandchild or other relative retrieving value.

Nonetheless, if interoperability was achieved, Kondakhchyan brings up the possibility of an interoperable [SSI](#) coexisting besides a governmental system, then possibly serving as vehicle for some foundational functions. In that sense, Zambrano brings up the example of a Red Cross ID for both Red Cross giving private medicines and accessing doctors provided by the government.

This coexistence thus would not mean, that governmental systems were to be replaced, but rather that the [SSI](#) would be trusted by e.g. service providers because of its linkage to the foundational public system (Kondakhchyan). This would assumingly imply, that an interoperable [SSI](#) would need to be backed by a foundational public ID.

### 9.3.7. Technical teething problems

As indicated in previous sections, [blockchain](#)-technology and the concept of [SSI](#) are not fully matured yet.

Zambrano, clearly states, aligning with Graf, Kondakhchyan and Levin that the technology itself is not "there yet" to reach sufficient scale. In that sense, mentions Zambrano the US-state Illinois, which piloted an [SSI](#), but lost interest because of technological scalability-issues – an environment which would be better positioned to

implement a scaled [SSI](#)-project than, for example, Malawi. Similarly, would the ID2020 initiative have dropped interest on [blockchain](#)-based [SSI](#) due to scalability issues.<sup>44</sup>

Although Graf and Zambrano envision that future technological developments could alleviate that problem, this technical issue underscores the need to show-case alleged advantages without yet necessarily having the technology at a stage being able to do so.

Accordingly, aligning with the other points above, a small-scale, functional [SSI](#)-pilot seems to be a more optimal pathway for now.

#### 9.4. Is providing a humanitarian, foundational ID desirable in these contexts?

##### 9.4.1. Filling the gap

Generally, besides various practical challenges for an [SSI](#) striving for a foundational purpose, most respondents expressed ethical concerns. This commonly resulted in the interviewee's asking various critical questions about the [digital ID system](#) and its aims before the recorded part of the interviews took place. One respondent only agreed to be recorded after over 20 minutes into the actual interview, after a certain level of trust and confidence was established, that this research's purpose was not unethical.

Most of the respondent's concerns revolved around the assumption, that the [digital ID-system](#) of concern could aim to replace or fill the gap of governmental systems. As previous sections already discussed, there is a strong opinion against undermining and weakening public structures by circumventing them (Sossouvi, Bansal, Zambrano, Kondakhchyan, Levin). Providing foundational [identity](#) infrastructures hence is generally seen as task of the public sector, not as of humanitarians.

A humanitarian agency thus must carefully balance between aiming to support longer-term development and replacing public tasks. Aiming at providing more foundational ID infrastructures to recipients of [humanitarian assistance](#) therefore might require a difficult trade-off to be considered.

---

<sup>44</sup> To the author's current knowledge, ID2020 is still investigating [SSI](#), but steering away from planning with public permission-less chains. As Stevens (2018) suggests, using public-permissioned chains could counteract scalability issues (while this might very well undermine an "ideal" [SSI](#)).

#### 9.4.2. Humanitarian Development Nexus

As should be clear by now, deploying an [SSI](#) as humanitarian agency with an, whether implicit or explicit, aim for a foundational character for longer-lasting development impacts, falls into a discussion about linking short-term [humanitarian assistance](#) with longer-term development goals.

Ideally, this would be the norm with humanitarian interventions (Sossouvi, Zambrano).

After Zambrano, connecting [humanitarian assistance](#) to longer-term, more sustainable development would require factoring in three basic principles:

- i) community ownership,
- ii) a participatory approach during or before the humanitarian intervention
- iii) a demand-driven need

Otherwise, after Zambrano, a sustainable utilization of the system is not given.

This means, in the context of Malawi and Kenya, but also on a more general level, that there would need to be

- i) a design allowing for maintenance, governance and inclusive utilization of the system without being dependent on external expertise in the long-term,
- ii) a bottom-up approach for the local appropriation of the system
- iii) a demand for specifically an [SSI](#) or some of its functions

These three principles may serve as a preliminary frame for some further ethical considerations.

##### 9.4.2.1. *Community Ownership & Challenges to Inclusivity*

As the desk studies' PESTLI-analyses already indicated, there are currently wide challenges for deploying the system in a fully inclusive way, if utilizing [ICT](#). Furthermore, the complexity and technical immaturity of [SSI](#), might make a sustainable, community-owned utilization of the technology questionable after a humanitarian intervention has ended (Zambrano).

Graf explicitly states, that "going digital" should not happen, if a large share of the target group cannot access the system.

In [Malawi](#), Kunje and Zambrano accordingly identify (digital) connectivity as key obstacle for a [digital ID](#), especially in rural areas. According to Kunje, even solely using

[mobile money](#) as delivery [mechanism](#) is currently not considered as practical, the MRCS would accordingly still distribute cash in envelopes. Recipients otherwise would need to travel long distances to obtain connectivity, yielding a considerable reduction of the value retrieved from [CBA](#).

Kunje and Zambrano also mention the issue of illiteracy. Kunje specifically talks about [authenticator](#) loss/forgetting the [PIN](#). Kunje thus expresses the associated delays due to [authenticator](#) recovery as highly problematic, especially when immediate relief is important. Building up on that, Zambrano mentions the potential complexity of key-recovery particularly for identity systems utilizing [blockchain](#) technology.

Kunje further suggests, that capacities of [digital ID](#) holders would need to be increased, before a successful deployment could take place. Zambrano extends the need for capacity-building to the government; Graf extends it to the employees of a given humanitarian agency.

For Kenya, Anonymous considers digital connectivity and the concept of receiving something digital, due to the wide penetration of [M-Pesa](#), as quite well understood.

Kondakhchyan, however, also points out alphabetical and technological illiteracy as main obstacle, if the [SSI](#) was not highly user-centric. As with [M-Pesa](#) (Anonymous), illiterate people affected would otherwise need to rely on third-parties for an appropriate use.

The current system's complexity and demanding relevant input factors, if dependent on (digital) connectivity, thus might undermine a sustainable utilization, maintenance and inclusive ownership within the communities, especially in Malawi.

Both contexts moreover seem to require a need for capacity-building, depending on the actual complexity of the end-product.

Nonetheless, Graf, assuming improving access factors in the contexts of Malawi and Kenya in the future, sees an argument to at least research potential deployments now.

However, even if feasibility and ethical studies would show that most of the target group was formerly able and capable to utilize a certain [mechanism](#), there would always be the need to provide alternatives for receiving assistance (Graf).

Finally, required factors for inclusive ownership might be dominant enough in a given community to purposefully serve at least a bulk of PA with an [SSI](#) (assuming its functional advantages).

#### 9.4.2.2. *A Participatory Approach*

While there might be a desirability of giving individuals more control and ownership about their [identity](#) (Levin, Zambrano), concerns were expressed that an [SSI](#) might not necessarily be geared towards the most urgent humanitarian and development needs (Zambrano).

Zambrano hence strongly emphasises on generally connecting technology utilization to the most pressing contextual development needs. Zambrano accordingly highly suggests reading into governmental development plans to identify political priorities and development needs when considering a pilot.

Logically, not only the government needs to be involved and consulted, when a foundational purpose of [SSI](#) is aimed for to eventually better the lives of the people affected.

Zambrano consequently suggests a participatory approach during the design face, to investigate whether [SSI](#) is really the best and most desired way to approach the needs the communities express. Primarily, one should focus on the actual needs first, and then look for the right technology to serve these needs (Zambrano).

Graf and Levin analogously advocate for asking communities on the ground, what their most urgent needs would be. Finally, an [SSI](#) would thus need to achieve the “[user-centric](#)” design (Kondakhchyan) by a strong focus on the individuals in question, aligning with the literature.<sup>45</sup>

As people affected might not be able to freely consent in the context of a [disaster](#) (Graf, Levin), one assumingly would need to capture specific needs by the communities beforehand. While, as stated before, this thesis cannot cover these kinds of elicitations, the next sub-chapter tries to provide at least some thoughts on that issue.

---

<sup>45</sup> Refer to „user-centric identity“ in glossary.

### 9.4.2.3. Demand for a (foundational) SSI

#### 9.4.2.3.1. The need for protecting data

Relating to one of the arguments of providing an [SSI](#) to individuals with special data protection needs, Zambrano points out, that the abstract concept of data sovereignty as political right rather would be relevant in industrialized nations with more sophisticated means to digitally surveil its citizens.

Furthermore, while risks of persecution are very dependent on the exact type of [disaster](#) (Graf), according to Zambrano, data protection properties of an [SSI](#) would not necessarily prevent governmental persecution. A government could persecute minorities regardless of a [digital ID](#) disguising [PII](#). Persecution would normally be based on from the analogue world retrievable information (Zambrano); e.g. people would know very well on the community level, whom to associate with which certain group etc.

Luckily, in both contexts, persecution from sides of the government is not identified as a big concern, though.

In Kenya, handing data to the government is not seen as very problematic, at least in most circumstances (Graf).

For Malawi, Kunje does not see ethnic minorities or other groups of people fearing to share their data with the government.

Finally, one of the compelling arguments for an [SSI](#) after Bansal, the need for data privacy due to e.g. persecution of minorities, might need to stem from another side than the public sphere.<sup>46</sup>

Potential data-protection concerns for marginalized populations however not only arise from governments.

Levin, an advocate for data and information protection of people affected, to some extend grounds his strong opinion on the need for humanitarian agencies protecting data in front of service providers, because of their, amongst others, non-consensual use and passing on of [PII](#).

---

<sup>46</sup> Obviously assuming a non-discriminating

Hence, according to Graf, in Kenya, while sharing data with the government may not be problematic, sharing information with service providers might be.

Internationally active companies, such as the [MNO](#) of interest, a subsidiary of an internationally active company, might process data to e.g. a refugee's adverse interest.

For example, if a refugee was receiving assistance over [M-Pesa](#) in Kenya, and subsequently migrating to Europe, the service provider of interest's mother company or another party gaining access might hold data preventing her or his eligibility to stay (Graf).

Having these service providers involved, thus might make data flows more complex and in-consensual third-party access may not be prevented.

Accordingly, after Kondakhychyan, complying with service providers' requirements, such as the collection of biometric data, might conflict humanitarian data protection needs (relating to the previous discussion around in-appropriate data processing, storage etc. of service providers).

Therefore, Levin confirms the potential of protecting individual data on the one hand, while ensuring transparency to align with [AML](#)-policies and ensuring accountability of the humanitarian actors with an [SSI](#).

On the other hand, Levin assumes, that adoption of a potential [SSI](#) would rather be driven by the traditional banking sector based on an argument around [KYC](#)-cost-reduction.

Whether this would yield a [PII](#)-reduction aligning with a humanitarian agency's aims, remains open.

#### **9.4.2.3.2. The need for recipients' open-loop KYC-compliance**

Coming back to the previous discussion about reduced [KYC](#) and risk-based approaches when delivering [humanitarian assistance](#), Levin strongly emphasizes, that concerns about people affected needing to comply with [KYC](#) would lead the discussion into the wrong direction. Firstly, as stated above, [KYC](#) regulates entities, not individuals. Secondly, would context determine appropriateness of seeking [KYC](#)-compliance, for example, a permanent business relationship. Facing a [disaster](#), or even [protracted crisis](#), humanitarian agencies should strongly insist on people affected not needing to fully comply with [CDD](#) in the first place. Levin accordingly implies, that

humanitarian agencies should/could take over the risks associated with a third party not performing due diligence on the person affected; usually one would find a legal basis for an agency being able to vouch for the individuals they assist.

Sossouvi furthermore explains, that [financial inclusion](#) impacts driven by [mechanisms](#) for [humanitarian assistance](#) delivery would normally be marginal. People affected usually would stop using the [mechanism](#) beyond cashing-out assistance, due to, inter alia, lack of funds or strong digital ecosystems. This would to an extent align with (Dubus and van Hove, 2017) for [M-Pesa](#) in Kenya.

Furthermore, the transactional limits with reduced [KYC](#) would normally align with the transactional capacities of the targeted populations.

This hence brings up the question, whether deploying a non-governmental ID to enhance [financial inclusion](#) into [open-loop](#) systems really responds to what humanitarian interventions need to focus on.

Nonetheless, as previous sections pointed out, the aim for [open-loop KYC](#) focusses rather on the long-term impacts of [financial inclusion](#), empowering recipients and increasing system sustainability. While recipients still might stick to more traditional/informal financial service providers after the interventions due to various reasons, such as familiarity with informal [mechanisms](#), or withdrawing the whole assistance at once to meet pressing consumption needs (Bailey, 2017), even if increasing access to [DFS](#) is neither an appropriate goal nor a priority of the interventions, humanitarian organizations still should use digital delivery systems where they offer the most efficient, accessible and transparent way to deliver [CBA](#) (Bailey, 2017). Thus, while [CBA](#) as response to emergencies should not be regarded as a primary tool for financial inclusion the opportunity to do so should be kept in mind (Fabre and Aggiss, 2017).

Sossouvi, accordingly, while implying that [closed-loop KYC](#) was potentially enough for assistance delivery itself, also implies, that systems usually would then be built from scratch for each single delivery.

Relating that back to the previous discussion around functional designs and instrumental approaches, this might accordingly yield massive duplication efforts and fragmentation - and accordingly, a wastage of resources for the agencies.

Moreover, there clearly is a need for [financial inclusion](#) in some contexts (Sossouvi).

A functional while interoperable [SSI](#), if bound into an open-loop system, could alleviate these issues. Implicitly, it would then serve wider, foundational purposes, as discussed above, given its government-approved long-term sustainability.

#### **9.4.2.3.3. The need for legal Identities**

Zambrano and Kondakhychyan explicitly confirm the need for [legal identities](#), aligning with the literature.

As Sossouvi mentioned, a lack of formal IDs is however not necessarily a problem for [humanitarian assistance](#) delivery itself.

According to Sossouvi, after best practice, an assisting humanitarian agency would furthermore facilitate for un-documented recipients obtaining a national/local ID. Aligning with the previously discussed possibility for reduced [KYC](#), the potential sufficiency of [closed-loop mechanisms](#), and the danger of replacing governmental duties, providing foundational IDs as humanitarian agency might thus lack compelling arguments. And in [Malawi](#), as both Bansal and Kunje clarify the ambiguities left from the desk-study - the government has rolled-out the national ID system with vast coverage, even in hard-to-reach areas.

After Kunje, obtaining the national ID would not be very problematic for Malawians, as even without another ID [credential](#) vouching for nationality, such as a letter of the chief. Individuals could acquire the ID by solely answering some questions at District Commissioner's offices in towns; Kunje hence did not come across a situation, where the ID was being denied to an individual.

Au contraire, Kunje, coming back to the current flexibility towards authenticating for public services with other forms of ID [credentials](#) than the national one, points out, that there would be a rather a need for sensitization proving an added value for the national ID to some people.

This situation could assumingly worsen if a foundational [SSI](#) was provided by a humanitarian agency, if it was running parallel to the public system(s).

Hence, after Bansal, the national ID, based on its characteristics and wide distribution, accordingly, will and should be the only ID [credential](#) for nationals to be accepted by the Reserve Bank Malawi and its regulated [FSPs](#) for (e-)[KYC](#)-compliance.

Kunje however also informs about the potential problematic of people living in the border areas to Mozambique, Tanzania and Zambia, who could have issues in accessing the ID.

This at least partially would provide an argument for providing legal foundational identification, while the need for legal identification to some groups in Kenya is more explicitly expressed (Anonymous, Kondakhchyan, Zambrano).

Coming back to above sub-chapter “Filling the Gap”, there however is an agreement among respondents, that it is a national and public obligation to provide public identification structure, not a task of the humanitarian sphere (Bansal, Levin, Kondakhchyan, Sossouvi, Zambrano).

Common sense was therefore, that humanitarian agencies could (rather) support national identification efforts (Kunje, Bansal, Levin, Kondakhchyan, Sossouvi, Zambrano) without setting up parallel structures hindering governments to organically grow the relevant capacity on its own (Sossouvi). Otherwise, weakening public structures by circumventing them, might worsen impacts of future disasters (Sossouvi); having agencies taking over public tasks in the long-term potentially undermines long-term stability of a context (Levin).

After Bansal, according advocacy for ID-inclusion should then also cover internally displaced populations or refugees.

Hence, if a lack of legal IDs for [KYC](#)-compliance was perceived as a problem, one thus should rather strive towards providing the required (public) infrastructure to fully comply with [KYC](#) (Bansal, Levin).

Or, as Levin put it, one can have an argument to provide legal IDs to everyone, without implying, that humanitarian agencies should be the ones providing it.

#### 9.4.3. Functional vs. foundational SSI

Finally, one may conclude the brief ethical discussion about foundational humanitarian [SSIs](#), that first and foremost, a functional deployment successfully improving [humanitarian assistance](#) itself should be the primary objective. This would align with the beforehand discussed political, social and technological factors in both countries making a controlled, functional deployment seemingly more adequate for now.

Focussing on the provision of a foundational [SSI](#) too much eventually could deter from delivering the actual core responsibility – providing [humanitarian assistance](#) (Bansal, Levin, Kondakhchyan, Sossouvi, Zambrano) as well as the core challenge of a lack in legal IDs excluding people from public services (Zambrano).

As pointed out previously, this does not necessarily mean, that a functional humanitarian [SSI](#) never can or never should serve some broader, more foundational purposes.

Relating to the previously mentioned possibility of non-undermining coexistence besides a public system, it could, backed by a foundational governmental ID, serve as vehicle to more foundational services, for example by satisfying [open-loop KYC](#) for [financial inclusion](#).

This might be especially appealing in a context, where the government so far provided analogue IDs but so far lacked the capacity to digitize the system sufficiently. A digital SSI could then alleviate that lack, potentially providing some advantages when compared to the analogue, foundational ID system of the government.

Conclusively, this could mean, that while a humanitarian agency should lobby and advocate for inclusion into public identification infrastructures, a more than functional [SSI](#), while primarily giving people affected more data control and protection and improving services of an agency, could have its rights to exist.

Again, amongst other decision-maker metrics, interoperability would be key for that.

## **10. Conclusion**

### **10.1. Chapter Overview**

The last chapter provides the conclusion, suggestions for further research and the limitations of the research.

### **10.2. Conclusion**

Compiling all the information retrieved, due to political (governmental sovereignty, adoption of [SSI](#) only feasible after successful use-case), economic and social (currently lacking factors for inclusive, national deployment), technical (scalability and infrastructural issues) factors and general ethical considerations (undermining public sovereignty and patronage), a deployment of a functional [SSI](#) in a controlled pilot seems to be the currently most feasible way in both contexts.

Whether an [SSI](#) as deployed by a humanitarian agency can and should alleviate the “global ID challenge”, a lack of legal IDs, thus remains questionable for now.

Both countries’ [KYC](#)-regulations and humanitarian mandates might still provide space to deploy an [SSI](#) implicitly serving a more foundational character immediately. Either, by convincing the service provider to formally accept it for [CDD](#), or due to a risk-based approach on humanitarian grounds, using the [SSI](#) internally for mitigating [ML/TF](#) risks. The first option, without consulting the relevant public bodies, inherently sets up parallel structures to the public ones. The second option, without consulting the relevant public bodies, makes long-term sustainability questionable, after a humanitarian intervention has ended.

Hence, a humanitarian agency should engage in discussions with the relevant regulators and ID-authorities immediately and openly. Due to the technical immaturity and complexity, one can however not necessarily provide a use-case without a convincing and transparent pilot.

Yielding formal legal recognition thus might be a long way consisting of incremental steps, dependent on yet uncertain improving political, economic and social, regulatory factors as well as technological advancements.

Reasonably, the only way an [SSI](#) thus should be focussed on for now, is, if it provides actual improvements to humanitarian interventions in the first place, constantly checked against do-no-harm principles, while at the same time ensuring that people affected demand any of the alleged advantages vis-à-vis alternative identity systems. A demand-driven need for legal IDs does not necessarily imply a demand-driven-need for a foundational [SSI](#) in particular.

A broader, foundational adoption hence should be in the scope of strengthening the public [identity](#) infrastructure. Otherwise, humanitarian agencies risk a deterrence from their core mandate – alleviating immediate suffering occurring from [disasters](#) and crises.

While this approach might undermine some anarchical ideals some advocates for a “pure” [Self-Sovereign-Identity](#) hold, due to the reasons above, it is not in a humanitarian agency to determine, whether these should be adhered to or not.

Eventually, there seems to be a conflict between wanting to create synergies between humanitarian interventions and long-term development, without replacing governmental tasks as humanitarian agency.

More specifically, the *Barcelona Principles*' demand for utilizing *financially inclusive open-loop mechanisms*, might deter from the humanitarian *mandate*, if the agency itself needs to provide a *KYC*-compliant solution to people affected in the long-run.

This conflict might solely be re-solved by rigidly prioritizing the core of *humanitarian assistance* and then, secondarily, carefully trying to support long-term development by linking to according *nexus*, without undermining or replacing a government.

Arguments vis-à-vis the relevant decision-makers for a more foundational humanitarian ID concerning improved *disaster* preparedness, delivery and recovery, *protracted* crisis and the *humanitarian-development nexus*, besides data protection, then could prove as successful.

Finally, the concluding answer to the Research Question, how and if a humanitarian-backed *SSI* could yield *open-loop* inclusion in Kenya and Malawi, to the author's current knowledge, is:

In both contexts, it could prove possible to deploy an *open-loop* enabled functional *SSI* as humanitarian agency, if based on humanitarian grounds and a risk-based approach. Ethically and politically, for a more formal legally-compliant and sustainable acceptance, the humanitarian agency must however involve the public sector and prove an *SSIs* advantages when compared to the incumbent systems.

Finally, a humanitarian *SSI* could formally coexist, serving as vehicle to at least some foundational functions.

This potentially would only happen based on its merits of interoperability, efficiency, transparency etc., and most importantly, based on the consent of both government and individuals.

### 10.3. Recommendations for further research

Ideally, this research would not end, but begin here.

As for example Kondakhchyan expressed, there is an immediate need to engage with relevant decision-makers in the contexts.

This should be pursued with an eye on clearly stating the, even if implicit, goals of an SSI's deployment and creating an accommodating space for innovation. Otherwise, this project could suffer the same fate as other pilots in the humanitarian sphere – “a pilot for the sake of piloting” (Kondakhchyan), eventually failing to reach meaningful scale.

However, that must be done on a higher hierarchical level; as the limitations to the research point out, it has proven infeasible to have a student writing his thesis “knocking on the door” of the Central Banks and the national ID authorities to engage in according discussions. Strengthening partnerships with these and other key authorities, as well as the relevant service providers needs to follow.

For that, it would make sense, to perform a more substantive stakeholder-analysis of both contexts and relevant institutions.

On the international level, the [ID2020](#)-initiative (Zambrano) and ID4D were brought up (Sossouvi, Zambrano). To prevent competition and further fragmentation and potentially leverage the expertise and political weight of involved stakeholders, 510 could consider an involvement, if possible. It needs to be researched, whether 510, adhering not only to [privacy-by-design](#) principles, but also the highest humanitarian standards and aiming to be non-proprietary with its ID system, could maintain according characteristics during that involvement. However, it might prove important to shape discussions in these spheres according to 510's ideals. In that sense, Levin stated, that lobbying for governmental [SSI](#)-acceptance on an international, rather than national level, could be a possibility. This potential clearly should be researched.

Moreover, did Graf, Kondakhchyan and Zambrano implicitly or explicitly suggest looking into “E-Estonia”, which after Graf, would be the most advanced example of a decentralized identity system in hands of a sovereign government. Kondakhchyan further mentioned “Caribou Digital” as potential provider of relevant information. Both these recommendations were unfortunately not investigated further, given time-constraints. A research following-up on these mentions might thus be valuable.

Finally, piloting the potential [digital identity system](#) needs to be accompanied by comprehensive co-design sessions in both contexts, for an adequate system's appropriation and a clear assertion of relevant needs of the people affected.

## 10.4. Limitations

### 10.4.1. Introduction

The limitations of conducted research are multi-faceted and could potentially provide enough writing material for a very own thesis. Besides limited time and scope, requiring a less than optimal approach and methodology, the research topic and processes demanded quite some flexibility.

Furthermore, the semi-structured interviews marked the author's first experience with conducting qualitative research, who's academic background neither is in law, technology, nor [humanitarian assistance](#) and who has so far not been to either Malawi or Kenya. These factors may have led to considerable flaws in both research methodology and approach - and consequently, the results. Flaws, of which the author still might not be aware of to date.

The subsequent sub-sections aim at providing a non-exhaustive overview about some of the research's limitations to the author's awareness.

### 10.4.2. Methodology and Research Process

#### *10.4.2.1. Narrow Scope and multi-faceted research topic*

On the one hand, scope and time demanded a narrow scope for pursuing the research. One the other, a lot of different disciplines were compiled, to gain a certain holistic overview and understanding of the subject matter. This resulted in a lot of "shallow dives" into various disciplines, without allowing for a true in-depth exploration and discussion, which is also reflected in the research's results. Therefore, a lot of issues were simply left behind and not tackled.

For example, when it comes to regulatory aspects of [blockchain](#) (which by the way are criminally under-explored from a technological perspective in this thesis), the crucial conflict between a ledger's immutability and the European GDPR – the "right to be forgotten" potentially making off-on chain data hybrids necessary and other complex cross jurisdictional boundaries (GSMA, 2018), also highly relevant to the system regarded, were not considered at all.

#### *10.4.2.2. Desk Studies and general literature review*

A substantive amount of literature consulted does not stem from peer-reviewed articles, given the novelty of blockchain technology and its prospect for identity

management systems. While this was to be expected given the topic, the vast amount of grey literature used for this paper might undermine its credibility.

Furthermore, given time-constraints, the desk-studies were conducted in a rather unstructured way. A structured literature review would have been a more adequate tool to provide more reliable and sophisticated secondary data. The desk-studies therefore were only able to represent the relevant macro-environments in a fragmented way.

Moreover, due to sometimes weekly new publications on the topic of [SSI](#) and upcoming regulations in the contexts, as well as very recent developments in the political environment and national identification systems, including all new relevant publications was not feasible. This might have led to a situation, in which some of the cited literature is already obsolete or redundant.

By partially validating the results of the desk studies within the semi-structured interviews, this was partially mitigated, but some of the risks concerning a lack in credibility, incompleteness or redundancy remain.

#### *10.4.2.2. Semi-Structured Interviews*

As indicated before, institutional representatives in both contexts were not overly eager to be part of the research (see ethical considerations below). This yields statements predominantly being made on the more general level. While they still might provide valuable insights for both contexts, the eventually small amount of semi-structured interviews lack not only a sufficient generalizability of findings, but also a satisfying contextual appropriation. This could have been alleviated by conducting a significantly higher number of interviews, which unfortunately was not possible, given the time-intensity every (on average 80-minutes long) interview demanded in preparation and following up. While the research tried to include as much context as possible and all respondents showed considerable contextual sensitivity, generalization still sometimes comes from “the outside”, just as the author, increasing the risk of e.g. “Western” bias. Another considerable amount of bias can stem from the interviewees. As the conducted interviews hopefully underscore, all respondents are equipped with high expertise in their field, a strong normative compass and a high added value to this thesis. However, as some of them were explicitly chosen based on the previously consulted literature, in the end, experts validating the literature they

wrote by themselves is probably not adhering to the highest academic standards. Furthermore, although a quite substantive amount of literature was consulted beforehand, the interviews were mostly suffering from the author's shallow knowledge and inexperience in conducting them. Although quite some meaning making to the research question might have been achieved after all, conducting interviews with exactly the same respondents could thus potentially still provide additional knowledge. The analysis of the interviews, placing some interpretative burden on the author, is furthermore highly exposed to flaws, such as mis-understanding or mis-interpretation. While this was partially mitigated by sending the complete and summarized versions of the interviews to each respondent for approval, and thus, confirming the summaries' preliminary structuring and meaning-making, the analysis in the main text above, compiling all the interviews was not read by all respondents, as this was not feasible due to time-constraints. There, structuring multivariate streams of data into a chronological structure for a more or less concise text, has proven to be very difficult and might undermine investigating the full depth of statements made. This was potentially worsened by the author's approach to structure the chronological order after the three last Sub-Questions, which was not completely possible, as the overlap of statements between the sub-chapters show.

However, after all, some meaning making was achieved. With the knowledge generated, further interviews should follow, now allowing for more in-depth discussions.

#### 10.4.3. Ethical Considerations

While the author aimed at acting as ethical as possible when arranging and conducting the semi-structured interviews in relation to the research's underlying intentions and the freedoms given to potential and actual respondents, some noteworthy ethical issues might persist.

Firstly, what also was rightfully indicated by some respondents, we need to ask ourselves, whether the individuals targeted by the digital ID-system actually want and need an [SSI](#), or a [mechanism](#) enabling [financial inclusion](#), or whether [CBA](#) is actually the preferred over [in-kind assistance](#). This being a very context-dependent question, before this research was conducted, obviously, the people affected, should have been consulted. Due to the reasons stated when outlining the motivation for SQ vii, which

was aiming to partially mitigate that issue, this was however not feasible. However, solely assuming access to digital solutions is the end to the problem, without carefully analysing recipient's demands and needs, risks omitting important considerations to be made (Bailey, 2017).

Secondly, relating to the political sensitivity of the question of filling the gap, or even just complementing a national identity management system, public representatives should have been included much more in the research process. While this was aimed for by reaching out to the as relevant identified national institutions, the lack of responses could not be mitigated. As proven by substantive concerns expressed by the respondents, was there a general fear, that the regarded [digital identity system](#) would aim to circumvent public structures. Knowing the 510-team, the author truly believes, that this is not the case, and that the team is highly sensitive to these and other crucial ethical considerations. However, as the examples of the cover letter and the initial mail sent in Appendix 9 and 10 indicate, this does not necessarily become clear, as they quite straight-forwardly bring up the question of how a more legal character could be achieved with the identity system. Establishing a certain level of trust and a shared understanding of the ethical and political sensitivity was rather performed while conducting the actual interviews. This led to a situation, in which many institutional stakeholders in the context did not follow-up accordingly, after initially indicating an interest to be interviewed.

This straight-forwardness of the initial mails and cover letters was however performed due to an ethical consideration by itself – immediately unveiling the research's underlying questions to not trick a potential respondent in participating based on a disguised motivation. Giving the potential respondent to freely and fully informed consent to an interview was prioritized. Nonetheless, this, together with the academic standard to take a respondent's signature for the letter of informed consent before the interview, could have been a considerable deterrent for some individuals to take part – then yielding the ethical problem of concluding the research without sufficiently involving representatives from the public sphere in both contexts.

This eventually increases the previously mentioned risk of "Western bias", potentially exacerbated by focussing on larger, international humanitarian agencies throughout the research, while leaving out grass-root organisations or small NGOs.

Finally, as with the underlying assumption, that blockchain-technology will eventually improve, assuming that current problems in terms of e.g. hardware possession or literacy capabilities will be massively overcome in the countries or by a humanitarian organisations' [\*mechanism\*](#)-design, is inherently a very strong one. From the perspective of a humanitarian agency, these assumptions are necessary to argue for this kind of research, but also impose a strong uncertainty about its credibility.

Thus, a comprehensive set of complementary measures to counter current hindrances needs to be undertaken, along with a critical reflection on [\*market-based approaches\*](#) seeking sustainable, equitable intervention impacts via [\*financial inclusion\*](#) and the desirability of an explicit focus on the [\*humanitarian-development nexus\*](#).

## Appendix

### Appendix 1: Glossary

Accretionary ID	Accretionary ID models potentially allow undocumented individuals to establish an initial ID with little or no supporting information; supporting attestations are incrementally added over time. This form of ID would start with relatively rather confidence that identity claims made are valid and unique, thus insufficient for e.g. KYC requirements. However, they would become more trustworthy with the subsequent addition of more information. Enrolment then becomes a process of identity accretion, not a one-time event. Accretionary ID technologies are currently mostly in the pilot phase (USAID, 2017).
Activation (prepaid card or SIM)	According to the Cash Learning Partnership (CaLP) <sup>47</sup> , activation is defined as linkage of an individual with a specific card or SIM and authorization of usage (by SMS, online activation, or phone) (CaLP, 2017). Also known as “personalization.”
Agent	An entity where an e-transfer can be redeemed for cash (Sossouvi, 2013), and/or where e-cash account holders can perform other transactions (CaLP, 2017). Different Financial Service Providers (FSP), for example banks or mobile network operators can have agents. Agents are managed by FSPs, not humanitarian agencies (CaLP, 2017).
Algorithmic ID	Refers to authenticating identity based on making inferences about the patterns and unique features of an individual’s digital footprint. When compared to a one-time (e.g. biometric) capture, identity is inferred from a subject’s ongoing behaviour (USAID, 2017).

---

<sup>47</sup> CaLP embodies a partnership of humanitarian actors engaged in policy, practice and research within cash based assistance (CBA) on the global scale; its members collectively deliver the majority of CBA in humanitarian contexts worldwide. CaLP itself does not deliver CBA directly (CaLP, ND).

AML/CTF standards	Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) standards refer to a set of rules, normally issued by central banks, which aim to prevent and detect the utilisation of financial services for money laundering (ML) or financing terrorism (FT) (GSMA, 2017). The Financial Action Task Force (FATF, 2012-2018) has made 40 non-binding recommendations designed to assist financial institutions to tackle money laundering and financing of weapons and terrorism. These constitute the international standards for AML and CFT.
ATM	Automatic Teller Machine. A computerised telecommunications device for performing financial transactions without the need for a cashier (Sossouvi, 2013).
Authentication	The process of verifying a person’s identity (CaLP, 2017), using one or more factors or credentials in order to establish that persons are who they claim to be (World Bank and GSMA, 2016). This can also relate to the context of digital identities (World Bank and GSMA, 2016).
Barcelona Principles for Digital Payments in Humanitarian Response	<p>Based on Global Innovation Exchange (2016):</p> <p>8 principles guiding the utilisation of digital payments in humanitarian responses. Endorsed by, amongst others, CaLP, CGAP, FAO, UNDP, UNICEF, WFP:</p> <ul style="list-style-type: none"> <li>i) <b>Select payment mechanisms for beneficiary empowerment</b> - People in need of assistance should be put first, maximization of recipient value and choice should be aimed for.</li> <li>ii) <b>Collect data that is relevant and proportional</b></li> <li>iii) <b>Safeguard the right to data privacy and protection</b></li> <li>iv) <b>Facilitate pathways to financial inclusion whenever possible and appropriate</b> - Priority is given to open-loop systems. This means, that recipients should be connected with a personal account or “wallet” (see</li> </ul>

	<p>according term in below), leveraging local markets and ecosystems, enabling end-users to access a formal transaction instrument that can satisfy payment needs (Blake et. al, 2016).</p> <p>v) <b>Prioritize and build on existing local systems and infrastructure</b> - Agencies should give preference to digital financial and payment services that are already locally available, and which are under the supervision of the country’s central bank or other relevant regulatory body. Domestic social cash-transfer programs should be leveraged if possible, to avoid duplication. Agencies should further coordinate with existing national identification schemes, if possible, to strengthen access to national ID systems.</p> <p>vi) <b>Invest in organizational preparedness to quickly leverage digital payments whenever appropriate</b></p> <p>vii) <b>Develop institutional and collective capacity for effective humanitarian &amp; private sector engagement</b></p> <p>viii) <b>Coordinate the use of multipurpose and shared payment systems</b></p>
Biometric Authentication	Technologies measuring and analysing human physical/behavioural characteristics for authentication purposes, such as fingerprints, voice prints, iris scans (CaLP, 2017).
Blockchain	Blockchains are digitally distributed ledgers with some additional key characteristics such as the use of a wide variety of <b>cryptographic</b> functions (for example hashing algorithms), <b>peer-to-peer</b> discovery and synchronisation mechanisms, <b>consensus algorithms</b> determining sequence and validity of transaction, <b>cryptographically linked</b> blocks bundling together the lists of transactions, <b>validity rules</b> of the network determining what transactions are considered valid and how the ledger gets

updated, etc. and **Crypto economics** - a combination of cryptography and economics (game theory) ensuring incentivization of actors to remain honest in the **decentralised system** (GSMA,2018). The ledgers itself is not quite a database. It rather resembles a log file of transactions (Zambrano, 2018a).

Strongly simplified, blockchains thus can be defined “as a **public spreadsheet** that **sequentially records transactions** among users operating within a **decentralized peer-to-peer network**” (Zambrano, 2017, p. 6). All nodes and users of the “spreadsheet” have **real-time and full access to data** recorded in the database. The possible **transparency of blockchain metadata** to and **complete transaction history** for all nodes and users in real-time leads to “distributed trust” within the system. Previous **third-party authorization** or permission or a pre-existing **central authority is not required** for a transaction. No central server is needed, the interconnected nodes can be equal (depending on the application), there is **no single point of failure** in the system (Zambrano, 2017; Pilkington, 2015 and Schlatt et al., 2016). Involved network nodes store an updated copy of the data, **updates automatically diffuse** among all nodes. One of the key innovations of blockchain technologies is how the records of transactions are interlinked: Each record row, comprised of a block of transactions, has a unique identifier linked to the previous one. The unique identifier of the previous block is used to compute the identifier for the new block thus creating a mathematical link between blocks in the chain. Because of this stored **data** is seen as **basically immutable**, as it would require changing all records in the chain; **user integrity is ensured**. Adding new rows to the data requires the decentralized nodes’ consensus, originally achieved with the help of the proof of work<sup>48</sup> algorithm which

---

<sup>48</sup> However, other algorithms to reach distributed consensus, such as proof of stake or proof of capacity are used in some applications as well (Schlatt et al., 2016), but not further elaborated here.

	<p>nodes must run. Proof of work resembles a traditional ‘guess the number’ puzzle with much higher complexity. The outcome of proof of work is shared among network nodes that can then validate the result. Once this happens, the block is added to the existing blockchain (GSMA, 2018; Zambrano, 2017). To access the system, the use of cryptographic tools is needed. While creating a profile or providing personal information is not required, all nodes and users must use public key cryptography to identify themselves and access the network. A private key (kept like a password) is used to encrypt transactions which can then be decrypted by the intended recipient using the sender’s public key. It is considered as mathematically impossible to use a public key to decipher a private one (Zambrano, 2017 and Pilkington, 2015).</p> <p>Basically, the blockchain as incorruptible “public spreadsheet”, or ledger, can be programmed to not only record financial transactions, but virtually any form of transaction. Thus, while the first applications utilizing blockchain, such as the cryptocurrency-incumbent Bitcoin released in 2009, blockchain-technology is also seen as key enabler of Self-Sovereign Identities (refer to according term in glossary) (Sovrin, 2018; Gemalto, 2018; Baars, 2018).</p> <p>This is due to the use of sophisticated cryptographic tools enable to generate unique, transparent, resilient and integer and identities for individuals interacting within the distributed network (GSMA, 2018). Generally, these identities can be pseudo-anonymous, secure, immutable, and directly created and managed by the individual. This in principle makes blockchain an ideal candidate to enhance innovation in the digital identity sector (Zambrano, 2018).</p> <p>Also refer to Distributed Ledger Technology below.</p>
Cards	Card-based systems form e.g. humanitarian organisations are not necessarily linked to a bank account, although they can be. They

	are loaded with funds that recipients can access directly via ATMs to collect cash or via PoS devices/terminals for purchases at registered merchants. They can thus be either for CTs or for voucher programmes (Sossouvi, 2013).
Cash Based Assistance (CBA)	CBA refers to all programs where non-contributory cash and/or vouchers are directly provided to beneficiaries to satisfy minimum needs (Garcia and Moore, 2012). In humanitarian assistance, it refers to the provision of cash/vouchers for individuals, households or communities; not to public sector actors (CaLP, 2017). The term can be used interchangeably with Cash Based Intervention (CBI), Cash Based Transfers (CBT) and Cash Transfer Programming (CTP).
Cash Transfer (CT)	The provision of assistance in the form of money (either physical or electronical) to beneficiaries (individuals, households or communities). Cash transfers are a modality and distinct from vouchers and in-kind assistance. The nature of cash usually implies there is no spending restriction, a CT may however be regarded as restricted when an intervention’s design, targeting and objectives intended that the cash is spent on specified goods/services (CaLP, 2017).
Closed-Loop	In a broad sense, according to the International Telecommunication Union and the Universal Postal Union (2017), “closed-loop” refers to payment systems, in which the <b>payment provider is also the payment operator</b> . This means, the payment system is used by a single provider, or a very tightly constrained group of providers, <b>creating a proprietary system</b> , which is <b>expensive to maintain and scale</b> (International Telecommunication Union and the Universal Postal Union, 2017; Blake et. al, 2016; Zimmerman et. al, 2016). A simple example might be an ATM card which can only be used at bank branches of the financial service provider that owns both the cards and the ATMs (Blake et. al, 2016). Another example might be a prepaid

phone card, or a gift card from a specific company (Cornish, 2016), say Burger King, only redeemable at their stores for burgers, and **not interoperable** with, for example, buying burgers at Mc Donald's. Generally, closed-loop systems do not allow storage of funds or expire after a certain period and are based on expensive (Zimmerman et. al, 2106).

In the sphere of humanitarian assistance, "closed-loop" thus refers to a system, in which the entity that issues the e-transfer device is always the same institution that provides the acquiring infrastructure, thus is holding the relationship with the transaction points (CaLP, 2017; Sossouvi, 2013). A simple example here would be the distribution of a mobile cash voucher to be redeemed at locations specifically selected by the humanitarian organisation (Zimmerman et. al, 2016).

These systems hence restrict the account's capacity, **only allowing recipients to access their funds via designated agents or ATMs and restricting additional deposits/savings** (Ford, 2017, Zimmerman et. al, 2016). A closed-loop system thus **usually cannot be leveraged for further financial inclusion** beyond the humanitarian intervention (Zimmerman et. al, 2016; Zimmerman and Martin, 2016)

Advantages of these accounts to the organisation are **lighter (KYC-) regulation requirements** due to limited risk of money laundering or other illegal activities when compared to open-loop systems, an **advantage if speed of delivery is critical**. Further, **increased transparency** - as accounts are easier to monitor - can be achieved (Ford, 2017, Cornish, 2016). Also known as "limited-purpose instruments" (Bold et al., 2012, pp. 3, 4).

After a disaster, the priority is to get assistance to the human affected as quickly as possible. Oftentimes, and particularly in nascent markets where digital payments do not yet have a large user base or supporting agent infrastructure, the logistics of using

	<p>digital payments can cause unacceptable delays. Hence, digital payments, if used at all, are often disbursed through closed-loop systems (Cornish, 2016; Zimmerman et. al, 2016; Zimmerman and Martin, 2016).</p> <p>Also refer to “open-loop” below in glossary.</p>
Commodity Voucher	<p>Commodity vouchers can be exchanged for a fixed quantity and quality of specified goods or services at participating vendors. They share some similar characteristics with in-kind assistance by restricting and specifying the benefit. On the contrary however, the benefit is accessed at local markets through merchants (CaLP, 2017). See also Value Voucher and Voucher below.</p>
Conditionality	<p>Conditionality implies that a human affected must fulfil prerequisite or qualifying conditions, activities or obligations to receive assistance. It is distinct from “restriction” which entails only how transfers are utilized. Conditionality can in principle be used with any type of assistance, depending on the objectives and design of the programme (CaLP, 2017). See also Restricted Transfer below.</p>
Contactless Card	<p>A smart card which can be read by a near field communication device (NFC, check according entry in glossary) by being tapped on a PoS, terminal or a smartphone with card reading capabilities (Sossouvi, 2013).</p>
Cost-Effectiveness	<p>Cost-effectiveness is the extent to which the program has achieved or is expected to achieve its results (outcomes/impacts) at a lower cost compared with alternatives (World Bank, 2007).</p>
Credentials	<p>Mechanisms, processes, devices or documents vouching for the identity of a person with a set of claims made by and entity, through some method of trust and authentication (Longley and Sporny, 2018; Wolrd Bank and GSMA, 2016). Government-</p>

	recognized credentials can for example entail (ID) cards, digital certificates, identifying numbers etc. (USAID, 2017).
Critical Market Systems	The specific market systems most urgently relevant to the target population's needs. Essentially those markets that (could) have a major role in meeting the essential needs of the target population (Juillard and Sloane, 2016).
Digital Financial Services (DFS)	Digital financial services (DFS) refer to the access to fundamental financial services, such as savings, credit and insurance as well as performing transactions via digital channels, e.g. mobile phones, cards, computers (Grossman and Nelson, 2014).
Digital Divide	Here defined as (individual) socio-economic inequality regarding the access to, use, or impact of ICTs (Organisation for Economic Co-Operation and Development [OECD], 2001).
Digital Identity (Digital ID)	<p>For a definition of the concept of "identity" in general, refer to according term below.</p> <p>A Digital ID is a set of electronically captured, stored and transmitted identity attributes that uniquely identify a person (Malik and Mittal, 2017; Saxby, 2013) and are used for electronic transactions (World Bank and GSMA, 2016). Hence, for an ID to be considered digital, the credentials or certificates issued must store and communicate data electronically, e.g. like smartcards or mobile identities (World Bank and GSMA, 2016). Accordingly, digital IDs lie at the core of interactions between human-machine or human information systems (World Bank, 2014).</p> <p>Normally, the information required for transactions entail full name, gender, date of birth and at least one piece of identifying information such as a numerical identifier or signature (Saxby, 2013).</p> <p>Digital IDs are potentially providing a transformative solution to the challenge of many citizens in developing countries not</p>

	<p>possessing an officially recognized ID. Leveraging, inter alia, the extensive use of mobile devices in developing countries, digital IDs allegedly offer the ability to leapfrog the development of paper-based systems and their inefficiencies, to rapidly establish a robust identification infrastructure (World Bank, 2017; World Bank and GSMA, 2016).</p> <p>A person’s digital ID can register a variety of attributes, including amongst others, biographic data (e.g., name, age, gender, address) and biometric data (e.g., fingerprints, iris scans, hand prints). When these data are collected and validated, they can be used to identify a person and thus answer the question “who are you?”. These attributes, along with credentials issued by the service provider, can then also be used as authentication factors to answer the question “are you who you claim to be?”.</p> <p>The attributes and authentication factors used in a digital identity vary depending on context and the type of identity system (World Bank and GSMA, 2016).</p>
<p>Digital Identity Systems</p>	<p>Refers to the processes and systems managing the lifecycle of individual digital identities (World Bank and GSMA, 2016), shaped by the contextual social and political dynamics (USAID, 2017). The lifecycle includes three fundamental steps: <b>a) registration</b>, including enrolment and validation, <b>b) issuance</b> of credentials, and <b>c) authentication</b> for service delivery or transactions (World Bank, 2017):</p> <p style="text-align: center;"><b>A) Registration</b></p> <p>The registration of the identity owner (in this case, the human affected) by the identity/attribute provider marks the start of the life cycle. How and which identity attributes are recorded have implications for how useful, interoperable and trustworthy the system is to/compared with other identity systems (World Bank, 2017).</p>

Registration consists of enrolment and validation, answering the question “who are you?” (see above in “Digital Identity”) (World Bank and GSMA, 2016).

Enrolment itself usually includes several processes. “Identity proofing” firstly links records in a database to a real-world person. This requires matching the record with individual attributes sufficiently unique and stable for ensuring that the match remains valid over time. Each digital ID system normally requires a specific set of information to prove one’s identity. Many digital ID systems rely on so-called “breeder documents”, e.g. birth certificates and build upon birth registries or similar population databases (USAID, 2017).

After a person has claimed an identity during enrolment, this identity is validated by checking the attributes presented against existing data (World Bank, 2017). The validation process thus establishes whether the claimed identity exists and is unique (World Bank and GSMA, 2016).

“De-duplication” ensures the uniqueness of each identity in the system. Hence, enough must be known about each enrollee to create differences from every other individual enrolled. This requires collecting several pieces of information, for example, name, birthdate, and mother’s name, or biometrics for providing additional uniqueness in combination with biographical data (USAID, 2017).

### ***B) Issuance***

Subsequently, completing the exchange between and individual and the ID-provider during enrolment, a registered identity goes through an issuance/credentialing process, before it can be used. Traditionally, ID issuers provide ID holders a new ID token, e.g. documents (e.g., a birth certificate) or credentials (e.g., (e)IDs,

(e)Passports), which can be used to assert one’s identity (USAID, 2017; World Bank and GSMA, 2016).

Individuals thus entrust the provider with their personal data, and in return, they are given a credential proving they have been counted by the institution (USAID, 2017).

### **C) Authentication**

After registration and credentialization, persons can use their attributes in the digital identity along with the credentials to access the associated benefits and services or to transact (USAID, 2017; World Bank and GSMA, 2016).

After she or he presents ID credentials, an authenticator queries the ID database to confirm that her or his assertion matches the information linked to the credential at enrolment (USAID, 2017).

In a secure authentication, two tokens are normally used together, a public and a private one. Public tokens can be seen as analogous to a username; they can be shared with everyone. Private tokens are like a password and used for proving legitimate ownership of a public token (USAID, 2017). Authentication typically further involves a combination of three types of credentials: Something one has – e.g., an ID card or registered SIM card, something one knows – e.g., a PIN or password and something one “is” – e.g. biometrics (USAID, 2017; Levin et. al, 2015).

The use of data during authentication processes differs from enrolment, it is only necessary to check whether a given set of credentials exists in the database without a de-duplication process. As a result, authentication typically requires less information than enrolment (USAID, 2017).

Once the ID system has confirmed that the ID tokens presented is matching a known individual in the database, service providers determine which services the authenticated person is authorised

to access (such as withdrawing cash) (USAID, 2017). To access these, the user must be authenticated using one or more authentication factors to answer the question “are you who you claim to be?” (World Bank, 2017; World Bank and GSMA, 2016).

According to World Bank and GSMA (2016), ID ecosystems (referring to the broader ID environment of a particular context in which there may be multiple ID systems, according to USAID (2017)) can be loosely categorized into four types dependent on different cultural, legal, and political approaches to national identity management. These types vary based on whether they are provided by the public or by the private sector and the degree of centralization:

- i) **Government-driven centralized system.** Individuals’ identity attributes are stored in one or more government-owned database(s), state-issued eID are the basis for all/most digital transactions for both public and private sector (e.g., Belgium, Germany, Italy, Pakistan, Malaysia). The official e-ID can be a basis for verifying other digital identities, e.g. banking and mobile phone credentials.
- ii) **Semi-centralised, “federated” system** of multiple, government-endorsed digital identity providers (e.g., Sweden, Finland, UK, Australia). Here, citizens are free to choose between multiple trusted identity providers (e.g., banks, mobile operators, etc.), for using their credentials to access a broad range of public and private digital services. This can be performed via an identity hub/gateway facilitating authentication across multiple platforms. The private sector often plays a key role as Digital ID provider, after governments provide breeder documents (e.g. birth certificates) as an official basis of identification. The public sector may also supply trusted identity providers. Further, the

	<p>government still has a crucial position in defining and regulating the identity framework as well as endorsing providers.</p> <p>iii) <b>Decentralised, open identity system</b> without any national scheme (e.g., USA). In such a system, public and private sector organisations create, utilize and manage their own digital interoperable identities based on a self-regulated framework. This system has not yet been utilized in the context of a developing country, due to lack of credible national identification and low birth registration rates.</p> <p>iv) <b>Self-asserted Digital ID ecosystem.</b> Here, users choose their own digital identity attributes, and no verification against official identity documents is required. At the time of writing (World Bank and GSMA, 2016) there were no example of countries having considered this approach to provide access to their digital services, this type of ecosystem was rather driven by the largest internet players (such as Facebook, Google etc.).</p> <p>Most identity management systems are currently based on a centralised or federated model (Malik and Mittal, 2017).</p> <p>However, the categorization into the various digital identity systems is disputed. Allen (2016) for example, categorizes them into centralized identity, federated identity, user-centric identity, and self-sovereign identity.</p> <p>Also refer to terms “Self-Sovereign Identity” and “User-centric identity” in glossary.</p>
Disaster	<p>According to the United Nations Office for the Coordination of Humanitarian Affairs (2008, p. 19), a disaster is a “serious disruption of the functioning of a community or a society causing widespread human, material, economic or environmental losses</p>

	which exceed the ability of the affected community or society to cope using its own resources”.
Distributed Ledger Technology	A distributed ledger (technology) is a shared, replicated and synchronized digital data consensus spread across multiple nodes. Central administrators or centralized data storages are not required, making DLT more resistant to e.g. fraud or cyberattacks. Therefore, peer-to-peer networks are set-up as well as consensus algorithms to ensure replication across the nodes of the network. One form of distributed ledger design is the blockchain system (GSMA, 2018).
Due Diligence	Due diligence can be described as a careful investigation of a business or person before a contract is signed, or more generally as an act with a certain standard of care before an agreement is reached (Investopedia, N.D.)
E-Cash	Any electronic substitute for cash that provides full, unrestricted flexibility for purchases. It can be stored, received and spent through, inter alia, a mobile phone, prepaid ATM/debit card or other form of electronic transfer device (CaLP, 2017).
E-Transfer	A digital transfer of money or vouchers from the implementing agency to a human affected relying on digital payment systems (Grossman and Nelson, 2014). E-transfers provide access to cash, goods and/or services through mobile devices, electronic vouchers, or cards (e.g., prepaid, ATM, credit or debit cards). “E-transfer” is an umbrella term for e-cash and e-vouchers (CaLP, 2017).
E-Voucher	A card or code that is electronically redeemed at a participating distribution point, over e.g. the internet or a mobile data device (CaLP, 2017; Sossouvi, 2013). E-vouchers can represent either cash or commodity value (CaLP, 2017).  Each transaction is authenticated at the time of purchase in the system, thus less reconciliation-time is spent when compared to

	paper vouchers (Sossouvi, 2013). For more information on vouchers, refer to according term in glossary below.
E-Wallet	<p>Software that resides on a smart card or mobile phone SIM card and holds or can receive electronic cash and a digital signature (CaLP, 2017).</p> <p>According to the Reserve Bank of India (2017), e-wallets, such as mobile wallets, can be closed, semi-closed and open (see terms closed-loop and open-loop in glossary). Aligning with the definition of a closed-loop payment system, closed wallets issued by a company allow only for paying for in-house services and goods and carry not the advantage of cash withdrawal or redemption (Reserve Bank of India, 2017). A semi-closed wallet can be used for goods and services, including financial services, at selected merchant locations or establishments that have a contract with the issuing company to accept these payment instruments, but do not permit cash withdrawal or redemption by the holder as well (Reserve Bank of India 2017). Open wallets, on the other hand, can be used for purchase of goods and services, including financial services such as funds transfer at any merchant location or PoS terminal, and also cash withdrawals at e.g. ATMs (Reserve Bank of India, 2017).</p>
Effectiveness	Effectiveness relates to how well outputs are converted to outcomes and impacts (Hodges, White and Greenslade, 2011).
Efficiency	Efficiency refers to the ability of a programme to achieve its intended objectives at the least cost possible in terms of use of inputs (CaLP, 2017).
Enabling Environment	The environment and rules that influence how a market system works (CaLP, 2017).
Financial Inclusion	Financial inclusion is defined as access and the ability to use affordable financial products and services entailing transactions, payments, savings, credit and insurance, delivered in a

responsible and sustainable way in a well-regulated environment (World Bank, 2018 and Grossman and Nelson, 2014). Promoted as playing a crucial role in reducing extreme poverty and inequality as well as supporting a transformative, sustainable development (World Bank, 2018; El-Zoghbi, 2016; Park and Mercado, 2015). Access to financial services enables poor to benefit of a market-based economy, such as by building risk-resilience with saving schemes or permitting credit-based investments in productive assets or human capital (World Bank, 2018; El-Zoghbi, 2016; Arun and Murinde, 2010). At the macro level, financial inclusion is seen as crucial for economic growth and advancing other development priorities such as education or women's empowerment (Costa and Ehrbeck, 2015). Accordingly, apart from financial inclusion being prominently positioned as enabler in eight of the 17 Sustainable Development Goals<sup>49</sup>, do some see financial inclusion as part of social protection promotion (World Bank, 2018; UN-DESA 2015a; Parker, 2010).

However, 1.7 billion adults still not possess a formal bank account, amongst others, due to market failures, weak public policies and/or infrastructure (Demirgüç-Kunt et al., 2018; Gardeva and Rhyne, 2011).

In that sense, especially in the context of developing countries, new technologies play a major role to overcome current obstacles and thus can significantly enhance financial inclusion (Demirgüç-Kunt et al., 2018; World Bank, 2017; Haahr, M., 2017). The success of mobile banking in e.g. Kenya has shown, that developing countries have the potential to leapfrog many steps of previous infrastructural and technological developments in industrialized nations (Haahr, 2017).

There is however still more than a fourth of the adult population not having access to a formalized bank account. These

<sup>49</sup> Namely in SDG 1, 2, 3, 5, 8, 9, 10 and 17.

	<p>individuals are oftentimes forced to turn to informal, oftentimes less efficient, solutions (Campos and Coricelli, 2010), such as storing cash home or with friends (Morduch, 1993). The isolated effect of providing a formal bank account to these individuals would be a significant reduction in risk and costs associated with informal solutions while granting access to financial services, such as savings, which is increasing the poor’s productive investments and savings behaviour (Campos and Coricelli, 2010; Morduch 1999).</p> <p>Oftentimes, the unbanked cannot access a formal account, because of a lack of governmental or banking (infra-)structure, or because of not possessing formal IDs (World Bank, 2018; Gardeva and Rhyne, 2011).</p> <p>Financial inclusion efforts hence usually focus on increasing access to formal financial services (services offered by regulated entities) to poor and underserved communities (Grossman and Nelson, 2014).</p> <p>Being able to have access to a transaction account and therefore to store, send and receive money, is seen as a first step toward broader financial inclusion (World Bank, 2018). Accordingly aims the World Bank at a global universal access to a transaction account at 2020 (World Bank, 2018).</p>
Financial Service Provider (FSP)	An entity providing financial services, which may also include e-transfer services. In CBA-related literature, FSP generally refer to those providing according transfer services (CaLP, 2017). FSPs may include e-voucher companies, financial institutions (e.g. banks and microfinance institutions) or mobile network operators (MNOs), depending on the context.
Humanitarian Assistance	“Aid” that seeks, to save lives and alleviate suffering of a crisis-affected population. Humanitarian assistance must be provided in

	<p>accordance with the basic humanitarian principles of humanity, impartiality and neutrality (UN-OCHA, 2008).</p> <p>Various intergovernmental (e.g. the UN and its implementing organisations, such as the WFP, UNHCR and UNICEF) and religious institutions, NGOs and the International Committee of the Red Cross (ICRC) and donor government are providers of humanitarian assistance (Bailey and Harvey, 2015). Many have specific mandates (refer to according term in glossary) and missions about the types of assistance provided and the individuals whose interests they seek to protect (e.g. children and refugees). These entities aim to complement or even substitute for national and local efforts to assist and protect populations suffering the consequences of natural disasters and conflicts (Bailey and Harvey, 2015).</p> <p>Usually, disaster response occurs on a local level. In cases where local and national capacities are exhausted and a state (usually) requests external assistance, international humanitarian interventions occur (Bailey and Harvey, 2015).</p>
<p>Humanitarian- Development Nexus</p>	<p>One sense of humanitarian mandate (refer to according glossary entry below) distinguishes between humanitarian and developmental goals. Some institutions are having a “multi-mandate”, meaning that they respond to humanitarian crises as well as the broader long-term crisis of poverty, human development and social justice (Bradley and Slim, 2013). As humanitarian interventions are often required over decades, oftentimes addressing needs going beyond people affected’s immediate survival (Schmitz Guinote, 2018), protracted crisis is making multi-mandate programming increasingly common, the long continuity of crises makes doing both humanitarian and development work inevitable (Bradley and Slim, 2013).</p> <p>On a broad level, these concerns about long-term impacts of humanitarian assistance, can be situated in a re-surfaced</p>

discussion around a “humanitarian-development nexus”. Stemming from the increased occurrence of protracted crisis, seeking linkages between (short-term) humanitarian and (long-term) development efforts has gained attraction in recent years ((United Nations Development Programme [UNDP] Europe, 2018; UN-OCHA, 2017).

With these extended time commitments, extended ethical responsibilities and an organic moral to move towards developmental values become a necessity. Mandate expansion then becomes compulsory, also for single mandate organisations, creating an ethical problem between the original mandate of providing life-saving assistance and the required promotion of measures avoiding future crises. Thus, the nexus between emergency response and tackling structural inequalities thickens, or, the nexus between humanitarian action and development. This thickening of responsibilities and obligations is especially an issue for indigenous organisations, such as local NGOs and the Red Cross/Crescent societies, which cannot leave a crisis-context, as they are part of the society in crisis. Unlike exogenous NGOs, they thus experience entrenched staying dilemmas. These are usually resolved by taking on more responsibilities, and not less (Bradley and Slim, 2013).

In that sense, is not only cash-delivery itself considered as an important corner stone to bridge the nexus’ divide as a humanitarian agency, but also the provision of financial services (El-Zoghbi, 2017; El-Zoghbi et. al, 2017).

The humanitarian-development nexus then is often perceived as a pathway towards development, and ultimately towards peace (Schmitz Guinote, 2018). However, arguably, the responsibility for development lies eventually in the hands of a government. Eventually, a humanitarian’s responsibility for delivering assistance impartially, independently and neutrally might very

	<p>well stand in conflict to these longer-term development goals and strengthening governmental structures (Schmitz Guinote, 2018).</p>
<p>Humanitarian Information Management (and Exchange) Principles</p>	<p>Based on UN-OCHA (2002).</p> <p>Timely, accurate information is recognized as integral part of humanitarian action in both natural disasters and complex emergencies. The international humanitarian community's ability in collecting, analysing, disseminating and acting based on key information is regarded as fundamental to effective responses.</p> <p>Therefore, the following operational principles to guide information management and exchange activities were formulated:</p> <ul style="list-style-type: none"> <li>i) <b>Accessibility.</b> Humanitarian information and data should be made widely accessible to all humanitarian actors over a variety of channels.</li> <li>ii) <b>Inclusiveness.</b> Information management and exchange should be based on a collaborative system with a high degree of participation and ownership by multiple stakeholders, especially representatives of the population affected.</li> <li>iii) <b>Inter-operability.</b> All sharable data and information should be made available in formats that can be easily retrieved, shared and used by humanitarian actors.</li> <li>iv) <b>Accountability.</b> Reliability and credibility of data and information should be evaluable by knowing its source.</li> <li>v) <b>Verifiability.</b> Information should be accurate, consistent and based on robust methodologies, validated by external sources.</li> <li>vi) <b>Relevance.</b> Information should be practical, flexible, responsive, as well as driven by operational needs to support of decision-making.</li> <li>vii) <b>Objectivity.</b> Information should entail a variety of sources during collection and analysis.</li> </ul>

	<p>viii) <b>Humanity. Information should never distort, mislead or cause harm to affected or at-risk populations and respect the dignity of victims.</b></p> <p>ix) <b>Timeliness.</b> Information should be kept up to date.</p> <p>x) <b>Sustainability.</b> Humanitarian information and data should be preserved, catalogued and archived for future use.</p>
<p>ID2020 Alliance</p>	<p>“The ID2020 Alliance is a global partnership committed to improving lives through digital identity. This alliance of governments, NGOs and the private sector will work to ensure that the technology development is informed by the needs of countries and individuals and that policies and standards reflect the latest technological innovations. By coordinating funding for identity and channeling those funds towards high-impact projects, this alliance model enables diverse stakeholders - UN agencies, NGOs, governments, and enterprises - to pursue a coordinated approach and creates a pathway for efficient implementation at scale” (ID2020, 2019).</p>
<p>Identity</p>	<p>Defining a social construct such as identity with a single definition, risks omitting characteristics crucial to some contexts the definition of identity takes place.</p> <p>According to Fearon (1999), an “identity” can either refer (i) to a social category, defined by membership rules and (alleged) characteristic attributes or expected behaviours, or (ii) socially distinguishing features that a person takes a “particular pride” in or views as immutable but socially consequential, or (i) and (ii) at once. In the latter sense, according to Fearon (1999), a modern formulation of dignity, pride, or honour are implicitly linked to the conception of identity.</p> <p>Thus, for this thesis, an identity in the broader sense shall be described as <b>a collection of attributes uniquely describing an individual or entity</b> (Bansal et. al, 2018; World Bank, 2017a; World Bank 2014), implicitly and explicitly capturing answers to</p>

the question “Who am I?” Koles and Nagy, 2014). These accumulated features play a key role in our societies, Many, such as gender, religion, nationality or poverty level, are of central relevance for development (Clark and Gelb, 2013).

According to World Bank (2014), the role of identity has not changed since the beginning of civilisation, namely the utilisation of identification for determining in which kind and degree of interactions to engage with other individuals. In a narrower sense, identity is hence used for the considerations whom to trust and whom not to. Therefore, identity is closely linked to reputation, defined as what earns an individual trust within the community and thus facilitator of an individual’s actions depending on her or his level of trust (World Bank, 2014). As an individual conduct more actions, the volume of reputational data increases and the level of trust is continuously adjusted through the judgment of the existent social, legal and moral norms of a society (World Bank, 2014). Thereupon, is identity at the core of human-human interactions (World Bank, 2014).

However, in the modern age, are many of the interpersonal interactions digital, oftentimes solely, and thus, nearly anonymous; the relational basis for trust breaks down (USAID, 2017). If relationships exceed an individual’s immediate community, proxy-based systems for establishing trust are becoming critical (USAID, 2017). Such systems therefore often rely on ID tokens (see according term in glossary below) (USAID, 2017).

For establishing a trust-based relationship between an individual and e.g. a government, the process of identification/registration of an “official”, or, “**legal**” identity, where an individual’s identity is “created” and/or recorded by an institution, then becomes important to operate in a structured society (USAID, 2017; World Bank, 214; Clark and Gelb, 2013). “Official identity”, or, “legal

identity” includes both static and mutable characteristics that individuals can use to identify themselves when interacting with (formal) institutions (Clark and Gelb, 2013). Oftentimes, they include name, sex, current address, nationality, familial relationships, place and date of birth, or other information needed to determine individuals’ rights and responsibilities towards these institutions. Because characteristics such as names, birthdays and addresses may be shared by several individuals, official identification normally necessitates unique identifiers - data points or characteristics that are unique to one individual (Clark and Gelb, 2013). This eventually oftentimes results in the issuance of an identity document (ID, see according term in glossary), or an equivalent ID token (Clark and Gelb, 2013), for example, when a registered birth yields the issuance of a birth certificate (Clark and Gelb, 2013).

Currently, most legal identification is provided by or on behalf of governments (World Bank, 2017a). Accordingly, are legal identity systems usually registering and identifying individuals for the provision of government-recognized credentials (see according term in glossary), that can be used as proof of identity, for building trust and decreasing institutional risks (USAID, 2017; World Bank, 2017a; Clark and Gelb, 2013). Legal identification in this sense is unrelated to legal status in the sense of nationality or citizenship (World Bank, 2017a).

These credentials are often inconsistent and not unified by any unique identifier and only reaching a population partially (Decker and Gelb, 2011).

The role of identity and identification and its importance to development outcomes is therefore expressed in the SDG agenda, specifically as one of the proposed SDG targets (16.9)<sup>50</sup>, but also as a key enabler of the efficacy of many other SDG

---

<sup>50</sup> “By 2030, provide legal identity for all, including birth registration“ (UN-DESA, 2015).

	<p>targets, including, amongst others, targets 1.3 (implementation of appropriate social protection systems), 1.4 (gender equality concerning rights to economic resources, as well as access to basic services, property, new technology and financial services and more), 5a and 5b (gender equality in access to economic resources, including finance, and promoting women’s empowerment through ICT), 17.7 (strengthen of domestic tax collection) (Dahan and Gelb, 2015; UN-DESA, 2015a).</p> <p>IDs including ethnicity or religion can and have been used to persecute specific groups of individuals. Conversely, a government’s identifying power can also foster national unity, build trust, and reconcile internal strife (USAID, 2017).</p>
ID Token	<p>An ID token is a portable piece of hardware that individuals carry as trust proxy to support his or her claim to be a particular person. The ID token thus supports to authenticate the claim to access a network, e.g. to engage in a government transaction (USAID, 2017; Techopedia, N.D.). The token supports his or her identity and authenticating him or her for the use of the service, replacing anonymity with a proxy for trust (USAID, 2017). Also referred to as a security token or an authentication token (Techopedia, N.D.)</p>
Impartiality	<p>“Humanitarian assistance must be provided without discriminating as to ethnic origin, gender, nationality, political opinions, race or religion. Relief of the suffering must be guided solely by needs and priority must be given to the most urgent cases of distress” (UN-OCHA, 2008; p. 30).</p> <p>Humanitarian agencies generally strive to meet this principle (Bailey and Harvey, 2015).</p>
Information and Communicatio	<p>An umbrella term including all technologies for the communication of information (IGI Global, 2018). ICTs for financial services</p>

n Technology (ICT)	include, amongst others, ATMs, Smart Cards or telephone banking (Agboola, 2005).
In-kind assistance	Non-cash assistance in form of materials or services (e.g. food or tents), according to the United Nations Office for the Coordination of Humanitarian Affairs (UN-OCHA, 2008).
Know Your Customer (KYC)	<p>KYC usually refers to the information a local regulator requires financial institutions and regulated financial service providers to perform due diligence to identify their customers to discourage financial products being used for money laundering or other crimes.</p> <p>The Financial Action Task Force (FATF, 2012-2018) has made 40 non-binding recommendations designed to assist financial institutions to tackle money laundering and financing of weapons and terrorism. Know Your Customer (KYC) standards are normally derived from the FATF Recommendations (Levin et. al, 2015). Financial institutions that operate in countries that have adopted the FATF recommendations through relevant legislation must abide by these laws (Levin et. al, 2015). Financial institutions that are based in or operate in countries that do not have any relevant laws may have nevertheless put in place KYC standards, due to above concerns. Furthermore, the KYC standards have become an international standard that all financial institutions, and especially international financial institutions, are expected to put in place (Levin et. al, 2015).</p> <p>In established banking environments, regulators are normally required to monitor and reduce risks caused by the activities of financial service providers. However, in a lot of countries in which mobile money is operating, regulators are also determined by the objective of extending banking and financial services to the unbanked, thus, promoting financial inclusion. Financial inclusion</p>

	<p>then becomes part of their institutional mandate, or a unit in their regulatory institution (Buckley et. al, 2015)</p> <p>Some countries thus allow lower levels of information for accounts that they deem to be “low risk” (CaLP, 2017; GSMA, 2017 FATF, 2012-2018). This can be e.g. due to the lack of formal identity documents in some markets. Solutions such as tiered KYC (e.g. restricting deposit limits) and adjusting acceptable (“simplified”) KYC documentation can then help to facilitate increase financial inclusion, especially in rural areas (GSMA, 2017).</p> <p>The simplified KYC procedure is compliant with the FATF, which recommends balancing the objectives of financial inclusion and integrity and to adopt proportional risk-based CDD procedures (FATF, 2012-2018; Buckley et. al, 2015).</p>
Marginalized Populations	<p>Marginalised populations are defined as those excluded from the mainstream social, economic, cultural, or political life. Examples are, amongst others, groups excluded due to race, religion, age, gender, political, cultural, or financial status (Given, 2007).</p>
Magnetic Strip Card	<p>A plastic card with a magnetic stripe able to store data using magnetic particles on a band on the card and secured by PIN, signature or biometrics to verify the identity of the recipient before granting access to funds (CaLP, 2017).</p>
Mandate	<p>Based on Bradley and Slim (2013).</p> <p>In the humanitarian sphere, this term des- and proscribes the different kinds of legitimacy, mission and values held by the wide variety of organisations engaged in humanitarian actions in armed conflict and disaster. The mandating of agencies refers to three different dimensions: i) a legal dimension; ii) a technical or demographic specialism, and iii) organisational positions along a spectrum of ethical goals:</p> <p>i) The legal mandate of an international humanitarian organisations can be categorized into two main types:</p>

	<p>state-mandated or self-mandated. UN organisations, such as UNHCR, UNICEF, WFP, WHO and OCHA, possess international mandates being legally recognized by states. The same applies to the International Committee of the Red Cross (ICRC), the International Federation of Red Cross and Red Crescent Societies, National Red Cross/Crescent Societies. These agencies are described as “state-mandated”. All other agencies tend to be self-mandated as voluntary organisations set up as private initiatives seeking public support. Self-mandated agencies are usually registered, recognized and regulated by states to differing degrees but do not carry a formal international mandate. This first sense of the term mandate reflects an idea of international legitimacy grounded in the power of either states or civil society.</p> <p>ii) The technical mandate of an organisation refers to its field of professional practice and the demographic target group. An agency’s specialism can be very specific and focus on e.g. children and health, or civilians and human rights, or multi-mandated, for example, if the organisation focusses on poverty and social justice in general and thus covers a wide variety of demographic groups and/or technical specialisms.</p> <p>iii) The third form of mandate distinguishes between humanitarian and developmental goals. While for example the ICRC is regarded as having specifically a “single-mandate”, working only with an emergency humanitarian mission based in international humanitarian law and humanitarian principles, other institutions are seen as having a “multi-mandate”, meaning that they respond to humanitarian crises as well as the broader long-term crisis of poverty, human development and social justice.</p>
--	---

	<p>Protracted crisis is making multi-mandate programming increasingly common, the long continuity of crises makes doing both emergency and development work inevitable. With these extended time commitments, extended ethical responsibilities and an organic moral to move towards developmental values become a necessity. Mandate expansion then becomes compulsory, also for single mandate organisations, creating an ethical problem between the original mandate of providing life-saving assistance and the required promotion of measures avoiding future crises. Thus, the nexus between emergency response and tackling structural inequalities thickens, or, the nexus between humanitarian action and development. This thickening of responsibilities and obligations is especially an issue for indigenous organisations, such as local NGOs and the Red Cross/Crescent societies, which cannot leave a crisis-context, as they are part of the society in crisis. Unlike exogenous NGOs, they thus experience entrenched staying dilemmas. These are usually resolved by taking on more responsibilities, and not less.</p>
<p>Market-based Approach</p>	<p>Generally, the narratives around financial inclusion and “the unbanked” follow a market-based approach, targeting at the inclusion of those who were not able to benefit from a market-driven development dynamic (Costa and Ehrbeck, 2015). In principle, this approach assumes that when the marginalized are included in the formal capital markets by combatting market inefficiencies due to external factors, inequality and poverty can be fought (Carant, 2017; Scott, 2016; Stewart, 2009). Here, one firstly critically needs to ask the question, whether financial inclusion is of any good as long as multiple deprivations of marginalized groups prevent them from exploiting opportunities of improved access and adequacy of financial tools (Stewart, 2009;</p>

	<p>Stewart, 2002). Thus, we need to ask, whether financial inclusion really is to be solved solely by searching a profitable technological solution, or whether financial exclusion is an integral part of an unequal economic system (Scott, 2016; Stewart, 2009). Hence the broader question, whether it should really be the end goal, to include marginalized individuals into formal financial markets, or whether the focus should not lie on creating meaningful alternative institutions and systems based on principles of social solidarity (Scott, 2016), and not capitalism.</p>
Merchant	<p>Supplier of goods and services but does not redeem e-transfers for cash (Sossouvi, 2013). They may be contracted by a humanitarian organisation to participate in cash-based interventions. Term can be used interchangeably with vendor and trader (CaLP, 2017).</p>
Mechanism	<p>Means of delivering a cash or voucher transfer, e.g. by smart card, mobile money, “hard” cash, etc. (CaLP, 2017).</p>
Mobile Banking	<p>The ability to access a bank account and conduct transactions using a mobile phone as channel (CaLP, 2011).</p>
Mobile Money	<p>Mobile money refers to the ability of using a mobile phone on a mobile network for conducting financial and commercial transactions such as cash deposit, withdrawal and payments (Sossouvi, 2013) and (potentially) a range of non-transactional financial services (Grossman and Nelson, 2014). It is a paperless version of a national currency that can be used to provide humanitarian e-cash payments (CaLP, 2017).</p> <p>Mobile money is issued by an “e-money issuer”; usually a telecommunication company or sometimes a regular bank. The exact terminology varies across countries and literature, but e-money is commonly defined as a type of stored value instrument or product that:</p> <p>i) is issued on receipt of funds;</p>

- ii) consists of electronically recorded and stored value on a device
- iii) may be accepted as a means of payment by other parties than the issuing party;
- iv) is convertible back into cash

Customers then can make payments and transfers by sending short message service (SMS) mobile notifications to each other (Buckley et. al, 2015)

Unlike mobile tokens and mobile vouchers, mobile money requires subscription to a mobile wallet account, where value is stored. The account is linked to a specific SIM card or hosted on a technology platform that creates a link (via USSD or SMS) with the mobile handset based on the telephone number (Sossouvi, 2013).

Mobile money is the most complex form of mobile transfers. Depending on context and maturity of the service, it provides recipients with the widest range of transactional capabilities and broader access to basic financial services (Sossouvi, 2013). Thus its proponents argue for mobile money's potential of reducing poverty and increasing financial inclusion.

Mobile money users need to have constant access to a phone and to a SIM card that can be linked back to them for the duration of the programme. A mean of authentication is always required to grant access to the e-wallet, and initiate transactions. Vendors and agents need to access at least a basic phone (Sossouvi, 2013).

Mobile money is a hybrid service, createing novel regulatory challenges, as it enables a variety of non-banks to perform functions of traditional banks (Buckley et. al, 2015), usually resulting in an overlap of several regulatory authorities, e.g. the banking sector, the telecommunications sector, and financial

	<p>intelligence units (FIUs)) dealing with anti-money laundering (Madise, 2014).</p> <p>Often used synonymously with the term “mobile financial services” (Grossman and Nelson, 2014).</p>
Mobile Phone Penetration	<p>Refers to the number of SIM cards or mobile phone numbers in a certain country, it does not refer to the number of mobile phone devices (Infobip, 2018). This information is represented by the mobile phone penetration rate which shows the number of SIM cards used in a given country (Infobip, 2018). There however is a significant difference between the number of SIM cards and actual individuals (unique subscribers) using mobile phones, mostly due to multiple SIM-ownership (George et. al, 2016).</p>
Mobile Token/Mobile cash voucher	<p>Mobile tokens are a form of mobile transfer used to collect cash only. They are a unique authentication code that can be activated only once to release payment at an authorised agent. This authentication code, known only to the receiver, effectively plays the function of a PIN to unlock cash payment (similar to a Western Union tracking number to receive a money transfer). Receivers of mobile tokens must have access to a SIM card and are required to collect the full amount that was sent to them, as residual value cannot be stored on the system. Agents need to have access at least a basic phone to process cash collection (Sossouvi, 2013). The term mobile token is used interchangeably with mobile cash-out voucher (GSMA, 2017).</p>
Mobile Transfers	<p>Mobile transfers are a form of e-transfer occurring over the mobile network. Mobile phones for e-transfers significantly reduce the need for additional hardware and equipment such as cards, PoS terminals, etc. (Sossouvi, 2013). Mobile transfers have three different forms, mobile tokens, mobile money and mobile vouchers. See according terms in glossary.</p>

Mobile Vouchers/Mobile Voucher for Goods & Services	Mobile vouchers are a type of mobile transfer for redeeming goods or services, but not for collecting cash. They are created on a dedicated software system and redeemed at authorised transaction points using some form of authentication. Unlike with mobile tokens, residual value can be stored on the system. Human affected hence have greater flexibility in redeemable amounts and the number of purchases. Recipients of mobile vouchers do not always need to have access to a SIM card but always need to have a mobile voucher number and e.g. a PIN to authenticate transactions. Merchants need to have access to at least a basic phone to process purchase transactions (Sossouvi, 2013). The term is used interchangeably with mobile voucher for goods and services (GSMA, 2017).
Modality	Form of transfer (cash, vouchers, in-kind, or combination) of humanitarian intervention (CaLP, 2017).
Mobile Network Operator (MNO)	A service provider offering mobile network coverage and related products and services (Sossouvi, 2013). In both investigated contexts, Malawi and Kenya, MNOs offer mobile-based payment systems, such as Safaricom's M-Pesa in Kenya, or Telekom Network Malawi.
M-Pesa	Kenya's incumbent mobile money system. For more information, refer to various parts of Appendix 6.
Multisector Cash Transfer	A coordinated approach to CTs whereby a range of sector would need to be addressed through CTP by one or a range of organisation(s) working together, possibly using one delivery mechanism, but otherwise managing their program with their own targeting, cash amounts, etc. (CaLP, 2017).
NFC	Near Field Communication (NFC) devices can be used for contactless payment, with e.g. a credit card (Sossouvi, 2013).

Open-Loop	<p>In a broader sense, an “open” payment infrastructure can be accessed by all transactions accounts providers, within the regulated<sup>51</sup> realm (Benson et. al, 2018). Thus, “open-loop” refers to a payments network enabling otherwise closed-loop payment systems to share endpoints (Blake et. al, 2016). Therefore, an individual can utilize the systems’ device not only at the issuing entity’s endpoints. Ideally, they connect recipients with a personal account / e-wallet that leverages already existing local markets and ecosystems (Blake et. al, 2016; Cornish, 2016).</p> <p>A simple example would be a card-based payment system, say a Visa Card, enabled to be used at another bank’s proprietary ATMs (Blake et. al, 2016; Cornish, 2016). Ideally, such a system results in an inclusive payment infrastructure. When the payment infrastructure is both open and inclusive, it drives digital payment volumes (Benson et. al, 2018).</p> <p>In the context of the Barcelona Principles (see according term in glossary), open-loop systems refer to “payment systems that <b>enable recipients to store value, withdraw cash, purchase items, or perform a variety of other transactions</b> based on what the digital payment mechanism being used allows for” (Global Innovation Exchange, 2016, p. 3). Also referred to as “mainstream financial accounts” (Bold et al., 2012, pp. 3, 4). In the humanitarian context, they have been utilized in post-disaster or conflict recovery programmes to rebuild local economies (Cornish, 2016).</p> <p>In contrast to closed-loop, open-loop payment systems thus <b>allow more flexibility and choice for recipients and access to further financial services</b> (Ford, 2017, Cornish, 2016).</p>
-----------	--

---

<sup>51</sup> “regulated” in this sense implies, that the providers meet the minimum standards and requirements related to risk management imposed by the regulators and payment system operators (Benson et. al, 2018).

	<p>They work most effectively if they already have broad acceptance from local merchants and financial institutions (Cornish, 2016).</p> <p>They however generally <b>reduce transparency</b> for the intervention as it is difficult to verify exactly how funds have been spent (Ford, 2017), thus being potentially inadequate if organisations require detailed spending-reporting (Cornish, 2016). Additionally, there are <b>considerable Know Your Customer (KYC)-regulation and identification requirements</b> associated with these systems. Therefore, they are <b>not regarded as practical in crises, where speed of response is crucial</b> (Ford, 2017).</p> <p>There are many hybrids between fully closed and fully open-loop systems (Ford, 2017).</p>
P2P	Person-to-Person transfer (also referred as “one-to-one”) (Grossman and Nelson, 2014).
Personal Identifiable Information (PII)	Any data potentially identifying a certain individual. Any information enabling to distinguish one individual from another, or data for de-anonymizing anonymous data (Rouse, 2016).
PIN	Personal identification numbers generated through a coding system which makes each PIN unique.
Point of Sale (PoS)	E.g. a retail or mobile location where payments are made for goods or services. PoS-devices do not contain money but have the capability of performing transactions (CaLP, 2017 and GSMA, 2017).
Privacy-By-Design (PbD) Principles	<p>Based on Cavoukian (2009), aiming to establish the globally highest standard in the area of data protection/privacy:</p> <p>i) <b>Proactive not Reactive; Preventative not Remedial</b> – Proactive rather than reactive measures should be</p>

	<p>undertaken, anticipating and preventing privacy invasive events before they happen.</p> <ul style="list-style-type: none"> <li>ii) <b>Privacy as Default Setting</b> - No action should be required of an individual to protect his or her privacy, it should be built into the system, by default. Specifically relating to purpose specification, data minimalization, collection, use, retention and disclosure limitation of information.</li> <li>iii) <b>Privacy Embedded into Design</b> – Privacy as core function of e.g. IT, not as an add-on.</li> <li>iv) <b>Full Functionality; Positive-Sum, not Zero-Sum</b> - PbD should accommodate all legitimate interests and objectives in a positive-sum “win-win” manner, not through a zero-sum approach, with unnecessary trade-offs. PbD should avoid the pretence of false dichotomies, e.g. privacy vs. security, demonstrating that it is possible, and far more desirable, to have both.</li> <li>v) <b>End-to-End Security; Full Lifecycle Protection</b> – PbD should be continuously embedded throughout the complete life-cycle of the data in question.</li> <li>vi) <b>Visibility and Transparency</b> – All involved stakeholders should be subject to independent verification. Its Operations should be visible and transparent, to both users and providers alike.</li> <li>vii) <b>Respect for User Privacy</b> – Interfaces should be human-centred, user-centric and user-friendly so that informed privacy decisions may be reliably exercised, the data protection of the individual should be centre of all considerations and operations.</li> </ul> <p>Not many of the humanitarian information management systems currently incorporate privacy-by-design considerations (van der Veen et. al, 2018, Levin et. al, 2015).</p>
--	---

Protracted Crises	Protracted crises are defined as environments with a significant proportion of the population acutely vulnerable to death, disease and disruption of livelihoods over a prolonged period of time (Food and Agriculture Organisation, 2010).
Red Rose	<a href="https://www.redrosecps.com/about">https://www.redrosecps.com/about</a>
Restricted Transfer	Requires utilizing (humanitarian) assistance to access specific, pre-determined goods or services. Vouchers are by default restricted transfers (CaLP, 2017).
Self-Sovereign Identity (SSI)	<p>Moving from centralized over federated to a decentralised ecosystem, self-sovereignty marks the newest type of a Digital ID ecosystem and is about entities or individuals owning and controlling their own digital ID (Allen, 2016). Due the weaknesses of centralized and federated ID solutions (dependence on third-parties in willingly issuing IDs, security and data risks, lack in interoperability, individual’s control and consent etc.) identity systems” above), and the emergence of blockchain-technology, the concept of self-sovereign identity (SSI) is becoming more popular (Stevens, 2018; Juden and Pisa, 2017; USAID, 2017). Blockchain technology may finally provide the required underlying software-architecture for enabling SSI, which was not deemed possible before (Juden and Pisa, 2017). According to Allen (2016), Rosenfield’s (2012) “What is ‘Sovereign Source Authority’?” blogpost marks one of the first references to an SSI. In his text, Rosenfield describes that individuals have an established right to identity, prior to a formal registration process. This registration process, currently in the hands of governments, would conflict with this natural right to identity, as it would imply that an administration process controlled by society is required for "identity" to exist, thus destroying individual sovereignty.</p> <p>The concept of SSI thus is the next step beyond user-centric identity (refer to according term), with the same starting point: the</p>

user must be central to the administration of identity (Allen, 2016). That requires not only interoperability of an individual's identity across multiple locations, with the individual's consent, but also true user control of that digital identity, creating user autonomy (Allen, 2016).

In contrast to centralised systems, in which ID credentials are issued by institutions, SSIs are meant to empower individuals to control the formalisation of their identities and actively manage their personal data.

Due to a so far absent universal definition of SSI (Allen, 2016), it is disputed in literature, whether self-sovereign identity needs to be self-asserted. Windley (2016) defines an SSI as necessarily being self-asserted, while some see it differently (GSMA, 2018; van der Veen et. al, 2018). In the humanitarian context, it would oftentimes make sense, to e.g. have an assistance worker supporting an e.g. illiterate individual in the process of self-registering (van der Veen et. al, 2018), while still giving the individual the control and access in the broader sense. Whether self-asserted or with the support of another party, eventually, self-reported claims will need to be verified (Windley, 2016), e.g. by the humanitarian organisation, or, in the simplest form, by an appointed member of the community (van der Veen et. al, 2018).

In absence of an exact definition of SSI, and which principles it should adhere to, Allen (2016) defines ten principles to be fulfilled for satisfying the central aspect of an SSI – user's control:

- i) **Existence:** An independent existence of users is required; in limited form, an SSI makes already existing aspects of an identity available and accessible to the public.
- ii) **Control: Users must ultimately control their identities,** control in that sense means the ability to refer to it, update it or hide it. This however does not

	<p>imply they have to control the claims or credentials about their identity issued by others.</p> <p>iii) <b>Access:</b> Users must have access to their own data. This does not entail that a user can modify all the claims associated with his or her identity, but they should be aware of them. Further, it does not mean that a user has equal access to others' data, only to his/her own.</p> <p>iv) <b>Transparency:</b> Systems managing identities must be transparent to the user, so he/she can understand how they function and how they are managed. Algorithms must be free and open-source.</p> <p>v) <b>Persistence:</b> identities must be long-lived, without the <b>“right to be forgotten” (see GDPR)</b> being forfeited.</p> <p>vi) <b>Portability:</b> information and services about identity must be transportable and not held by a singular entity. This means that also if issuers or identity providers change or disappear, the identity should continue to be usable.</p> <p>vii) <b>Interoperability: Identities should be as widely usable as possible</b> (the author assumes, KYC-alignment is covered by that statement, as DLT provides significant advantages for specifically interoperability for KYC-purposes (GSMA, 2018))</p> <p>viii) <b>Consent: Users must consent to the use of their identity.</b></p> <p>ix) <b>Minimalization:</b> Disclosure of claims must be minimised. This can be done by e.g. zero knowledge techniques, such as giving an age range without disclosing the actual year, when age is asked for.</p> <p>x) <b>Protection: The freedoms and rights of the users must be protected before the network's interest.</b></p>
SIM	The Subscriber identification module (SIM), is an integrated circuit securely storing data for identifying and authenticating

	subscribers on mobile telephony devices. The circuit is embedded on a small card, commonly known as SIM card (Sossouvi, 2013).
Social Safety Nets	A sub-set of broader social protection systems, consisting out of non-contributory transfers (in-kind, cash or vouchers). They can be provided conditionally or unconditionally (CaLP, 2017).
Smart Card	Includes an embedded integrated circuit being either a secure microcontroller or equivalent intelligence with internal memory or memory chip alone. The card can be connected to a reader with direct physical contact or with a remote contactless radio frequency interface. With an embedded microcontroller, smart cards can store large amounts of data and carry out own functions such as encryption and mutual authentication (CaLP, 2017). Smart Cards can be linked to a bank account (thus allowing the potential for further financial access), as funds are stored digitally on it, along with relevant recipient information, making a life connection unnecessary, unless the funds should be topped up (Ford, 2017). Smart cards may therefore be appropriate for rural environments with less well-developed infrastructure, however require a PoS device. Withdrawals can often be made via an ATM (Ford, 2017).
Transaction Point	A location where a(n e-transfer) transaction can be conducted. Not limited to cash collection but also including merchant purchases (Sossouvi, 2013).
Unique identification number (UIN)	A number uniquely identifying individuals. Can be used to link an identity across databases and systems in both public and private sectors. National identity providers may issue a UIN to citizens and residents for their lifetime (World Bank and GSMA, 2016).
Unique Mobile Subscribers	The definition is not restricted to the number of people that possess a mobile phone, but rather the number of people that are subscribed to a mobile tariff or service normally over a SIM card (Gillet, 2014). This is due to the “device sharing phenomenon”,

	<p>meaning that individuals do not necessarily need to possess a mobile phone to become a mobile subscriber (Gillet, 2014). Estimating unique mobile subscribers from registered SIM connections supports in deriving a more accurate picture of mobile penetration (George et. al, 2016; Gillet, 2014), when compared to mobile phone penetration. In 2016, 99% of the global population would be defined as having access to a mobile by regarding the number of SIM-cards, while regarding unique mobile subscribers, only 65% of the global population would be counted as having access (George et. al, 2016).</p>
User-centric (ID)	<p>Rather an approach than a technology, placing ownership of data into the hands of the individual, e.g. by letting him or her choose which data to provide at enrolment, where it is stored and what is revealed during authentication (USAID, 2017). In the humanitarian sphere, a user-centric system means using a digital platform putting people affected at the centre of the design (Ford, 2017).</p>
USSD	<p>Unstructured Supplementary Service Data. A protocol used by Global System for Mobile Communications (GSM) cellular telephones to communicate with service provider's computers. USSD messages create real-time open connections and thus allow a two-way exchange of data sequences. This makes USSD more responsive than services using SMS (Sossouvi, 2013).</p>
Value for money	<p>Refers to the optimal use of resources to achieve the best outcomes for human affected by crises and disasters (CaLP, 2017).</p>
Value Voucher	<p>A value voucher has a denominated cash value and can be exchanged with participating vendors for goods or services of an equivalent monetary cost. Value vouchers tend to provide relatively greater flexibility and choice than commodity vouchers</p>

	but are still necessarily restricted as they can only be exchanged with designated vendors (CaLP, 2017).
Vendor	Supplier of goods/services. They can be contracted by a humanitarian organisation to participate in a cash-based assistance intervention (CaLP, 2017). Term can be used interchangeably with merchant and trader (CaLP, 2017).
Voucher	<p>A paper, token or e-voucher that can be exchanged for a pre-determined quantity or value of goods/services, denominated either in cash value or commodities/services, or a combination of both. They are redeemable with preselected vendors, retail stores, or fairs created by the issuing humanitarian agency. Wide variations in the degree of restriction/flexibility voucher-based programmes provide exist. Therefore, vouchers are a hybrid form of transfer that display features of both cash (value-based vouchers allow for some level of choice) and in-kind transfers (quantity-based vouchers are very similar to a decentralized system of local in-kind procurement) (CaLP, 2017; World Bank, 2016).</p> <p><b>The terms vouchers, stamps, or coupons are often used interchangeably.</b></p>

## Appendix 2: E-transfer Mechanisms

<b>E-transfer delivery mechanism</b>		<b>Description</b>	<b>Min. beneficiary equipment</b>	<b>Infrastructure at the transaction point</b>	<b>Application</b>
Cards	<i>Magnetic stripe card</i>	<ul style="list-style-type: none"> <li>- prepaid plastic cards with a magnetic stripe capable of storing data</li> <li>- HA provides signature or <i>PIN</i> for authentication at <i>PoS</i> or <i>ATM</i></li> </ul>	Card + signature (+ <i>PIN</i> at <i>ATMs</i> )	Vendor with <i>PoS</i> or <i>ATM</i>	Goods/services + cash
	<i>Smart card</i>	<ul style="list-style-type: none"> <li>- plastic cards with embedded chip containing entitlement</li> <li>- can work offline</li> </ul>	Card + <i>PIN</i> , signature or biometrics	Vendor with <i>PoS</i> or <i>ATM</i>	Goods/services + cash
	<i>Contactless card</i>	<ul style="list-style-type: none"> <li>- basically, smart cards tapped on <i>NFC</i>, <i>PoS</i> or modified smartphone</li> <li>- <i>PIN</i> can replace formal IDs for authentication</li> </ul>	Card + <i>PIN</i> , signature or biometrics	Vendor with <i>PoS</i> , <i>NFC</i> or <i>ATM</i>	Goods/services + cash
Mobile transfers	<i>Mobile token</i>	<ul style="list-style-type: none"> <li>- funds are transferred as mobile cash-out voucher</li> <li>- used to collect cash (only) at an <i>agent</i> outlet</li> <li>- residual value cannot be stored on the system</li> <li>- greater spending autonomy than mobile vouchers, but lower choice in whether to cash-out at once or not</li> </ul>	<i>SIM</i> + <i>PIN</i>	<i>Agent</i> with basic phone	Cash
	<i>Mobile voucher</i>	<ul style="list-style-type: none"> <li>- funds are transferred as mobile commodity or service voucher; no cash-out possible</li> <li>- redeemed at authorised transaction points at designated merchants/vendors</li> <li>- residual value can be stored on the system</li> <li>- low purchasing flexibility (closed loop system) but greater freedom in amount redemption</li> </ul>	( <i>SIM</i> ) + <i>Voucher</i> number + <i>PIN</i>	Vendor with basic phone	Goods/services
	<b>Mobile money</b>	<ul style="list-style-type: none"> <li>- Funds transferred from organisation to individual's mobile money account</li> <li>- The recipient thus must be registered for a mobile money account <ul style="list-style-type: none"> <li>- cash-out is possible at a mobile money <i>agent</i> outlet <ul style="list-style-type: none"> <li>- possible to store residual value</li> </ul> </li> </ul> </li> <li>- most complex form of mobile transfers, but potentially provides recipients with the widest range of transactional capabilities and broader access to basic financial services</li> </ul>	<b>Phone</b> + <i>SIM</i> + <i>PIN</i>	<i>Agent</i> with basic phone	Cash + <b>Mobile money services</b> including transactions like <b>money transfers</b> + Goods / services
Vouchers	<i>E-vouchers</i>	<ul style="list-style-type: none"> <li>- can represent cash or commodity value</li> <li>- card or code that is electronically redeemed at a participating transaction point, over e.g. the internet or a mobile data device</li> </ul>	<i>Voucher</i> number + <i>PIN</i>	Merchant with smartphone or computer	Goods/services

Source: Based on GSMA (2017), CaLP (2017), Sossouvi (2013) and CaLP (N.D.a)

### Appendix 3: Elaboration Figure 1

Dimension: Access		
Relates to the availability of the <i>e-transfer's</i> device to the individual (Neil, 2010) and the <b>possibility to formally make use of it</b> . Linked to regulatory, market, and technology environments (World Bank, 2012). Access indicators hence reflect the depth of outreach, such as penetration of <i>point of sale (POS) devices</i> in rural areas (World Bank, 2012).		
Macro-Enablers	Exclusion Factors	Enabling Mechanism Design
Favourable regulatory environment, e.g. (KYC) friendly towards un-identified (Bemo et. al, 2017; Levin et. al, 2015; Al Mahdi, 2015).	<b>Lack of formal ID credentials</b> Lack of formal ID oftentimes means failure to comply with Know Your Customer (KYC)-requirements for payment systems (Bemo et. al, 2017; Al Mahdi, 2015; Sossouvi, 2013).	<b>Humanitarian agency-provided IDs are accepted for KYC-alignment (research question).</b>
Comprehensive hardware penetration, e.g. mobile phone availability to at least one household member (Sossouvi, 2013).	<b>Hardware inaccessible</b> Required hardware inputs inaccessible to the recipient (Zambrano, 2017; GSMA, 2017; Gigler, 2015; Sossouvi, 2013), e.g. no access to mobile phone. Especially prevalent among marginalized and vulnerable individuals in LDCs (International Telecommunication Union, 2018; World Bank, 2016, Minges, 2012)	- Required hardware is pre-provided by the humanitarian agency (Sossouvi, 2013) - Hardware-light mechanism is picked (Sossouvi, 2013)
Expansion of competitive service providers (e.g. competing MNOs); for increased agent & vendor; PoS network; telecommunication and energy regulators, competition authorities (Al Mahdi, 2015);	<b>Limited agent &amp; vendor network</b> Limited agent & vendor network/transaction points and liquidity in e.g. remote areas (Bailey, 2017; Gigler 2015, Sossouvi, 2013) due to e.g. lack of competitive MNOs. Problematic because this indirectly increases (time and transport) costs (Dumas et. al, 2017.; Bailey, 2017).	- Design minimizes required intermediaries (Zambrano, 2017), - Acquiring infrastructure provided by humanitarian agency (Bold et. al, 2012).
Provision of technological infrastructure (Al Mahdi, 2015)	<b>Limited connectivity and electricity</b> Network connectivity, electricity and bandwidth requirements not fulfilled in e.g. remote or crisis affected areas (Bailey, 2017; Dumas, 2017; Ford, 2017 Zambrano, 2017; GSMA, 2017; Gigler, 2015). For example, above a billion individuals do currently not have access to electricity (World Bank, 2017a).	Offline-enabled design (van der Veen et. al, 2018; Bemo et. al, 2017).
Robust household and census data available for e.g. Proxy Means Testing	<b>Targeting</b> Targeting of marginalized is one of the biggest challenges in humanitarian assistance (Bailey and Harvey, 2015a).	- Self-targeting enabled design (van der Veen et. al, 2018)

**Dimension: Appropriateness**  
 Local appropriation of technologies and contextualization of information through *ICT* are key factors determining the impact (Gigler, 2015). “Appropriateness” hence relates to the “meaningful” use of ICTs/e-transfer e-mechanism, where the recipient exercises a degree of control and choice over technology and content to meet his or her needs targeted by the intervention (World Bank 2012; Neil, 2010). A humanitarian intervention is unlikely to yield a sustained use of digital financial services if informal financial services are deemed more appropriate or relevant (Bailey, 2017).

Macro-Enablers	Exclusion Factors	Enabling Mechanism Design
<ul style="list-style-type: none"> <li>- Educational system</li> <li>- Previous exposure of households to mechanism’s hardware and enabled financial services (Bailey, 2017)</li> </ul>	<p><b>Illiteracy</b>            Limited (financial/technological/alphabetical) literacy of marginalized (Zambrano, 2017; GSMA, 2017; Bailey, 2017; Gigler, 2015; Grossman and Nelson, 2014; Sossouvi, 2013). For example, according to Holzmann and Jørgensen (2001), a certain degree of financial literacy is required to use financial instruments in a welfare-enhancing manner. Makes reliance on local intermediaries more likely (Bailey, 2017; Zambrano, 2017).</p>	<ul style="list-style-type: none"> <li>- Several transfer instalments to increase exposure with mechanism’s hardware/financial services (Bailey, 2017)</li> <li>- Illiteracy friendly design</li> <li>- Training to intermediaries or human affected (Bailey, 2017)</li> </ul>
<ul style="list-style-type: none"> <li>- Good governance</li> <li>- Previous exposure to mechanism components etc.</li> </ul>	<p><b>Limited trust</b>            Limited cultural acceptance or trust of/into <i>e-transfer</i>, authentication method or involved intermediaries (Bailey, 2017; USAID, 2017; Gigler 2015; Sossouvi, 2013).</p>	<ul style="list-style-type: none"> <li>- Contextual/local appropriation (Bailey, 2017)</li> <li>- Strong privacy by design</li> <li>- Reliance on trusted intermediaries (van der Veen et. al, 2018)</li> </ul>
<ul style="list-style-type: none"> <li>- Educational System</li> <li>- Safety etc.</li> </ul>	<p><b>Equipment/authenticator loss</b>            Increased risk of equipment loss for marginalized (Sossouvi, 2013), or increased danger of forgetting authentication factors, e.g. PIN (Bailey, 2017).</p>	<ul style="list-style-type: none"> <li>- Recovery mechanisms</li> <li>- biometric authentication or other contextually adequate design</li> </ul>
<ul style="list-style-type: none"> <li>- Competitive service providers</li> <li>- Relative, not absolute fees as standard</li> </ul>	<p><b>Transaction fees</b>            Transaction fees relatively too high for the poorest and vulnerable for long-term use of mechanism (Bailey, 2017; 2013; Barr, 2004), or when vulnerability is exploited by cash agents (Dumas et. al, 2017).</p>	<ul style="list-style-type: none"> <li>- Picking the most adequate service provider</li> </ul>
<p>Data privacy and security standards and practices (Al Mahdi, 2016), consumer protection and empowerment authorities (Al Mahdi, 2016)</p>	<p><b>Data protection issues</b>            Data protection issues due to privacy risks of mechanism (USAID, 2017; Levin et. al, 2015; Grossman and Nelson, 2014; Sossouvi, 2013).</p>	<ul style="list-style-type: none"> <li>- Privacy by design (van der Veen et. al, 2018)</li> </ul>

**Dimension: Outcomes**

Refers to the positive or negative value derived by recipients (du Preez and Lee, 2017).

Dependent on appropriateness mechanism design. Potential negative consequence of in-appropriate mechanism design or inadequate access-factors are show-cased here.

**Potentially arising negative outcomes due to fraudulent mechanism design**

Surveillance and privacy violation (USAID, 2017) Stigmatization, violence etc. due to ill-designed data protection either due to a) technical b) regulatory issue or due to an ill-informed choice, data protection issues due to privacy risks of mechanism (Ford, 2017; USAID, 2017; Levin et. al, 2015; Grossman and Nelson, 2014; Sossouvi, 2013,)

**Dimension: Impacts**

Positive and negative, primary and secondary medium/long term consequences of intervention(s), directly or indirectly, intended or unintended, e.g.in terms of production activity; political activity; social activity; consumption activity (Simister, 2015; Neil, 2010).

*Source: Author's own contribution, explanatory table's structure based on synthesis of various [ICT](#), impact evaluation and [financial inclusion](#) frameworks, mainly; du Preez and Lee, 2017; Gigler, 2015; Simister, 2015; Grossman and Nelson, 2014; World Bank, 2012; Neil, 2012)*

Above Appendix elaborates the in figure 1 mentioned factors potentially undermining a, regardless of its formal potential, hindrance to a financially inclusive, thus formally accessible and objectively adequate, [e-transfers mechanism](#).

Moreover, some crucial macro-factors and [mechanism](#)-design decisions as potential “enablers” of inclusive [e-transfers](#) are pointed out, together with requirements to an inclusive [mechanism](#)-design, out of the humanitarian perspective. Above tables and figure 1 contents are non-exhaustive, and solely provide the reader with some important considerations to be made in relation to the subject matter.

#### Appendix 4: Benefits and drawbacks of e-transfer mechanisms

Mec.	Dimension	Benefits	Drawbacks
<b>Cards</b>			
<b>Mag. stripe cards</b>	Access	- formal ID or bank account not needed	- connectivity and compatible <i>PoS</i> required - restricted number of outlets for card utilization (proprietary system)
	Appropriateness	- Can be used for cash or commodities	- Illiteracy may be a challenge to read the instructions on <i>ATM</i> - Potential commission charges for transactions and withdrawals
<b>Smart cards</b>	Access	- Not always need for formal ID or bank account - Can be used off-line anywhere with <i>PoS</i>	- May require bank account and formal ID - restricted number of outlets for card utilization (proprietary system)
	Appropriateness	- Can be used for cash or commodities - Residual value can be saved on the card	- Illiteracy may be a barrier to read the instructions on an <i>ATM</i> - Potential commission charges for transactions and withdrawals
<b>Contact-less cards</b>	Access	- Not always need for formal ID or bank account	- restricted number of outlets for card utilization (proprietary system)
	Appropriateness	- Easy to use - Can be used off-line anywhere with <i>PoS</i> - Can be used for cash or commodities - Change can be saved on the card	- High risk of loss of funds if card is lost, since the user does not always need to present ID or enter security info to use the card for value up to a particular threshold - Literacy may be a barrier to read the instructions on an <i>ATM</i>
<b>Mobile</b>			
<b>Mobile tokens</b>	Access		- Formal ID may be required (depends on regulation)
	Appropriateness	- Fast and discreet - Transactions can be done by the agent	- Limited by network connectivity, agent coverage and liquidity management - All funds must be withdrawn at once

<b>Mobile vouchers</b>	Access	<ul style="list-style-type: none"> <li>- No need for formal ID</li> <li>- Low hardware requirements</li> </ul>	
	Appropriateness	<ul style="list-style-type: none"> <li>- Not limited by agent cash-flow</li> <li>- Reduced risk of theft/ fraud compared to paper vouchers</li> </ul>	<ul style="list-style-type: none"> <li>- Network issues may cause delays</li> <li>- Literacy may be a barrier; significant training may be required</li> </ul>
<b>Mobile money</b>	Access		<ul style="list-style-type: none"> <li>- Formal ID required</li> <li>- Cost of phones and charging equipment</li> </ul>
	Appropriateness	<ul style="list-style-type: none"> <li>- Fast and discreet, spending freedom</li> <li>- Potentially full suite of transactional options available reducing need to “cash out” (e.g. P2P transfer, savings)</li> </ul>	<ul style="list-style-type: none"> <li>- Literacy may be a barrier, significant investment in training may be required</li> <li>- Limited by network connectivity, agent coverage and liquidity management</li> <li>- Recipients may be charged commission for transactions and withdrawals</li> </ul>
<b>E-vouchers</b>			
<b>E-voucher</b>	Access	<ul style="list-style-type: none"> <li>- No need for formal ID</li> <li>- Very low hardware requirements</li> </ul>	
	Appropriateness	<ul style="list-style-type: none"> <li>- Not limited by <a href="#">agent</a> cash-flow</li> <li>- Can be used with any mobile operator</li> <li>- Relatively easy to use; residual value can be stored</li> </ul>	<ul style="list-style-type: none"> <li>- May require customisation from a provider’s existing platform</li> <li>- Network issues may cause delays</li> <li>- Literacy may be a barrier</li> </ul>

Source: Based on GSMA (2017), CaLP (2017), Sossouvi (2013) and CaLP (NDa)

## Appendix 5: Complete Desk Study Malawi

### Political Environment

#### Political Environment towards e-transfers

The Reserve Bank of Malawi (RBM) recently suggested scaling up [mobile money](#) to increase [financial inclusion](#) (Chauwa, 2018) and wants to increase usage of the various electronic payment products and services (RBM, 2018).

The government Social Cash Transfer Programme partially uses [mobile money](#) and bank cards as e-payment mechanisms (Hemsteede, 2018; Zimmerman et. al, 2015).

RBM's upcoming law (in December 2018) will force companies to accept at least one form of digital payment (Tobor, 2018).

**Conclusion: Conductive Political environment.**

#### National Identity System

Absent national ID system until 2017. Lack of official IDs was cited as the second biggest challenge to [financial inclusion](#) in 2017 (Demirgüç-Kunt et. al, 2018). Then, mass registration efforts, the government now claims universal (digital) ID coverage (Bansal et. al, 2018; United Nations Malawi, 2018). The issued [credentials](#) an ID card, entail information about the name, gender, date of birth, unique ID number, nationality, fingerprint, facial and signature image (Bansal et. al, 2018). Furthermore, they entail a QR-code and a machine-readable zone from which information can be extracted with a scanner, containing two fingerprints, a digital photo and some additional information, which can be accessed using a card reader (Bansal et. al, 2018).

**It can therefore satisfy e-KYC and enable access to financial services** in a fast and cost-efficient way to yet underserved segments (Bansal et. al, 2018). Accordingly, Bansal et. al (2018) suggest, **that there is no apparent need for having a separate, digital financial ID.** Thus, lack of IDs is not seen as a big challenge to [financial inclusion](#) anymore (Bansal et. al, 2018). **Most or all Malawian**

**citizens would thus not require a humanitarian-supported ID for [KYC](#)-alignment.**

Drawing from above findings, universal coverage might still not completely be achieved, as requirements for obtaining a Malawian ID (providing another type of identification supporting [identity](#) claims) might be exclusive to some (Malenga, 2017). This potentially leaves some citizens un-documented (Bansal et. al, 2018). This sentiment is confirmed by the fact, that President Mutharika claims universal coverage would have been achieved by issuing IDs to the 9 million Malawians registered in the National Registration and Identification System (Ligomeka, 2017), while UN-DESA's (2017) population estimates for Malawi are around 18 million, the adult (15+) population is above 10 million (World Bank, 2017a). Thus, for 2018, World Bank (2018c) **estimates that above 20% of Malawians are still unregistered**, with more than 35% of unregistered births in the poorest quintile. While Bansal et. al state that in July 2018, approximately 9.2 million Malawians aged 16 years and over and thus over 98% were registered, it remains to be inquired during the interviews, whether transitioning from a lack of birth certificates to obtaining the national ID is non-exclusive.

Furthermore, are IDs only issued to Malawian citizens (Malenga, 2017), potentially excluding e.g. refugees or ethnic minorities (Michael-Phiri, 2017). However, even the refugees in Dzaleka refugee camp now have access to formal banking services (Msiska and Ghelli, 2018), as UNHCR-issued IDs have recently been recognized as valid document for refugees and asylum seekers to open a bank account (Hansen, 2018), seemingly enabling the holder to participate in [mobile banking](#) as well (Crosman, 2018). Which refugee information needed to be disclosed to the government, and which [DFS](#) exactly can be accessed now, remains to be seen.

## Economic Environment

Relevance of MNOs for DFS		
Share of average daily payment systems turnover for retail <a href="#">DFS</a> -transactions (June 2018), based on RBM (2018).		
<a href="#">ATM DFS</a> Transactions		0.03 %
Internet Banking		0.81 %
PoS		0.45 %
<b>Mobile Payments</b> ; of which		<b>98.7 %</b>
Bank-led: 11.7%		
<b>Non-bank led: 88.3 %</b>		
MNO-led registered accounts in June 2018 (RBM, 2018)	Total	Of which active in the last 90 days
	4.7 million	38%
<a href="#">Unique mobile subscribers</a> (2016), based on GSMA (2017a).	Total	Relative
	4.7 million	26%

Relevant Digital Financial Services Providers	
Key providers	Airtel, Telekom Networks Malawi (TNM), NBS Bank, Opportunity International Bank Malawi, and Zoono (United Nations Capital Development Fund [UNCDF], 2017).
Relevant ( <a href="#">MNO</a> )- <a href="#">DFS</a> providers	<b>Airtel and TNM are the dominant incumbents</b> (UNCDF, 2018; Madise, 2014). Zoono is currently only offering money transfer services and no deposits into <a href="#">wallets</a> for Malawi (UNCDF, 2017; Zoono, 2017), therefore not (yet) enabling customers to participate

	<p>in an <a href="#">open-loop</a> payment system as defined by the <a href="#">Barcelona Principles</a> .</p> <p>Regarded key <a href="#">DFS</a> providers are therefore solely <a href="#">mobile network operators</a> (MNOs). This is as they (at least in the past) had lighter regulation than regular banks (Bansal et. al, 2018; Madise, 2014) and due to given <a href="#">agent</a> penetration vs. the <a href="#">ATM</a>-network (approx. 400) of the nine commercial banks in the country (Mchulu, 2018) and the high share of retail <a href="#">DFS</a>-volume to non-bank led mobile payments providers (see above).</p>		
<p>Services of regarded <a href="#">MNO</a> <a href="#">DFS</a> providers</p>	<p>Airtel</p> <p>Airtel Money, also called Khusa M'manja (Madise, 2014), allows for sending and receiving money (across networks), make payments for goods and services, perform bank transactions, withdraw at <a href="#">ATMs</a> and store value on a mobile <a href="#">wallet</a> (Airtel, 2018 and Airtel, 2018a).</p> <p>Furthermore, the loan service Kutchova (Airtel 2018b) was launched in 2016 (Wardak, 2018). There are currently about 230,000 Kutchova loans (Wardak, 2018).</p> <p><b>Conclusively, Airtel Money can be defined as <a href="#">open-loop</a> payment system.</b></p>	<p>Telekom Networks Malawi</p> <p>Mpamba, works in a similar manner as Khusa M'manja and allows for similar services, including a mobile <a href="#">wallet</a> (Telekom Network Malawi, 2017; Madise, 2014). Both services show strong parallels with the Kenyan <a href="#">M-Pesa</a> service by Safaricom and fall under the definition of financial services (Madise, 2014).</p> <p><b>Conclusively, TNM's <a href="#">mobile money</a> can be defined as <a href="#">open-loop</a> payment system.</b></p>	
<p>Mobile Money Agent Network in June 2018 (RBM, 2018)</p>	<p>Total</p> <p>35,865</p>	<p><b>Of which in rural areas</b></p> <p><b>11.5%</b></p>	<p>Urban/semi-urban</p> <p>78.5%</p>

<b>Conclusion: Rural areas <u>agent</u>-coverage lags behind.</b>			
Number of <b>active</b> DFS agents per 100,000 adults (30 days)  (UNCDF, 2018)	2012	2017	
	<1 (200 <u>agents</u> )	134 (approx. <b>12,750</b> active <u>agents</u> )	
<b>Conclusion: Regardless the improving trends, exclusion factors are likely to remain.</b>			

## Social Environment

<b>Financial Inclusion</b>		
Account <sup>52</sup> (% age 15+), based on World Bank (2018a)	2011	2017
	16.5	<b>33.7</b>
Financial Institution Account <sup>53</sup> (% age 15+), based on World Bank (2018a)	2011	2017
	16.5	23.0
Mobile money account <sup>54</sup> (% age 15+), based on World Bank (2018a)	2014	2017
	3.8	<b>20.3</b>
Percentage of adults with an active registered DFS account (90 days), based on UNCDF (2018).	2012	2017
	<1; approx. 1,000 active accounts	21; approx. 2.1 million active accounts
Total Mobile Banking subscribers in June 2018 (RBM, 2018) <sup>55</sup>	534,892	
Reasons for not possessing any account according to the 2017 Global Findex (Demirgüç-Kunt et. al, 2018a) survey for ages 15+		
Insufficient funds to open account	66%	
<b>Lack of IDs</b>	<b>30%</b>	

<sup>52</sup> Account (by oneself or together with someone else) at a bank or another type of financial institution (see financial institution account) or personal usage of a [mobile money](#) service in the past 12 months (World Bank, 2018).

<sup>53</sup> Denotes the percentage of respondents who report having an account (by themselves or together with someone else) at a bank or another type of financial institution (World Bank, 2018a)

<sup>54</sup> Denotes the percentage of individuals personally using a [mobile money](#) service in the past 12 months (World Bank, 2018a).

<sup>55</sup> Low because mobile banking is a service extended to customers with bank accounts while the non-bank mobile money services are used by both banked and non-banked customers (RBM, 2018).

Financial Services too expensive	23%
Distance	13%
<p><b>Conclusion: Despite positive developments, the majority is still excluded from <a href="#">(digital) financial services</a>, lack of legal IDs might be an important factor (see below).</b></p>	

**Social & technological factors applying to target groups of humanitarian assistance, potentially restricting inclusive and appropriate [ICT](#)-use.**

- Illiteracy, especially in rural areas (UNCDF 2017)
- Transaction charges potentially inadequate to the poor (UNCDF, 2017; Kita, 2014)
- Connectivity (UNCDF, 2017)
- Low [agent](#) liquidity and accessibility, especially in rural areas (RBM, 2018; UNCDF, 2017; Kita, 2014)
- Travel distance to distribution points (Kita, 2014)
- Lack of electricity (Buckley et. al, 2014)
- Mistrust/lack of acceptance (Buckley et. al, 2015; Kita, 2014)
- Poor or no network coverage (Kita, 2014)

Refugees and Asylum seekers	As of November 2018, about 35,000 in Dzaleka camp (United Nations Malawi 2018a).
-----------------------------	--

## Technological Environment

2017 ICT Development Index <sup>56</sup> country ranking (International Telecommunication Union [ITU], 2017)		<b>Malawi is ranked place 167 out of 176 countries.</b>
Access to electricity (%) of population World Bank (2018d)	1990	2016
	1.1	<b>11.0</b>
Mobile phone penetration (World Bank, 2018b) <sup>57</sup>	2011	2017
	25.3	<b>41.7</b>
<u>Unique mobile subscribers</u> (2016), based on GSMA (2017a).	Total	Relative
	4.7 million	26%
3G coverage (% of population) in 2016 (ITU, 2017a)	<b>42.0</b>	
Price of Broadband Data (1GB mobile prepaid) as % of GNI per capita (2017), based on (Alliance for Affordable Internet, 2018)	2015	2017
	36	<b>17.85</b>
<b>Conclusion: Despite improving trends, technological challenges for utilizing <u>ICT</u> during a humanitarian intervention remain.</b>		

<sup>56</sup> The ICT Development Index (IDI) is a composite index combining 11 indicators (as proxies for ICT use, access and skills). It is utilized for monitoring and comparing developments in ICT between countries and over time (ITU, 2019).

<sup>57</sup> Measured in mobile cellular subscriptions (%) (United Nations Statistics Division [UNSD], ND).

## Regulatory Environment

Key DFS Regulators	
Key <a href="#">mobile money</a> regulator	<b>Reserve Bank of Malawi</b> (Buckley et. al, 2015). RBM does not directly regulate <a href="#">agents</a> except for some activities, including monitoring and enforcing <a href="#">KYC</a> for <a href="#">agents</a> (Buckley et. al 2014).
Further regulators involved in <a href="#">AML/CFT</a>	The <b>Ministry of Finance</b> (MOF) is involved in the strategic policy development for <a href="#">mobile money</a> as part of its broader role in improving <a href="#">financial inclusion</a> in the country (Buckley et. al, 2014). The <b>Financial Intelligence Unit</b> (FIU) is responsible for compliance with <a href="#">AML/CFT</a> regulations (Buckley et. al, 2015). There are also several other important institutions involved in <a href="#">AML/CFT</a> , their work however does not directly relate to <a href="#">KYC</a> -standards for <a href="#">mobile money</a> (Buckley et. al, 2015).

Key DFS Regulation	
Airtel and TNM <a href="#">AML</a> Policies	Officially, <b>the National ID or passport for <a href="#">SIM</a>-registration and accessing <a href="#">DFS</a> is required</b> (Airtel 2018c). Potential exemptions are however implied.
The Deployment and Usage of Electronic Payments Channels Regulation 2018	Upcoming December 2018 (Tobor, 2018).
E-Money Regulations 2018 (?)	Upcoming, currently revised by RBM (UNCDF, 2018), withdrawn for better alignment with National Payment Systems Law (Government of Malawi, 2017a). Will replace the existing guidelines of 2011 and is supposed to apply to both banks and non-banks (Buckley et. al, 2015). This implies, that <a href="#">MNOs</a> might be as strictly tied to <a href="#">KYC</a> -standards as formal banks.

<p>Money Laundering Proceeds of Serious Crime and Terrorist Financing Act (2006)</p>	<p>§24.-(1) “Every financial institution shall (...), ascertain the <u>identity</u> of the to verify customer or beneficial owner on the <b>basis of an official or other customer’s identifying document</b>, and shall verify the <u>identity</u> of the customer <u>identity</u> on the basis of reliable and independent source documents, data or information or other evidence as is reasonably capable of verifying the <u>identity</u> of the customer (...)” (RBM, 2006, p:20)</p>
<p>Guidelines for Mobile Payment Systems (2011)</p>	<p>§9.1.4: “<b>Enrolment of consumers should satisfy Know Your Customer (KYC)</b> requirements as laid out in the Money Laundering, Proceeds of Serious Crime and Terrorist Financing Act (2006) and regulations thereto” (RBM, 2011, p:12).</p>
<p>Communications Act (2016)</p>	<p>§92.2: „Any electronic communications licensee or the distributor, <u>agent</u> or dealer of the electronic communications licensee, shall__</p> <p>(a) where a potential subscriber is a natural person, obtain and</p> <p>fill in a form the following information__</p> <p>(i) the full name of the subscriber;</p> <p><b>(ii) the <u>identity</u> card number, or any other document that proves the <u>identity</u> of the subscriber;</b> and</p> <p>(iii) the residential and business or registered physical address of the subscriber (...)” (Government of Malawi, 2016, p: 45)</p>
<p>Financial Crimes Act (2016)</p>	<p>§16.1: “Every reporting institution shall (...) identify the customer or the beneficial owner, <b>on the basis of an official document and verify the identification through reliable and independent source documents</b>, data or information or other evidence as is reasonably capable of</p>

	<p>verifying the <a href="#">identity</a> of the customer or beneficial owner (...)” (Government of Malawi; p.22 ,2017).</p> <p>§16.2.b: “(...) if the customer is a natural person, adequately identify and verify the <a href="#">identity</a> of the person, including information relating to— (i) <b>the name, address and occupation of the person</b>; (ii) <b>the national <a href="#">identity</a> card or passport or other applicable official identifying document of the person</b> (...)”(Government of Malawi,2017, p.23).</p>
Tiered KYC?	<p>Increasing <a href="#">due diligence</a> requirements with increasing transaction sizes (Zimmerman, 2017) and vice versa. The FIU is authorised to allow the use of reduced <a href="#">KYC</a> requirements (Buckley et. al, 2015). Before the national ID roll-out <a href="#">mobile money</a> providers applied a tiered <a href="#">KYC</a> approach for across the different <a href="#">mobile money</a> accounts (Bansal et. al, 2018). <b>Some low-value accounts did not require any proof of identification</b> (customers with monthly average income below 50,000 MKW, supposed to be adjusted to 300,000 MKW, which is around 60 € and 360 € respectively) while upper-limit accounts required proof of identification and other requirements, for example a proof of an income source. There were no designated standard tiers and respective acceptable documents for each tier (Bansal et. al, 2018).</p>
<b>Conclusion</b>	<p>Due to an absent national ID system (see political environment aboe) until the middle of 2017 (Bansal et. al, 2018), aligning with the <b>ambiguous identification requirements</b> in the regulations above, the regulating body and service providers did accept some or all identification documents of the county, for example a letter of the local chief, driving licenses, student cards, or even <a href="#">SIM</a>-card registration information (Bansal et. al, 2018; Government of</p>

Malawi, 2017a; Buckley et. al, 2015). [Financial Service Providers](#) therefore had discretion in establishing what documents were accepted for [KYC](#) (Bansal et. al, 2018), a potential which could be reaped by a humanitarian agency when wanting to include un-documented. The large variety of documents accepted for [KYC](#)-purposes however left [Financial Service Providers](#) open to fraud (Bansal et. al, 2018). Therefore, it is likely, that due to the new ID system, only the national ID will be accepted from now on for [KYC](#)-alignment with the upcoming regulations stated above, as it provides a good opportunity for easy identification across all providers (Bansal et. al, 2018). Accordingly, Bansal et. al (2018) suggest **making the national ID mandatory** for use in the financial sector. The more flexible regulations could therefore tighten in the nearby future.

## International Humanitarian Organisations

Relevant humanitarian actors utilizing <a href="#">e-transfers</a>		
Malawi Red Cross (MRCS)		
Year	Intervention Type	Open-loop?
2016	<a href="#">Disaster</a> (flood) relief	<a href="#">Open-loop</a> payment system, utilisation beyond intervention not clear and whether restrictions, then yielding <a href="#">closed-loop</a> , were imposed.
Description		
The recipients were given mobile phone handsets to ease the process and the MRSC <b>made special arrangements with Airtel Malawi</b> to access cash via Airtel Money (Washon, 2016).		
Open Questions		
<ul style="list-style-type: none"> <li>- Which arrangements were made with Airtel? Easier identification requirements (reduced <a href="#">KYC</a>)?</li> <li>- Could recipients use the <a href="#">e-transfer mechanism</a> beyond the intervention to store, receive and send money over the transaction operators within the regulated realm?</li> </ul>		
USAID		
Year	Intervention Type	Open-loop?
2012-2016	Creating use-cases to show advantages of <a href="#">mobile money</a>	Implied (Chibwana and Kanjo, 2015), but ambiguous.
Feed the Future Malawi Mobile Money was a four-year long project seeking to increase <a href="#">mobile money</a> adoption in Malawi (USAID, 2018). Lack of impact evaluations and progress reports.		
Open Questions		

Any experiences with inclusion into <a href="#">open-loop</a> payment systems?		
World Food Programme & INGO Consortium led by Oxfam and Save the Children (Kita, 2014)		
Year	Intervention Type	Open-loop?
2012/ 2013 & 2013/ 2014	Emergency Cash Transfer Response Project” - Food Insecurity Response	No. <a href="#">Mobile Vouchers</a> . Seemingly no lasting <a href="#">financial inclusion</a> impact.
Description		
<p>The <a href="#">cash transfer</a> was delivered through different mechanisms, including commercial banks, <a href="#">mobile money</a> as well as direct disbursement through third parties (Kita, 2014). The recipients were given a phone, with a <a href="#">SIM</a> card. Prior distribution, a message would be received on the phone indicating the amount of money to be cashed out (Kita, 2014) at predetermined sites (Mita, 2015).</p> <p><b>Inherently, this, although framed as <a href="#">mobile money</a> by WFP, is just a <a href="#">mobile voucher</a>.</b> Therefore, this <a href="#">closed-loop</a> proprietary solution has failed to <a href="#">financial inclusion</a> beyond the interventions (Zimmerman et. al, 2015).</p> <p>Contracted service providers were Airtel Money, OIBM, and G4S Security (Zimmerman et. al, 2015)</p>		
Open Questions		
- What were underlying reasons for the proprietary solution?		
<p><b>Conclusion: There are some hints, that humanitarian actors previously used payment channels which are <a href="#">open-loop</a> enabled. How and what arrangements were reached based on humanitarian grounds, and whether <a href="#">financial inclusion</a>, especially of previously un-documented took place, remains unclear.</b></p>		

## Appendix 6: Complete Desk Study Kenya

### Political Environment

#### Political Environment towards e-transfers

The Government of Kenya prioritized universal access to ICT as enabler for mobile money and recognized its contribution to financial inclusion in its Development Plan 2013-2017 (Republic of Kenya, 2013a). The success of M-Pesa can, amongst others, be attributed to a very friendly regulatory and political environment from early on (Lepoutre and Oguntoye, 2018). Accordingly, Kenya was the first country in the world to use mobile phones for cash transfers (Datta et. al, 2008).

In collaboration with Master Card, the government is on the verge to issue a multipurpose service pre-paid payment card allowing holders to make or receive payments. The “Huduma Card” is supposed to serve as **main digital payment gateway of governmental services, without requiring the holder to have a bank account**. The card will have a smart chip storing the holder’s personal data and host multiple applications and additionally using the whole MasterCard network (Huduma Kenya, 2016). Set to roll-out in October 2018 (The Standard, 2018), it is not clear, whether it has happened or when it will take place exactly.

Government services are digitally accessible through the country’s e-government platform, e-Citizen. It processes application and payment services on behalf of 26 government agencies that have integrated into the platform. In total, over 300 unique government services are offered, with the goal to include 5000 government services by 2020. This is considered as a **strong indication that the government is committed to drive a purely digital agenda**, also due to the fact, that **cash is not accepted for services** offered through the eCitizen platform (Frydrych and Wasunna, 2017).

**Conclusion: HIGHLY Conductive political environment towards e-transfers.**

#### National Identity System

Kenya’s system for the civil registration and identification is described as well established (World Bank, 2016b). The national *ID* card is widely held and needed to

access basically all governmental services, receive cash transfers and register for a [SIM](#), [mobile money](#) or banking (World Bank, 2016b). Until recently however, did Kenya not have a single authority with the [mandate](#) of providing identification services across the population (World Bank, 2016b). This implied considerable duplication of registration facilities (World Bank, 2016b)

The nation now is on the verge of changing that situation, by the parliament's decision of amending a change in the statute of law to implement a national [identity](#) management system<sup>58</sup> which aims to become the single source of identifying individuals (Republic of Kenya, 2018; §9A (2)). This "National Integrated Identity Management System" (§9A (1)) (NIIMS) has the "**functions (...)**

- a) to create, manage, maintain and operate a national population register as a **single source of personal information of all Kenyan citizens and registered foreigners resident** in Kenya;
- b) to assign a unique national identification number to every person registered in the register;
- c) to harmonise, incorporate and collate into the register, information from other databases in Government agencies relating to registration of persons;
- d) **to centrally print and distribute for collection all national identification cards, refugee cards, foreigner certificates, birth and death certificates, driving licenses, work permits, passport and foreign travel documentation, student identification cards (...)**" (Republic of Kenya; §9A (2); pp.271-273, 2018).

---

<sup>58</sup> Linkages with the since 2015 existing (World Bank 2016b) Integrated Population Registration system (IPRS) which seeks to harmonize all government population registration databases into one national data base and currently is populated with 39 million records of citizens and foreign residents (State Department for Immigration, Border Control and Registration of Persons, 2018) are not clear, but what might matter most, is the sentiment that the ID system is on the verge of becoming more centralized. The mandate of the IPRS is to enable authorized public and private entities to conduct a validation check on ID credentials issued by the previous departments, especially the national *ID*. It can be accessed by e.g. financial institutions, mobile operators, a wide range of other entities, but not by individuals. (World Bank 2016b). Data from the different sources including birth and civil registration, alien and refugee registration and the national population register are combined into the IPRS (World Bank, 2016b).

Hence, Kenya will move from a federated to a centralized ID system.<sup>59</sup> The new system builds on [biometric](#) information, which is viewed as critical by some, as although Article 31 of Kenya's Constitution enshrines a right to privacy, there is no corresponding data protection legislation to operationalize it, which is seen as specifically worrisome regarding [biometrics](#) enabling e.g. mass-surveillance (Muthuri et. al, 2018). While the parliament recently has enacted the Data Protection Act (Republic of Kenya, 2018a), for example warranting the individual's right to object to data collection and processing (§23 (1c)), it remains to be seen, whether this does not conflict with the necessity to acquire a national ID. **While an [SSI](#) could become a key alleviator in that sense, will the political economy assumingly insist on the centralized database containing [PII](#).**

The procurement process is expected to be completed by the end of 2018 (Wakaya, 2018).

Still, ID-related exclusion is possible:

First, Kenyan citizenship is not granted based on birth on national territory but based on ancestry. This requires that at least one parent can demonstrate Kenyan citizenship. Especially in border counties many births are to parents without ID cards and therefore of undetermined citizenship, the children can therefore become stateless (World Bank, 2016b). The estimated rate of birth registration, 63% (World Bank, 2018c), is not enough to provide a solid foundation for the national registration system. There is thus not a smooth flow of [identity](#) between birth/civil registration and the national ID (World Bank, 2016b). Furthermore, long-time residents who are not citizens and who have not been registered as either resident aliens or refugees remain un-documented (World Bank, 2016b).

As the inability to provide birth certificates may yield failure to obtain the national ID, also the new centralized system might thus fail to include all citizens and non-citizens. **The importance of the national ID might be exacerbated by shifting to a centralized ID system, thus exacerbating exclusion effects** for those who do not hold it.

---

<sup>59</sup> Refer to [Digital Identity Systems](#) in glossary.

Eventually, according to InterMedia (2018) and World Bank (2018c), **18% of the population were lacking national ID** in 2017 and 2018 respectively.<sup>60</sup> ID coverage particularly lacks behind in the poorest and border areas, that have the lowest ratio of birth registrations and the highest percentage of vulnerable people (World Bank, 2016b), with nearly **50% of unregistered births in the poorest quintile** (World Bank, 2018c).

**Conclusion: Due to the increasing centralization of legal [identity](#) issuance, the entry point for a humanitarian foundational ID could become increasingly restricted. This does somehow not oblivate the need for more legal IDs in the context (also see social environment below).**

**Identity Providers - Ministry of Interior And Coordination Of National Government**

<b>Department of Civil Registration</b>	Equipped with the <a href="#">mandate</a> to register births and deaths and to issue the according paper certificates (World Bank 2016b).
---	---

<b>National Registration Bureau</b>	Key agency responsible for determining individuals' claims to Kenyan citizenship (World Bank, 2016b). Has the mandate to register citizens meeting the according criteria at the age of 18 and to issue national ID cards and numbers. It collects biographic and <a href="#">biometric</a> data. Also operates the system-wide Automated Fingerprint Identification System (AFIS) that checks against possible duplicates or multiple registrations (as well as for the registration of aliens and refugees and the inclusion of their fingerprints into the AFIS) (World Bank, 2016b). Selected data from these sources is then captured by the Integrated Population Registry Service (World Bank, 2016b).
-------------------------------------	---

---

<sup>60</sup> Which approximately resonates with the share of people stating lack of ID as reason of not possessing any account at all in the Global Findex Survey of 2017 (Demirgüç-Kunt et. al, 2018).

Department of Immigration Services	Provides visas and residence permits to aliens and passports to citizens (World Bank, 2016b).
Refugee Affairs Secretariat (RAS)	Main lead in refugee registration (Norwegian Refugee Council, 2017).

Providers Digital Financial Services Providers <sup>61</sup>	
Key providers	Safaricom, Orange, Airtel, Telkom Kenya, and increasingly formal banks (Communications Authority of Kenya, 2018; Lepoutre and Oguntoye, 2018; Deynes, 2014; Republic of Kenya, 2013a).
Regarded relevant ( <a href="#">MNO</a> )- <a href="#">DFS</a> provider	Safaricom due to major market share of mobile subscriptions and transfer services (Communications Authority of Kenya, 2018; Financial Inclusion Insights, 2018a), an <a href="#">agent</a> -network with extensive coverage when compared to branch networks of banks (Ndung'u, 2017) and due to playing a key role in shaping the regulatory environment together with the Central Bank of Kenya (Lepoutre and Oguntoye, 2018).
Services of regarded <a href="#">MNO-DFS</a> provider	<p><a href="#">M-Pesa</a>.</p> <p>Developed jointly by Safaricom, (a subsidiary of Vodafone), and the Commercial Bank of Africa <a href="#">CBA</a> (Lepoutre and Oguntoye, 2018; Ndung'u, 2017). Started in 2007 as electronic <b>P2P money transfer product</b>, enabling users to <b>store value</b> on their mobile phones. Safaricom established a network of <a href="#">agents</a> forming the <i>PoS</i>, where customers can <b>convert cash into electronic units</b> of money to load into their mobile <a href="#">SIM</a> card <b>and vice versa</b> (Ndung'u, 2017).</p> <p>In subsequent years, <b>formal banks started using the platform to link into existing products and services</b>, as well as to offer new products on the platform using <a href="#">M-PESA-KYC credentials</a> (Ndung'u, 2017; Deynes, 2014).</p> <p>Thus, <a href="#">M-Pesa</a> evolved into a platform for a wide range of financial services such as <b>cross-border remittances, savings accounts or credit/loans</b> (most notably, <b>M-Shwari</b>, since 2012) (Ndung'u, 2017; Deynes, 2014).</p> <p><a href="#">M-Pesa</a> has thus emerged as the central platform for digital credit assessment and the distribution of microcredit (Ndung'u). This</p>

<sup>61</sup> Due to the dominance of [M-Pesa](#), the relevance of [MNOs](#) for [DFS](#) is automatically given in Kenya.

transformation carried important implications for financial sector formality and adherence to [AML/CFT](#) standards (Ndung'u, 2017).

Based on its interoperability with the formal banking sector, wide availability and potential of accessing wider *DFS*, it **satisfies the characteristics of an [open-loop](#) payment system** (but does not need to necessarily (Vohra, 2015)). [M-Pesa](#) shows strong parallels with the Malawian [mobile money](#) services provided by Airtel and TNM (Madise, 2014).

Financial Inclusion	
<p>Kenya is leading in developing <a href="#">mobile money</a> payment systems and in widespread usage (Financial Inclusion Insights, 2018). <a href="#">M-Pesa</a> made Kenyan <a href="#">mobile money</a> the most successful <a href="#">DFS</a> deployment the world has seen (Denyes, 2014). <a href="#">M-Pesa</a> and similar <a href="#">digital financial services</a> represented a significant improvement in the national payments technology, reducing transaction costs and lowering the barriers to entry into the formal financial system (Ndung'u, 2017). Kenya thus is THE example of how <a href="#">mobile money</a> can accelerate <a href="#">financial inclusion</a> and leapfrog formal banking infrastructure (Ndung'u, 2017; Deynes, 2014), mainly attributed to the success of <a href="#">M-Pesa</a>, evolving from a simple mobile payment system to wider <a href="#">digital financial services</a> (Ndung'u, 2017).</p>	
<p><b>However, some are still financially excluded from e.g. <a href="#">mobile money</a>, lack of legal ID is an important reason.</b></p>	
<p>Reasons for not possessing any account according to the 2017 Global Findex (Demirgüç-Kunt et. al, 2018a) survey for ages 15+</p>	
Insufficient funds to open account	39%
Financial Services too expensive	19%
Distance	16%
<b>Lack of formal identification</b>	<b>14%</b>
<p>Reasons for not <u>using</u> a <a href="#">mobile money</a> account according to a 2017 InterMedia (2018) survey for ages 15+</p>	
Financial Services too expensive	55%
Preference for cash	41%
<b>Lack of ID documents</b>	<b>37%</b>
<p>Reasons for not <u>registering</u> a <a href="#">mobile money</a> account according to a 2017 InterMedia (2018) survey for ages 15+</p>	

Lack of ID documents	58%
<p><b>Conclusion:</b> While the existence of <a href="#">M-Pesa</a> might have very well been an important technological and economic factor for increased <a href="#">financial inclusion</a>, the lack in legal IDs (also see below) might still undermine the full potential for a <a href="#">financially inclusive</a> humanitarian <a href="#">e-transfer mechanisms</a>.</p>	

<b>Social &amp; technological factors applying to target groups of humanitarian assistance, potentially restricting inclusive and appropriate <a href="#">ICT</a>-use.</b>	
<ul style="list-style-type: none"> <li>- Low number of birth certificates for accessing national <i>ID</i> (World Bank, 2016b)</li> <li>- <b>Lack of ID</b> for being included into <a href="#">M-Pesa</a> system (Kondakhchyan et. al, 2018; Datta et. al, 2008)</li> <li>- Connectivity (World Bank, 2016b)</li> <li>- Travel distance to <a href="#">M-Pesa agents</a> (Datta et. al, 2008)</li> <li>- Illiteracy, inexperience with <a href="#">mechanism</a> and language barriers (Kondakhchyan et. al, 2018)</li> <li>- Cultural resistance to seek information on appropriate use (Kondakhchyan et. al, 2018)</li> <li>- Security concerns particularly among displaced individuals (Kondakhchyan et. al, 2018)</li> </ul>	
<p>Non-citizens - Refugees and Asylum seekers</p>	<p>Kenya has a large population of officially recognized<sup>62</sup> refugees, above 400,000 at the end of 2017 (UNHCR, 2018a), which are assisted by UNHCR. Registration efforts were carried out jointly by the government and UNHCR (World Bank, 2016b). While UNHCR also issues <a href="#">mandate</a> cards to refugees, the government-issued Alien-ID for officially (from the government) recognized refugees however seems to be the only way for refugees and asylum seekers to be financially and digitally included, the UNHCR-<a href="#">mandate</a> cards seem to have a diminishing legal power (Norwegian Refugee Council, 2017). This implies, that <b>refugees</b></p>

<sup>62</sup> Persons recognized as refugees under the 1951 UN Convention/1967 Protocol, the 1969 OAU Convention (UNHCR, 2018).

**currently need to undergo governmental vetting and that humanitarian ID issuance is not sufficient for accessing fundamental financial and digital services.** Furthermore, while the government gradually extended its sovereignty in refugee status determination and according [credentialization](#) from 2014 onwards vs. UNHCR, the process of issuing Alien ID seems to have halted (Norwegian Refugee Council, 2017). Eventually, even if a valid Alien ID was possessed, acceptance is not certain (Norwegian Refugee Council, 2017).

The majority of these individuals has fled from Somalia (UNHCR, 2018a). More than 45 humanitarian organisations actively support refugees in Kenya under the aegis of the Kenya Comprehensive Refugee Programme (GSMA, 2017b).

**Conclusion: Besides various other exclusion factors, the increasing centralization and sovereignty of the Kenyan government in providing, if at all, legal IDs to non-citizens, might be highly problematic if a humanitarian has the intention to provide [financially inclusive](#) humanitarian [e-transfer mechanisms](#).**

## Technological Environment

2017 ICT Development Index <sup>63</sup> country ranking (International Telecommunication Union [ITU], 2017)	<b>Kenya is ranked place 138 out of 176 countries.</b>	
Access to electricity (%) of population World Bank (2018d)	1990	2016
	3.3	<b>56.0</b>
Mobile phone penetration (World Bank, 2018b) <sup>64</sup>	2011	2017
	0	<b>86</b>
3G coverage (% of population) in 2016 (ITU, 2017a)	<b>78.0</b>	
Mobile-broadband prices 1 GB (% GNI pc) (ITU, 2017a)	4.4	
<p>Physical infrastructure, such as road networks, rural electrification and mobile network coverage are well-established when compared to other countries in the region (Deynes, 2014). This is, besides a well-established <a href="#">agent</a>-network, seen as one of the key factors determining <a href="#">M-Pesa</a>'s success (Deynes, 2014).</p> <p>Connectivity in general however remains an issue (World Bank, 2016b).</p>		
<p><b>Conclusion: Vastly improving trends, minor technological challenges for utilizing <a href="#">ICT</a> during a humanitarian intervention however remain.</b></p>		

<sup>63</sup> The ICT Development Index (IDI) is a composite index combining 11 indicators (as proxies for [ICT](#) use, access and skills). It is utilized for monitoring and comparing developments in [ICT](#) between countries and over time (ITU, 2019).

<sup>64</sup> Measured in mobile cellular subscriptions (%) (United Nations Statistics Division [UNSD], ND).

## Regulatory Environment

Key DFS-Regulators	
Key regulator	Central Bank of Kenya (CBK) (Ndung'u, 2017).
Further regulators involved in <a href="#">AML/CFT</a> of <a href="#">mobile money</a>	Communication Authority (Ndung'u, 2017). Further, the National Treasury and the Competition Authority.

Key DFS Regulation and Policies	
General	For <a href="#">mobile money</a> to remain outside banking regulation, it needs to be restricted to payment services only. Every account is to be connected to a single and identifiable person with a valid ID (Lepoutre and Oguntoye, 2018).
Safaricom AML Policies	The previous role of the Kenyan banking regulator is seen as another key factor for <a href="#">M-Pesa</a> 's success (GSMA, 2017c; Evans and Pirchio, 2015; Consultative Group to Assist the Poor [CGAP], 2010). As the Kenyan financial regulator was in a niche phase (Lepoutre and Oguntoye, 2018), although the Central Bank of Kenya (CBK) was mandated to oversee payment systems in 2003, the operational modalities for its regulatory mandate, legislation for non-bank actors engaging in payment systems, had not been clarified when Safaricom started its pilot (Mas and Radcliffe, 2011; CGAP, 2010). CBK thus lacked the power to block <a href="#">M-Pesa</a> . If no-interest was made on the e-money and that money was made only on transaction fees, <a href="#">M-Pesa</a> was exempted from banking regulatory supervision (Lepoutre and Oguntoye, 2018; Central Bank of Kenya, 2013). The lack of regulation thus was a key enabler (CGAP, 2010), allowing Safaricom to pilot its services without confining strict regulations,

while the same approach to formal banks wanting to engage in the [DFS](#) market was not offered (Deynes, 2014). The evolving near-monopoly of Safaricom in [mobile money](#) was not considered a real problem by the government (Lepoutre and Oguntoye, 2018).

After Safaricom [KYC](#) policies, registration of prospective *M-Pesa* customers must occur **face to face**, with the **requirement to produce an original ID for registration**, the [agent](#) then must document customer names, ID number (and type), date and mobile number (Safaricom, 2012). Accepted IDs include the **Kenyan National ID Card**, a valid passport for foreigners and **recognized photo IDs issued by the government** e.g. an Alien ID (Safaricom, 2012). Accepted *IDs* therefore are more restricted than as defined in governmental regulations (see Proceeds of Crime and Anti-Money Laundering Act §45 (1) v below). **For any M-Pesa transaction** entailing depositing, withdrawing or giving cash, the **proof of identification must be provided**. Further, must the prospective customer already have an on the Safaricom **network registered [SIM](#) card**, which also requires possession of officially recognized *ID* (Safaricom, 2012). The strict [KYC](#)-procedures could implicitly be a response to the FATF dark-grey-listing of Kenya in 2011 (lasting until 2014), leading the CBK to request Safaricom to improve [KYC](#)-procedures (Ndung'u, 2017).

<p>Proceeds of Crime and Anti-Money Laundering Act (No. 9) (2009)</p>	<p><b>§45. Obligation to verify customer identity</b></p> <p>“1) A reporting institution shall take reasonable measures to satisfy itself as to the true <u>identity</u> of any applicant (...) by requiring the applicant to produce an official record reasonably capable of establishing the true <u>identity</u> of the applicant, such as—</p> <ul style="list-style-type: none"> <li>a) in the case of an individual— <ul style="list-style-type: none"> <li>i) <b>a birth certificate;</b></li> <li>ii) <b>a national identity card;</b></li> <li>iii) <b>driver’s license;</b></li> <li>iv) <b>a passport; or</b></li> <li>v) <b>any other official means of identification as may be prescribed (...)</b></li> </ul> </li> </ul> <p>3) Records required under subsection (1)(a) shall contain particulars sufficient to identify—</p> <ul style="list-style-type: none"> <li>a) <b>the name, physical and postal address and occupation</b> (or where appropriate business or principal activity) of each person— <ul style="list-style-type: none"> <li>i) conducting the transaction; or</li> <li>ii) on whose behalf the transaction is being conducted, <b>as well as the method used by the reporting institution to verify the identity of that person (...)</b>” (Republic of Kenya, 2009, [no page number]).</li> </ul> </li> </ul>
<p>Proceeds of Crime and Anti-Money Laundering Regulations (2013)</p>	<p><b>§12. Customer Due Diligence</b></p> <p>“1) Customer due diligence measures are to be undertaken by a reporting institution to enable it achieve the following objectives—</p> <ul style="list-style-type: none"> <li>a) <b>identify the customer and verify that customer’s identity using reliable, independent source documents, data or information;</b></li> </ul>

	<p><b>b) identify the beneficial owner, and take reasonable measures to verify the identity of the beneficial owner</b>, such that the reporting institution is satisfied <b>that it knows who the beneficial owners is (...)</b>" (Republic of Kenya, 2013, p.32).</p>
Bank Circular No. 2 of 2018	Reaffirms above Act's and Regulation's validity (Central Bank of Kenya, 2018).
E-Money Regulations (2013)	<p>"§3.2. This Regulation applies to: (a) <b>all issuers of e-money who are not licensed</b> as banks or financial institutions under the Banking Act (...)" (Central Bank of Kenya, 2013, p.3).</p> <p><b>§7 Compliance requirements applicable to e-money issuers</b></p> <p>"§7.2 E-money issuers shall put in place systems to maintain accurate and complete records of emoney accounts opened, <b>the identity of e-money holders, transactions undertaken by emoney holders (...)</b>" (Central Bank of Kenya, 2013, p. 9).</p> <p><b>§12 Consumer Protection</b></p> <p>"§12.1 d) <b>That e-money cannot earn interest (...)</b> and that <b>it is not a savings account or other investment instrument;</b></p> <p>(e) <b>That e-money is not a deposit (...)</b>" (Central Bank of Kenya, 2013, p. 14)</p>
National Payment System Regulations, (2014)	<p><b>§12 Register of customers</b></p> <p>"1) A payment service provider shall, at all times, maintain a register containing identification details of all customers and the funds outstanding in their e-money accounts of which the <b>details shall include the identity card number or the passport number.</b></p> <p>2) <b>The identity card number or passport of the customer shall be independently verified through the Integrated Population Registration System</b> database or through such other means as the Bank may approve.</p>

	<p>3) A mobile payment service provider shall ensure that the <b>subscriber identity module card and mobile phone number of its customer are registered</b>. (...)” (Central Bank of Kenya, 2014, p. 698)</p>
<p>Kenya Information and Communication s (Registration of SIM-cards) Regulations (2015)</p>	<p><b>§5 Requirements for registration</b></p> <p>“(I) A person who intends to register a <u>SIM</u>-card shall provide the following particulars to the telecommunications operator or <u>agent</u>-</p> <p>(a) full names;</p> <p>(b) identity card, service card, passport or alien card number (...)” (Communications Authority of Kenya, 2015, pp. 1000-1001).</p>
<p>Tiered <i>KYC</i>?</p>	<p>Yes. While the 2009 Act does not explicitly give room for a risk-based or tiered approach to <u>KYC</u>, it can be inferred that since <u>mobile money</u> providers can accept additional <u>KYC</u> information incrementally, e.g. a utility bill, employment or tax details, thus, a risk-based approach can be implemented. Regulatory authorities further may prescribe the extent to which and the circumstances under which incremental <u>KYC</u> documents may be requested (Muthiora, 2015).</p> <p>Aligning with FATF recommendations on balancing <u>financial inclusion</u> and integrity by adopting risk-based <i>CDD</i> procedures, there are tiered <u>KYC</u>-requirements for accessing <u>M-Pesa</u>, and wider financial services such as M-Shwari, depending on the fund/transaction size (di Castri, 2013; Safaricom, 2012).</p> <p><b>Whether this is still the case, remains open.</b></p>
<p><b>Conclusion: Seemingly, the regulations do not necessarily provide space for a humanitarian foundational ID, if not specifically authorized by the government. The authority of the government in determining, which form of ID is perceived as adequate, is confirmed. As previous sections already indicated, there is a substantive lack of legal IDs in Kenya, potentially because of these, when compared to Malawi, rather strict regulations.</b></p>	

## International Humanitarian Organisations

Relevant humanitarian actors utilizing <a href="#">e-transfers</a>		
Humanitarian organisations and the Kenyan government have been using (mobile) cash and <a href="#">vouchers</a> for many years; as part of recurrent drought and refugee assistance responses. Kenya's humanitarian cash system nonetheless remains fragmented, with limited coordination and harmonisation between the intervenors (Kondakhchyan et. al 2018).		
Kenyan Red Cross (KRCS)		
Year	Intervention Type	<a href="#">Open-loop?</a>
2016 and ongoing	Drought response	<a href="#">Open-loop</a> payment system, but restricted withdrawal options. Utilisation beyond intervention seems possible, but seemingly due to recipients already being registered <a href="#">M-Pesa</a> customers.
Description		
<a href="#">M-Pesa</a> is the default delivery <a href="#">mechanism</a> for the Kenyan Red Cross (KRCS) as part of an ongoing drought response (Kondakhchyan et. al, 2018). Eligible individuals are required to register their <a href="#">M-Pesa</a> phone numbers with the KRCS. Once a transfer is made, following verification, users can use their balance for <a href="#">e-transfers</a> or cash at licensed <a href="#">agents</a> (Kondakhchyan et. al, 2018). Kondakhchyan et. al (2018) imply, that there are special agreements between Safaricom and KRCS for delivering <a href="#">CBA</a> on the <a href="#">M-Pesa</a> platform, which needs to be verified during the interviews.		
Open Questions		
<ul style="list-style-type: none"> <li>- Which arrangements were made with Safaricom? Are there easier identification requirements (reduced <a href="#">KYC</a>) or do all recipients hold an official ID (as they seem to have already subscribed to <a href="#">M-Pesa</a> before the intervention)?</li> </ul>		

- Could recipients use the [e-transfer mechanism](#) beyond as [Open-loop](#) beyond the intervention?

UNHCR

Year	Intervention Type	Open-loop?
2012-2016	Refugee response	Potentially. Withdrawal restrictions however hint at a rather closed system.

Pre-paid bank cards were used by UNHCR to target vulnerable refugees with [CBA](#). Recipients received a pre-paid card, including a [PIN](#) code, at a bank branch. They could then withdraw money from [ATMs](#) in bank branches or through bank [agents](#), a Kenyan ID was not needed, but therefore, withdrawing and [authentication](#) with an Asylum seeker ID was restricted (Kondakhchyan et. al, 2018).

Open Questions

- Was deployed system [open-loop](#) (seemingly not)?
- Which restrictions occurred due to the non-citizen status of the recipients?

World Food Programme

Year	Intervention Type	Open-loop?
2015 and ongoing	Refugee response	No, <a href="#">mobile vouchers</a> . No <a href="#">financial inclusion</a> impacts.

Description

[Mobile vouchers](#) were introduced by WFP in 2015 in Kakuma refugee camp and further expanded to Daadab and Kalobeyei (Kondakhchyan et. al, 2018). Under the main programme “Bamba Chakula”, recipients got a [SIM](#) card, transfers through this [closed-loop mobile money](#) system, provided [vouchers](#) for purchase of food through selected traders in camps, by providing one’s Bamba Chakula phone number and a [PIN](#) for verification (Kondakhchyan et. al, 2018).

According to WFP (2018), the **restrictions on [CBA](#) to refugees in Kenya were implemented to align with governmental restrictions**, but WFP now wants to advocate for changes in national guidelines and the establishment of [cash transfer](#) systems that could make unrestricted cash transfers possible. Further, according to the new strategic plan for Kenya, **WFP (2018) wants to open Bamba Chakula** to other humanitarian agencies.

Open Questions

- What were underlying reasons for the proprietary solution? (Seemingly) [KYC](#)?
- Would such a proprietary solution be deployed again currently?
- To whom will the process of advocacy for an open solution be directed?

Concern Worldwide

Year	Intervention Type	Open-loop?
2008	Post-conflict relief	Not clear.

Recipients without ID as required for accessing [M-Pesa](#), nominated a trustworthy adult member of the household to receive cash on their behalf (Datta et. al, 2008).

**Conclusion: There are some hints, that humanitarian actors previously used payment channels which are [open-loop](#) enabled. How and what arrangements were reached based on humanitarian grounds, and whether long-term sustainable [financial inclusion](#), especially of previously un-documented took place, remains unclear.**

**Malawi- Interview questionnaire regulators**

(Reserve Bank of Malawi and Financial Intelligence Unit)

- 1) Your entity is responsible for monitoring and regulating [agent KYC](#) (RBM)  
/Your entity is responsible for compliance with [AML/CFT](#) regulations (FIU).

During the past year, Malawi has undergone a radical shift towards universal national ID coverage. Before that, individuals would sometimes be permitted to access [digital financial services](#) such as [mobile money](#), with a letter of the chief as proof of identity. Similarly, were [mobile money](#) providers able to register individuals who failed to provide officially recognized [credentials](#) for low-value transaction accounts. **With the upcoming regulations in December and the new national ID system, might these flexible approaches to [KYC](#)-standards be adjusted?**

- 2) Before the national ID-system was rolled-out, accessing [digital financial services](#) was restricted, a potential hindrance, also to humanitarian agencies and their interventions. Even today, some of the target groups, due to not possessing a Malawian ID, might fail to satisfy [KYC](#)-standards as laid out in the regulations. **Would using [mobile money](#) currently be possible during a humanitarian crisis, even if the recipients do not hold official ID [credentials](#)?**

- 3) Ideally, humanitarian agencies would like to have their target groups financially included (meaning that they at a minimum can make payments and transactions with the mechanism, and ideally, also access savings, insurance and credit schemes) beyond a humanitarian intervention. Is that currently possible for un-documented, for example with a tiered approach to [KYC](#)?

- 4) Humanitarian agencies usually issue functional IDs to their recipients for directing assistance efficiently. With the help of technology, these ID systems can be made highly trustworthy. A possible and internationally currently discussed approach relating to un-documented individuals thus would be the humanitarian support of governmental systems by providing a secure, trustworthy ID to yet un-documented. Generally, **would you think, that this approach could be accepted** for accessing basic [mobile money](#) systems (and

further mobile banking) if such an ID would **formally satisfy KYC-standards**, drawing from recent financial inclusion developments in Dzaleka camp? Could it further support un-documented citizens in receiving the national ID?

5) In some circumstances, when government-officials are absent, for example in a refugee camp, it might make sense that the registration and verification process for that kind of ID is solely supported by a humanitarian agency active in the community. Would that be possible?

6) Due to currently arising technology-trends, such an ID could provide information in a minimized, non-individualized form, without undermining the integrity of the claims. An individual could for example provide information about her age-group or area of residence and not the exact birthdate or address, when subscribing for e.g. mobile money. If the service provider can rely on the fact, that e.g. a humanitarian agency or government once verified the Personal Identifiable Information, could disclosing of minimized data be enough for KYC?

## **Malawi - Interview questionnaire Service Providers**

(Airtel and MTN; New Finance Bank)

- 1) Your entity is responsible for performing [due diligence](#) on your customers for satisfying [KYC](#)-standards, before allowing them to access your [digital financial services](#) via a registered [SIM](#).

During the past year, Malawi has undergone a radical shift towards universal national ID coverage. Before that, individuals would sometimes be permitted to access [mobile money](#) with a letter of the chief as proof of [identity](#). Similarly, was your organisation able to register individuals who failed to provide officially recognized [credentials](#) for low-value transaction accounts. **Are current and upcoming regulations, and the strong national ID system, calling for an adjustment of this flexible approach to [KYC](#)-standards?**

- 2) Before the national ID-system was rolled-out, accessing [digital financial services](#) was restricted, a potential hindrance also to humanitarian agencies and their interventions. Even today, some of the target groups, due to not possessing a Malawian ID, might fail to satisfy [KYC](#)-standards as laid out in the regulations. **Would sending cash over your [mobile money](#) service currently be possible during a humanitarian crisis, even if the recipients do not hold official ID [credentials](#)?**

- 3) Ideally, humanitarian agencies would like to have their target groups financially included (meaning that they at a minimum can make payments and transactions with the mechanism, and ideally, also access savings, insurance and credit schemes) beyond a humanitarian intervention. Is that currently possible for un-documented, for example with a tiered approach to [KYC](#)?

- 4) Humanitarian agencies usually issue functional IDs to their recipients for directing assistance efficiently. With the help of technology, these ID systems can be made highly trustworthy. A possible and internationally currently discussed approach relating to un-documented individuals thus would be the humanitarian support of governmental systems by providing a secure, trustworthy ID to yet un-documented. Generally, **would you think, that this**

**approach could be accepted** for accessing basic [mobile money](#) systems (and further mobile banking) if such an ID would **formally satisfy KYC-standards**?

5) In some circumstances, when government-officials are absent, for example in a refugee camp, it might make sense that the registration and verification processes for that kind of ID could be supported by a humanitarian agency active in the community, with according official procuration. Would that be possible?

6) Due to currently arising technology-trends, such an ID could provide information in a minimized, non-individualized form, without undermining the integrity of the claims. An individual could for example provide information about her age-group or area of residence and not the exact birthdate or address, when subscribing for e.g. [mobile money](#). If the service provider can rely on the fact, that e.g. a humanitarian agency or government once verified the Personal Identifiable Information, could disclosing of minimized data be enough for [KYC](#)?

## Malawi - Interview questionnaire - Humanitarian Organisations

(Malawi Red Cross, UNHCR, WFP, USAID, Oxfam)

1) Which kind of marginalisation and vulnerabilities can you think of apply to your target groups posing obstacles to receiving electronic cash-based assistance during or beyond a humanitarian crisis?

2) Your organisation utilizes/utilized some kind of [e-transfer](#) as [disaster](#) response.

a. Which [e-transfer](#) exactly?

b. What were your experiences with the [mechanism](#) (in terms of HA satisfaction, [efficiency](#), scalability etc.) in general?

c. Which intermediaries do/did you (have to) involve in the process?

d. Did your organisation reach a special agreement with regulators/service providers, is/was there a simplified/exemption to [KYC](#)-standards applicable to your target group?

e. Does/did the [e-transfer](#) mechanism(s) therefore enable HA to store, receive and send cash beyond the humanitarian intervention/crisis? What about access to credit, insurance and savings?

3) Due to the new national ID system, the conducive political environment for e-payment systems, do you think future humanitarian interventions now can increasingly make use of digital payment systems such as [mobile money](#)?

4) Some of your target groups might not be eligible to receive a national ID, due to e.g. being non-citizens, a hindrance for [KYC](#). Drawing from recent developments, **UNHCR was able to yield [financial inclusion](#) of refugees in Dzaleka camp with humanitarian IDs**. Accordingly, is a currently discussed approach using humanitarian [digital identities](#) to support [identity](#) claims of undocumented in general. Ideally, these [digital ID](#) would enable the recipient to be financially included due to [KYC](#)-alignment, also beyond a humanitarian intervention during a crisis. **Do you think, that this would be possible, if the**

**humanitarian agency formally collects and verifies the for [KYC](#) required information?**

**5)** Due to currently arising technology-trends, such an ID could provide information in a minimized, non-individualized form, without undermining the integrity of the claims. An individual could for example provide information about her age-group or area of residence and not the exact birthdate or address, when subscribing for e.g. [mobile money](#). If the service provider can rely on the fact, that e.g. a humanitarian agency or government once verified the Personal Identifiable Information, could disclosing of minimized data be enough for [KYC](#)?

**6)** Are you aware of any upcoming ([KYC](#)-)regulations potentially impacting the decision of transfer [modality](#)?

**7)** In general, do you have the perception that the national [KYC](#)-requirements conflict with your [mandate](#) as humanitarian organisation in any way, for example, data protection concerns or the difficulty of reaching [impartiality](#) in case of un-documented? What exactly?

## Appendix 8: All Interview Questionnaires – Kenyan Institutions

### Kenya- Interview questionnaire regulators

(CBK, CA)

1) Your entity is responsible for [KYC](#)-regulations (CBK) / Your entity is responsible for regulating the telecommunications industry.

When Safaricom started [M-Pesa](#), it had quite some discretion in determining its [KYC](#)-policies. Is it fair to say, that with, amongst others, the occurrence of wider financial services on the platform, this has changed in recent times?

2) Some of the targeted groups for humanitarian assistance, due to not possessing an officially recognized ID/being registered in IPRS and/or NIIMS, might fail to satisfy [KYC](#)-standards as laid out in the current regulations and Safaricom [AML](#) policies. Would using [mobile money](#) currently be possible, during a humanitarian crisis, even if the recipients do not hold official ID [credentials](#)?

3) Ideally, humanitarian agencies would like to have their target groups financially included (meaning that they at a minimum can make payments and transactions with the mechanism, and ideally, also access savings, insurance and credit schemes) beyond a humanitarian intervention. Is that currently possible for individuals not possessing the national or alien ID, for example with a tiered approach to [KYC](#)?

4) Humanitarian agencies usually issue functional IDs to their recipients for directing assistance efficiently. With the help of technology, these ID systems can be made highly trustworthy. A possible and internationally currently discussed approach relating to un-documented individuals thus would be the humanitarian support of governmental systems by providing a secure, trustworthy ID to yet un-documented.

a) Generally, **would you think, that this approach could be accepted** for accessing basic [mobile money](#) systems (and further mobile banking) if such an ID would **formally satisfy [KYC](#)-standards, even for the ones not qualifying for a national or alien ID?**

b) Would the individual still need to be registered in the IPRS/NIIMS?

c) Further, could it further support un-documented citizens in receiving the national ID?

5) The RAS has become sovereign in determining refugee status. In some circumstances, when government-officials are absent, and time is a factor, for example in a refugee camp, it might still make sense that the registration and verification process for that kind of ID is solely supported by a humanitarian agency active in the community. Would that be possible?

6) Due to currently arising technology-trends, such an ID could provide information in a minimized, non-individualized form, without undermining the integrity of the claims. An individual could for example provide information about her age-group or area of residence and not the exact birthdate or address, when subscribing for e.g. [mobile money](#). If the service provider (or government) can rely on the fact, that e.g. a humanitarian agency or government (or service provider) once verified the Personal Identifiable Information, could disclosing of minimized data be enough for [KYC](#)?

## Kenya- Interview questionnaire ID providers

(Ministry of Interior's Departments)

1) Your entity is responsible to provide for notification and registration of births and deaths (CRD) / Your entity is responsible for the national population register/ (IPRS Department) / for registering refugees (RAS) / to register and issue Identity cards (NRB).

When Safaricom started [M-Pesa](#), it had quite some discretion in determining its [KYC](#)-policies. Is it fair to say, that with, amongst others, the occurrence of wider financial services on the platform, this has changed in recent times?

2) Some of the targeted groups for humanitarian assistance, due to not possessing an officially recognized ID/being registered in IPRS and/or NIIMS, might fail to satisfy [KYC](#)-standards as laid out in the current regulations and Safaricom [AML](#) policies. Would using [mobile money](#) currently be possible, during a humanitarian crisis, even if the recipients do not hold official ID [credentials](#)?

3) Ideally, humanitarian agencies would like to have their target groups financially included (meaning that they at a minimum can make payments and transactions with the mechanism, and ideally, also access savings, insurance and credit schemes) beyond a humanitarian intervention. Is that currently possible for individuals not possessing the national or alien ID, for example with a tiered approach to [KYC](#)?

4) Humanitarian agencies usually issue functional IDs to their recipients for directing assistance efficiently. With the help of technology, these ID systems can be made highly trustworthy. A possible and internationally currently discussed approach relating to un-documented individuals thus would be the humanitarian support of governmental systems by providing a secure, trustworthy ID to yet un-documented.

d) Generally, **would you think, that this approach could be accepted** for accessing basic [mobile money](#) systems (and further mobile banking) if such an ID would **formally satisfy [KYC](#)-standards, even for the ones not qualifying for a national or alien ID?**

e) Would the individual still need to be registered in the IPRS/NIIMS?

f) Further, could it further support un-documented citizens in receiving the national ID?

5) The RAS has become sovereign in determining refugee status. In some circumstances, when government-officials are absent, and time is a factor, for example in a refugee camp, it might still make sense that the registration and verification process for that kind of ID is solely supported by a humanitarian agency active in the community. Would that be possible?

6) Due to currently arising technology-trends, such an ID could provide information in a minimized, non-individualized form, without undermining the integrity of the claims. An individual could for example provide information about her age-group or area of residence and not the exact birthdate or address, when subscribing for e.g. [mobile money](#). If the service provider (or government) can rely on the fact, that e.g. a humanitarian agency or government (or service provider) once verified the Personal Identifiable Information, could disclosing of minimized data be enough for [KYC](#)?

## Kenya - Interview questionnaire DFS Service Providers

(Safaricom)

1) Your entity is responsible for performing due diligence on your customers for satisfying KYC-standards, before allowing them to access your digital financial services via a registered SIM. When Safaricom started M-Pesa, it had quite a lot of discretion in determining its AML-policies. Is it fair to say, this has changed in recent times?

2) Some of the targeted groups for humanitarian assistance, due to not possessing an officially recognized ID, might fail to satisfy KYC-standards as laid out in the current regulations and Safaricom AML-policies. In the past, humanitarian agencies reached special agreements with Safaricom, e.g. taking over the risks associated with enrolling un-documented individuals into SIM cards for M-Pesa services. Would sending cash over the M-Pesa currently be possible during a humanitarian crisis, even if the recipients do not hold official ID credentials?

3) Ideally, humanitarian agencies would like to have their target groups financially included (meaning that they at a minimum can make payments and transactions with the mechanism, and ideally, also access savings, insurance and credit schemes) beyond a humanitarian intervention. Is that currently possible for un-documented, for example with a tiered approach to KYC?

4) Humanitarian agencies usually issue functional IDs to their recipients for directing assistance efficiently. With the help of technology, these ID systems can be made highly trustworthy and difficult to trick. A possible and internationally currently discussed approach relating to un-documented individuals thus would be the humanitarian provision of a secure, trustworthy ID to yet un-documented, entailing all the information required in KYC-regulations. In Kenya, a validation by Safaricom could be thought of. Generally, **would you think, that this approach could be accepted** for accessing SIM cards, basic mobile money systems (and further mobile banking)?

5) In some circumstances, when government-officials are absent, for example in a refugee camp, it might make sense that the registration and verification

processes for that kind of ID could be supported by a humanitarian agency active in the community, with according official procuration. Would that be possible?

6) Due to currently arising technology-trends, such an ID could provide information in a minimized, non-individualized form, without undermining the integrity of the claims. An individual could for example provide information about her age-group or area of residence and not the exact birthdate or address, when subscribing for e.g. [mobile money](#). If the service provider can rely on the fact, that e.g. a humanitarian agency or government once verified the Personal Identifiable Information, could disclosing of minimized data be enough for [KYC](#)?

## **Kenya - Interview questionnaire - Humanitarian Organisations**

(Kenya Red Cross, UNHCR, WFP, (IOM))

<p>1) Which kind of marginalisation and vulnerabilities can you think of apply to your target groups posing obstacles to receiving electronic cash-based assistance during or beyond a humanitarian crisis?</p>
<p>2) Your organisation utilizes/utilized some kind of <a href="#">e-transfer</a> as <a href="#">disaster</a> response.</p>
<p>a. Which <a href="#">e-transfer</a> exactly?</p>
<p>b. What were your experiences with the <a href="#">mechanism</a> (in terms of HA satisfaction, <a href="#">efficiency</a>, scalability etc.) in general?</p>
<p>c. Which intermediaries do/did you (have to) involve in the process?</p>
<p>d. Did your organisation reach a special agreement with regulators/service providers, are/were there simplifications/exemptions to <a href="#">KYC</a>-standards applicable to you and your target group?</p>
<p>e. Does/did the <a href="#">e-transfer</a> mechanism(s) therefore enable HA to store, receive and send cash beyond the humanitarian intervention/crisis? What about access to credit, insurance and savings?</p>
<p>f. To WFP: You are currently advocating for unrestricted cash transfers for refugee populations, implying that they could be financially included, even without alien ID. Can you give me an overview about the current developments?</p> <p>g. To UNHCR: The government has increasingly taken responsibility for refugee registration and issuance of according IDs, while seemingly preferring not issuing alien IDs. Do the IDs UNHCR issues currently have any legal power for subscribing to a <a href="#">SIM</a> card and <a href="#">M-Pesa</a>? Are there other potential solutions for refugees not holding the alien ID?</p>
<p>3) Some of your target groups are not eligible to receive a national/alien ID, a hindrance for <a href="#">KYC</a>. Accordingly, is a currently discussed approach using</p>

humanitarian [digital identities](#) to support [identity](#) claims of un-documented in general. Ideally, these [digital ID](#) would enable the recipient to be financially included due to [KYC](#)-alignment, also beyond a humanitarian emergency response. **Do you think, considering the political context and the national developments in ID systems, that this would be possible, if the humanitarian agency formally collects and verifies the for [KYC](#) required information?**

4) Due to currently arising technology-trends, such an ID could provide information in a minimized, non-individualized form, without undermining the integrity of the claims. An individual could for example provide information about her age-group or area of residence and not the exact birthdate or address, when subscribing for e.g. [mobile money](#). If the service provider can rely on the fact, that e.g. a humanitarian agency or government once verified the [Personal Identifiable Information](#), could disclosing of minimized data be enough for [KYC](#)?

5) Are you aware of any upcoming ([KYC](#)-)regulations potentially impacting the decision of transfer [modality](#)?

6) In general, do you have the perception that the national [KYC](#)-requirements conflict with your [mandate](#) as humanitarian organisation in any way, for example, data protection concerns or the difficulty of reaching [impartiality](#) in case of un-documented? What exactly?

## Appendix 9: Example of Cover Letter to Institutions in the Contexts



**The Netherlands  
Red Cross**

Head Office

Visiting address  
Anna van Saksenlaan 50

Postal address  
P.O. Box 28120  
2502 KC The Hague  
The Netherlands  
info@redcross.nl  
rodekruis.nl

IBAN NL26 INGB 0669 1137 00

Return Address: P.O. Box 28120, 2502 KC The Hague, The Netherlands

Place and date  
The Hague, 27.11.2018

Contact  
Jan Meyling  
jmeyling@rodekruis.nl  
+31(0)70 000 00 00

Regarding  
Research on Financial Inclusion

Dear [REDACTED]

As a member of the International Federation of Red Cross and Red Crescent Societies, does the Netherlands Red Cross Society (NLRC) investigate potentials of digital identities for a more efficient humanitarian assistance. Part of that research is attributed to the question, how and if this could be leveraged for financially including individuals without a national ID. To answer that question, [REDACTED] has been identified as a key stakeholder, as it works with individuals not holding a national ID.

With your support, we want to find out, if and how such a digital ID could sufficiently satisfy Know-Your-Customer regulations to allow for inclusion onto mobile-based payment systems. For that, we would like to conduct an approx. 30- to 45-minute-long interview with you. Broadly, we seek answers for following questions:

- How flexible are KYC-regulations for accessing digital financial services for individuals without national ID?
- Could the collection and disclosure of KYC-information in another than the national ID yield financial inclusion?
- Could a humanitarian organisation serve as collector and validator of information for that ID?

Upon request, a more detailed interview-guideline will be sent to you before the interview. Your contribution is extremely valuable to our research, so you will be, if desired, honourably mentioned as crucial contributor in the final version, which will be sent to you. Thank you in advance!

With kind regards,



Jan Meyling  
NLRC Researcher



Maarten van der Veen  
Initiator and Project Leader NLRC



Gumbi Gumbi  
Data Team Lead - Malawi Red Cross

 A part of the International Red Cross and Red Crescent Movement | Honorary President H.R.H. Princess Margriet of the Netherlands

 GOED DOEL

Kindly note

Ideally, the interview will be recorded for exact transcription, but consent for that can be withdrawn any time before and during the interview. You will be asked for consenting the recording again at the beginning of the interview. If consent is given, the records will be kept on a secure database and deleted 30 days after transcription, unless you want to have a copy.

Disclosure of name, position and any other information relating to your identity in the final research document can be freely determined by you.

You have the right to check the written version of conducted interview for desired adjustments, or to give overall disapproval. If you do not respond for over two weeks after receiving the written version of the interview, your approval will be assumed.

Before the interview will be conducted, you will be asked to sign a statement of informed consent, which will be made available to you prior the interview. If you prefer to express your informed consent in verbal form, you will be asked to do so at the beginning of the interview.

If you have any further questions, do not hesitate to reach out to Jan Meyling!

## Appendix 10: Example of Mail to Independent

Dear XX,

I am a huge fan of your XX work for XX on XX!

Let me quickly introduce myself: My name is Jan, and I am currently part of a Red Cross research around self-sovereign identities.

Currently, we are looking into an ID system supposed to make (digital) humanitarian assistance more efficient.

Ideally, the system could be further leveraged for supporting officially un(der)-documented individuals in accessing wider public services, for e.g. improved early action in cash transfer programming and recovery.

I am exploring, how and if this would be possible in Kenya&Malawi, through the analytical lens of subscribing to M-Pesa/Airtel Money with the identity system the Red Cross aims to provide, within the scope of my thesis.

Given your vast expertise in the subject matter, I would be more than happy to interview you about your personal opinion! Kindly let me know, if that would work out for you and I will be very happy to provide with more information.

Thank you in advance!

All the Best from the Dutch Red Cross and have a nice day

Jan Meyling

## Appendix 11: Summary Interviews

Context	Name	Current Position
Malawi	Wonderful Kunje	Data Analyst at MRCS
Malawi & General	Rajesh Bansal	Regional Director - Bankable Frontiers Association
Kenya	Anonymous	Project Leader at anonym. humanitarian agency
Kenya & General	Anna Kondakhchyan	ICT & DFS Adviser at Oxfam
General, Malawi & Kenya	Raul Zambrano	International Development Consultant
General	Kokoévi Sossouvi	Independent Consultant on DFS & CBA
General	Prof. Avner Levin	Professor of Law
General	Vincent Graf Narbel	ICT Adviser at International Committee of the Red Cross

## Summary Interview - Wonderful Kunje (WK)

***“People still don't see the importance of having the national ID.”***

### Position

Data Analyst at Malawi Red Cross Society (MRCS).

### Key Points

*The need for a (humanitarian) SSI*

- WK confirmed the sentiment retrieved from the literature, that the government rolled-out the **national ID system** with **vast coverage**, even in hard-to-reach areas
- Un-documented can still be registered in District Commissioner's (DC) offices in towns, hinting at a potential need for supporting still un-documented living in rural areas
- According to WK, humanitarian organizations **could thus support the further registration process of yet un-documented nationals** (aligning with KS, AK, RZ, RB, AL), by informing the government and getting an official to the field with according registration equipment
- After WK, **obtaining the national ID** would **not** be very **problematic** for Malawians, as even without another ID credential vouching for nationality, such as a letter of the chief, **individuals could acquire the ID by answering some questions** at the DC's office; thus, WK did not come across a situation, where the ID was being denied to an individual
- WK rather sees a current obstacle in individuals failing to see the added value of possessing the national ID, as accessing public services, such as healthcare, would still be possible with other ID credentials
- WK however also informed about the potential problematic of people living in the **border areas** to Mozambique, Tanzania and Zambia, who **could have issues in accessing the ID**
- WK further suggested, that **interoperability between the national ID** and a potential digital ID **would help support MRCS's** interventions (similar to AK, VG); WK informed, that recently, every SIM-card holder was asked to register their name against their phone number. In that sense, does WK suggest, that

this could support the link between a person's identity, ID and SIM [**in a centralized database**]; so far, the government's database and the service provider's database would not be linked (and thus, interoperable) yet

- While the government would be flexible in relation to humanitarian interventions, an agency would usually need to involve the government
- For example, in a recent intervention by MRCS, was the government involved in the selection process of recipients, as they were longer active in the communities of interest, than the MRCS. This materialized, inter alia, in the government determining the approximate location of the intervention and the targeting-process (two-level community-based self-targeting), as well as providing information on how many people would be in need for humanitarian assistance in these areas. Being part of the intervention, the government did require a list of names and location of the recipients
- Although the government's involvement, **WK sees no conflict of interest between the agency's operations and the government**
- **WK does not see a conflict of ethnic minorities** or other groups of people fearing to share their data with the government

#### *Feasibility of a humanitarian-agency supported digital ID for official KYC-alignment*

- According to WK, service providers could accept a non-governmental digital ID for KYC-alignment, if sufficiently economically incentivized
- If the government was not involved, WK says, that personal identifiable information could be maintained solely in the hands of the Red Cross
- **Network connectivity**, was identified as **key obstacle** to the current utility of a **digital ID system** (aligning with RZ)
- WK further suggested, that **capacities** of digital ID holders would need to be increased, before a successful deployment could take place (similar to AK, RZ, AL)
- Furthermore, there is a **need for sensitization** proving an added value for the digital ID due to the current flexibility towards authenticating for services with other forms of ID credentials

#### **Further Points**

*Marginalisation and vulnerabilities of target groups as potential obstacles to receiving electronic CBA*

- According to WK, **connectivity** is the biggest identified issue, specifically in rural areas. Recipients would need to **travel long distances** to obtain connectivity, potentially yielding a considerable **reduction** of the **value** retrieved from digital CBA
- Low agent's liquidity
- Security issues of holding non-digital cash
- Illiteracy specifically relating to authenticator loss/forgetting the PIN, and the associated delays due to authenticator recovery [hinting at **authenticator-recovery** for a digital ID being a crucial issue, especially **when immediate relief is important** (aligning with RZ)]
- **Hardware-possession** however is **not** considered **an issue**, relating to mobile money, as MRCS has low-cost phones disposable
- **KYC/lack of ID was not mentioned as exclusion factor** (aligning with KS)

*Agency's (MRSC) experience with e-transfer modality*

- Due to the issues outlined above, **utilizing mobile money is currently considered as impractical**, cash in envelopes is distributed with the help of a security provider (G4S)

## Summary Interview – Rajesh Bansal (RB)

Position
Asia Regional Director at Bankable Frontiers Association. Over twenty years of experience in designing electronic payment systems, electronic cash transfers, digital financial services, and electronic IDs to enable inclusive development.
Key Points
<p><i>The need for a (humanitarian) SSI</i></p> <p>i) <u>General</u></p> <ul style="list-style-type: none"><li>- Aligning with KS, AK, RZ, AL, according to RB, <b>should a humanitarian agency focus on its core mandate</b> – providing disaster relief – rather than <b>setting up parallel structures</b> besides governmental ones</li><li>- If a lack in legal identities was perceived as being problematic in a certain context, should a <b>humanitarian agency</b> rather consider <b>supporting national identification</b> efforts (RZ, KS, AK, AL, (WK))</li><li>- These efforts should not solely be restricted to nationals, but similarly apply to e.g. IDP or refugees - a humanitarian agency thus should advocate for their inclusion into the governmental ID scheme(s)</li></ul> <p>ii) <u>Context – Malawi</u></p> <ul style="list-style-type: none"><li>- After RB, the <b>NID</b>, based on its characteristics and wide distribution, will and <b>should be the only ID credential</b> for nationals to be accepted by RBM and its regulated FSPs <b>for (e-)KYC-compliance</b></li></ul> <p><i>The feasibility of a (humanitarian) foundational SSI</i></p> <p>i) <u>General</u></p> <ul style="list-style-type: none"><li>- If at all, RB sees a potential <b>use-case for SSI</b> in a <b>smaller</b> than national <b>scale</b> (aligning with AK, RZ) <b>depending</b> on the SSI'S <b>design's merits</b> and a compelling argument around the <b>need for data privacy</b>, due to e.g. persecution of minorities (contra RZ, KS and AK)</li><li>- RB furthermore strongly emphasizes on the need for contextual awareness and a robust understanding of applicable regulation, when deploying such a non-governmental identity system</li></ul>

ii) Context – Malawi

- RB confirms the sentiment, that recently, approaches to KYC were still a bit more flexible, as regulation lagged behind the national efforts to centralize previously a federated ID system
- Nonetheless, due the **vast effort** and spending **for rolling-out the NID**, providing an **SSI** striving for a more foundational purpose would most likely be considered as **duplication-effort**
- **Governmental acceptance** is, besides RB's general preference for supporting existing national infrastructures, perceived as a **core hindrance**. In the end, does RB still see a **possibility for providing an SSI in Malawi**. Due to the factors mentioned above, a successful deployment would however be **highly dependent** on the exact design, its merits, target group, scale of the programme and the ability to advocate for regulatory acceptance, together with an overall questionable normative desirability of such a parallel structure

**Discloser**

RB is, inter alia, an expert on digital ID and DFS. He has worked in Malawi and Kenya. For this interview, Malawi was focused on.

At the beginning of the interview, the regarded digital ID-system of 510/NLRC and the research were briefly introduced. According part of the interview, based on a confidentiality agreement, is not displayed here. Furthermore, based on an agreement to not record the conversation, solely a summary of the interview is displayed.

## Summary - Anonymous (A.)

***“Any system, which does not have the government involved in it, is inherently unsustainable”***

<b>Position</b>
Country project lead for a humanitarian agency in Kenya.
<b>Key Points</b>
<p><i>KYC in the humanitarian context</i></p> <ul style="list-style-type: none"><li>- No exemptions (yet) for accessing the M-Pesa system (people still need to possess official ID credentials to subscribe to the service), but this might change in the future</li><li>- As a separate step from accessing M-Pesa, exemptions were reached to provide SIM-cards</li></ul> <p><i>The feasibility of a (humanitarian) foundational SSI</i></p> <ul style="list-style-type: none"><li>- According to A., <b>currently not possible</b>. Deploying such an ID system will not automatically yield KYC-compliance. It <b>might however be feasible in the future</b>, as <b>Safaricom is not strictly obliged by law to solely accept the national ID</b> for KYC-compliance</li><li>- According to A., a <b>more feasible approach for now, would be advocating for exemptions</b> with the service provider - the <b>humanitarian organisation</b> would <b>absorb the KYC-requirements</b> to the individuals and be held accountable for adverse effects occurring due to individuals formally not complying with KYC (aligning with general statements of AL, VG, KS)</li><li>- Assuring a risk-appropriate approach could be done by <b>either having a strong internal identification system</b> [pathway for SSI and financial inclusion], or by <b>restricting the account’s capabilities</b> (KS and AL)</li><li>- According to A., if the functional identity system satisfies <b>conventional decision-maker metrics</b> (e.g. increases in efficiency, reduction of fraud and duplication) and is <b>interoperable</b> among various humanitarian actors yielding <b>intersectoral adoption</b>, there could be enough leverage to lobby for a foundational character (AL, AK). Thus, <b>if enough humanitarian agencies back</b></li></ul>

**the system, the regulating bodies could accept the ID system for formal KYC-compliance.** Therefore, access to wider financial services, without the humanitarian agency needing to absorb individual's KYC via an exemption, could be enabled

- Increasing **adoption** of such an ID system among various humanitarian actors thus would rather be likely **based on the improved conventional decision-making indicators, and not based on the ideals an SSI follows** [e.g. strong data protection and ownership of the individual].
- This implies the importance of **firstly implementing** a successful pilot (AL, AK, RZ, VG), **after** which a foundational ID system can be aimed for, meaning that a **foundational character is likely not achieved before or during** the pilot phase
- Conclusively, this means, that in Kenya, such a humanitarian ID would still firstly be deployed with the functional purpose of assistance delivery in a pilot (AL, AK), while a **foundational character would be an implicit, secondary goal** of an infrastructural approach
- However, similar to AL, AK, RZ, does A. point out the complexity of concept and technology as crucial obstacle to have policy makers engaging with both
- After A., the ideal would be a truly decentralized, interoperable system, certain standards and a code of conduct would apply to **various humanitarian and civil society actors being authorized to include individuals** into the system
- A **verification could be performed by two or three actors**, before identity credentials are issued. The ideal would thus not entail having a certain singular humanitarian agency being the sole executioner of SSI
- However, given the political agenda of the Kenyan government, but also more generally, the **government must be included** (AL, AK, KS, VG, RB, RZ) [this could imply that the government would want to take e.g. biometric data of any individual being included onto the system]

#### **Further Points**

*Marginalisation and vulnerabilities of target groups as potential obstacles to receiving electronic CBA*

- Due to M-Pesa being widely penetrated and both humanitarian and governmental actors utilizing the system, the concept of receiving an e-transfer is widely understood
- Illiteracy is not seen as a main obstacle for accessing the system, however, there are issues with the code of conduct within the agent-system (preventing recipients to receive the full CBA-amount), hinting at lack of mechanism-appropriateness for less experienced or literate individuals
- Targeting male household heads might undermine targeting other household's members

*Agency's experience with e-transfer modality (M-Pesa)*

- M-Pesa was and is used, involving Safaricom and its agent network
- Deployed only when context-appropriate, good experiences then
- **No explicit effect on financial inclusion** due to the interventions (KS). The recipients were only eligible to subscribe to the M-Pesa system because of prior ID ownership
- People are able to circumvent these requirements by utilizing some other person's ID, phone, SIM-card and account, but this is not a sustainable solution for the humanitarian sector

**Discloser**

At the beginning of the interview, the regarded digital ID-system of 510/NLRC and the research were briefly introduced. According part of the interview, based on a confidentiality agreement, is not displayed here.

AK was aware of the concept of an SSI beforehand and has contextual knowledge about Kenya in particular. Due to only giving explicit consent for the summarized version of the interview upon submission of this paper, the full version is not displayed here.

## Summary Interview - Anna Kondakhchyan (AK)

***“We’re exceptionally good at piloting, and we are exceptionally bad at scaling”***

<b>Position</b>
ICT in Humanitarian Programme Adviser - Digital Financial Services at Oxfam, with expertise in design and introduction of digital financial services in humanitarian and longer-term development settings.
<b>Key Points</b>
<p><i>KYC in the humanitarian context</i></p> <ul style="list-style-type: none"><li>- Oftentimes, complying with service providers’ requirements, such as the collection of biometric data, conflicts humanitarian data protection needs, but forces agencies to obey or pick a different delivery mechanism (VG, RZ, KS)</li><li>- AK is not aware of a context, in which reduced KYC would be permanently applicable (AL)</li></ul> <p><i>The need for a (humanitarian) SSI</i></p> <ul style="list-style-type: none"><li>- AK identifies a potential in SSI making humanitarian assistance more interoperable, efficient and preventing the current functional systems’ fragmentation (VG, AL, A.)</li><li>- Aligning with AL, KS, RZ, RB, providing a <b>foundational SSI</b> to recipients is <b>not</b> seen as part of the humanitarian <b>actors’ mandate</b>, focussing on its <b>provision might</b> therefore <b>deter</b> from <b>delivering</b> the actual <b>core responsibilities</b></li></ul> <p><i>The feasibility of a (humanitarian) foundational SSI</i></p> <p>i) <u>General</u></p> <ul style="list-style-type: none"><li>- While being a proven pathway for technological innovation to pilot on a small scale to build an initial use-case (VG, AL, A., RB, RZ), <b>scaling-up</b> from pilots would be a common <b>problem</b> in the humanitarian sphere</li><li>- Furthermore, like RZ, <b>technical scalability-issues</b> of the current applications are mentioned, besides <b>overall technical underdevelopment</b> (VG, RZ, AL)</li></ul>

- While still seeing a potential entry point for a functional humanitarian ID to provide access to wider services, according to AK, aligning with RZ, RB, VG, AL, KS and A., **gaining widespread acceptance** on the national, public level could be **difficult**, ultimately, even an SSI has to lie in the **hands of a government** (RZ, KS, RB, (VG, A.)) and some entity needs to hold the truth about identity claims
- AK eventually envisions a potential **SSI coexisting besides foundational public** systems, for example, if the design allowed for interacting between various MNOs (similar to WK, AL, VG)
- SSI is thus not seen as a replacement to national ID structures, **but as a potential new vehicle of providing some foundational ID functions**
- ii) Context – Kenya
- AK assumes, that M-Pesa would have been able to thrive because a lot of initial “closed-door discussions” between MNO Safaricom, donors and the government would have created an accommodating regulatory space for innovation; this could similarly apply to SSI given according high-level discussions, given the “good name” and agency might have established
- While Kenya is getting more restrictive in supporting refugees and the UNHCR-mandated refugee card to access wider services (assumably to decrease migration influxes), **compelling arguments** for an SSI (A., KS, RB, VG, RZ, AL), **engaging in discussions with the regulators ASAP** (RZ, KS) **and providing a long-term plan for scaling-up** (RZ), might make the regulator a bit more accepting
- However, the retention rate of humanitarian/development pilots is identified as an issue especially in Kenya
- In the end, does AK see not a pathway which would make the government lose control in providing legal identification beyond the camp-context, it would accordingly need to be involved in any effort for foundational systems from the start on

### Further Points

*Mentioned exclusion factors*

- Ak gives an example of a refugee in camp in Kenya: alphabetical and technological illiteracy - explicitly stating the need for an SSI's user-centricity
- and restricted mobility due to lack of legal identity

*Suggestions for further research*

- AK suggested contacting Caribou digital and looking into E-Estonia (similar to RZ and VG)

## Summary Interview – Raúl Zambrano (RZ)

**”Gap between practitioners of development and technology is getting bigger”**

### Position

International development expert on technology and governance at ICT for Development. RZ has supported the deployment and use of ICTs in nearly 100 developing countries to foster development agendas and promote social inclusion, working together with national governments, the private sector, and civil society organizations. A recent focus lies, inter alia, on open government and open data, social innovation, blockchain and AI and tackling these topics from a human development perspective.

### Key Points

*The need for a (humanitarian) SSI*

i) General

- Using the Rwandan genocide as example, RZ, as KS (and AK), points out, that persecution and violence directed towards a certain group can not be prevented by a digital ID. **Persecution** etc. would normally be based on from the **analogue world** retrievable information; e.g. people would know very well on the community level, whom to associate with which certain group etc.
- Relating to SSI, pushing its alleged advantages over other ID systems/concepts, e.g. the abstract concept of **data sovereignty as political right, rather are relevant in industrialized nations** with the means to digitally surveil their citizens
- As AL, AK, KS and RB, (A., WK) does RZ regard it as **public and national obligation to provide legal IDs, not** as a task of the **humanitarian sphere**
- A too rigid **focus** on the aspect **of self-sovereignty** might thus **undermine** a **solution** to the actual global challenge – a **lack of legal IDs**, especially in the global South
- Therefore, humanitarian actors should rather focus on advocating for desired changes the national ID system and rather focus on their core mandate of providing disaster relief

- RZ does not regard it as very likely, that an ID provided by a humanitarian agency can support accessing wider public services, unless the ID was connected well to the governmental system, e.g. its database
  - A humanitarian ID serving wider foundational purposes would, if at all, most likely occur on a smaller scale - **nation-wide adoption would be highly unrealistic** (similar to AL, VG, AK, RB, (A.))
- ii) Context - Malawi
- Providing SSI in such a context, thus would not prevent persecution etc. because it would not be occurring in the digital but analogue space
  - Providing an SSI hence might not necessarily be geared towards the most urgent humanitarian and development needs
  - RZ thus suggests a participatory approach, to investigate whether SSI is really the best and most desired way to approach the problems the communities face during the design phase

*The feasibility of a (humanitarian) foundational SSI*

- i) General
- Aligning with AK and KS, does RZ advocate for engaging with responsible decision makers, e.g. national ID and regulatory authorities immediately
  - Aligning with RB, VG and AK, while national adoption is considered as unlikely, a potential **pilot could**, provided proven advantages in relation to the incumbent national ID system (A., AK, VG, KS, RB, AL) **be used to entice a desired change on the national level**
  - RZ does not see it as feasible to have people registered solely by a humanitarian organization acting as verifier for a foundational SSI
  - According to RZ, some technological characteristics of existing blockchain applications, while expected to improve in the future, pose a considerable obstacle in scaling-up an SSI-pilot to the national level (e.g. scalability, efficiency and complexity). Here, RZ mentions the US-state Illinois, which, like the ID2020 initiative, terminated initial SSI-efforts due to **scalability-issues of blockchain-applications**
- ii) Context – Malawi
- Digital connectivity, literacy etc. currently pose a considerable obstacle to a successful deployment of an SSI

- The current system's complexity might further undermine a sustainable utilization, maintenance and ownership within the communities, after the humanitarian intervention itself has stopped, implying a need for capacity-building

## Further Points

### *Connecting development and technology*

- RZ strongly emphasises on connecting technology utilization to the most pressing contextual development needs
- However, would tech-providers normally not respond to immediate development needs, but allege providing solutions without knowing the exact problems, increasing the gap between technology and development practitioners
- Accordingly, does RZ highly **suggest reading into governmental development plans** (and the SDGs) to **identify political priorities and development needs** when considering a pilot

### *Humanitarian-development nexus*

#### i) General

- Connecting humanitarian assistance to longer-term, more sustainable development would require factoring in three basic principles: **i) a demand-driven need ii) community ownership, and iii) a participatory approach** during or before the humanitarian intervention, otherwise a long-term utilization will not take place

#### ii) Context

- This means, in the context of Malawi and Kenya, but also on a more general level, that there needs to be i) a demand for specifically an SSI ii) a design allowing for maintenance, governance and utilization of the system on the community-level without being dependent on external expertise in the long-term, by e.g. connecting to local public and private entities and building relevant capacities iii) a bottom-up approach for the local appropriation of the system

## Summary Interview – Kokoévi Sossouvi (KS)

*“Collaboration is always stronger than coercion”*

### Position

Independent Consultant on Cash Transfers, Digital Financial Services and Market-based Strategies. Currently concerned about innovative cash programming (concept formulation, intervention strategy design, process improvement, project management, etc.) and digital payments (landscape assessment, system requirements, user journey mapping, use case recommendations, etc.).

### Key Points

#### *KYC in the humanitarian context*

- Humanitarian agencies themselves can establish a business relationship with service providers when distributing SIM-cards, which are then associated with the agency, thus yielding a risk-based KYC for MNOs
- Normally, if the humanitarian agency holds the business relationship, e.g. a mobile wallet with reduced KYC could become permanent, if it was actively used beyond the humanitarian intervention

#### *The need for a (humanitarian) SSI*

- Commonly, after best practice, the assisting humanitarian agency would facilitate for recipients obtaining a national/local ID
- According to KS, this approach and lobbying at Central Banks for reduced KYC and according satisfaction with e.g. a UNHCR refugee ID, was sufficient for humanitarian interventions (aligning with WK, (RB, RZ, AL))
- Furthermore, as tiered KYC would usually align with the transactional capacities of the population, which usually also live out of the scope of strong digital ecosystems to make further appropriate use of the system beyond the intervention, there is **not necessarily a need for full KYC-compliance and open-loop accessibility**
- KS, similar to RZ, AK, AL, RB, is concerned that a humanitarian ID striving towards a more **foundational purpose could deter** from the humanitarian agencies' core mandate as well as the **governmental obligation to provide**

**public identification** infrastructure - hindering governments to organically grow the relevant capacity

- A **core focus** should thus lie on **strengthening the governmental capacity to roll-out universal national identification** ((WK), RZ, RB, AK) **not setting up parallel systems**; furthermore, financial inclusion should always happen within the national legislative realm, not outside
- The client for an SSI thus should be the governments (AK), not the humanitarian community
- Similar to RZ and AK, does KS argue, that a government could persecute a minority, or prevent a minority to subscribe to a financial service, making it difficult to counteract as humanitarian organisation

#### *The feasibility of a (humanitarian) foundational SSI*

- For e.g. efficient taxation, **governments would have a vested interest in having all citizens adequately identified** – thus an interest in closing the ID-gap. **If** therefore a **government would see an added value** to its national structures when utilizing a more sophisticated SSI-system (VG, A., RZ, AK, AL, RB), they could be keen on implementing it
- On the contrary, if a government would feel its sovereignty being undermined (AL, RZ, AK, RB, VG, A.), it would most likely act adversely
- Additionally, **if only a part of the population was included** solely under a foundational humanitarian ID scheme the government could have issues to get this part of the population back into the public scheme

#### **Further Points**

##### *Humanitarian-development nexus*

- According to KS, humanitarian agencies oftentimes do not make use of existing public structures, thus setting-up parallel structures lacking sufficient efforts to link to public disaster preparedness
- This would undermine linking humanitarian assistance to longer-term development efforts and creating synergies between e.g. social protection and humanitarian assistance

##### *Questionable financial inclusion impacts of CBA-mechanisms*

- KS further points out, that financial inclusion impacts on recipients would normally be marginal, as people affected normally would stop using the mechanism beyond cashing-out assistance, due to lack of funds and digital ecosystems and closed lines by MNO if the recipient does not use the mechanism repeatedly
- This creates the question, whether deploying a non-governmental ID to enhance financial inclusion really responds to the most pressing needs of a given context
- If a line is closed and the HA has no ID, re-gaining access is difficult

*Suggestions for further research*

- KS suggested looking into ID4D

## Summary Interview – Prof. Avner Levin (AL)

**“At what point do you stop assisting and start taking over things that the state should be doing?”**

### Position

Professor at Ryerson University’s Law and Business Department, Director of the Ryerson’s Law Research Centre and fellow at the Privacy and Big Data Institute.

### Key Points

#### *KYC in the humanitarian context*

- i) Reduced KYC for recipients
  - AL strongly emphasizes, that concerns about people affected needing to comply with KYC would lead the discussion into the wrong direction. Firstly, KYC would regulate entities, not individuals. Secondly, would context determine appropriateness of seeking KYC-compliance, for example, a permanent business relationship. Facing a disaster, or even protracted crisis, humanitarian agencies should insist on people affected not needing to comply with KYC
  - AL accordingly implies, that humanitarian agencies should/could take over the risks associated with a third party not performing due diligence on the person affected; usually one would find a legal basis for an agency being able to vouch for the individuals they assist without the requirement individual due diligence (KS, (AK, VG, A.))
  - KYC from a policy perspective (reducing ML/TF) would actually apply to the agency’s level more than to the individual level of a human affected, as the agency itself has greater access to funds, possibilities to manipulate etc.
- ii) Reduced KYC beyond a humanitarian intervention
  - AL is not aware of a context, where a reduced/simplified KYC beyond the scope of immediate disaster relief was applicable to recipients of humanitarian assistance (AK), contra KS
  - Relating that to KYC from a policy perspective, AL, similar to KS, sees difficulties in making a compelling argument for the humanitarian agencies’ target groups not needing to formally comply with KYC the longer, the intervention’s time-frame

gets; arguments for a simplified KYC thus would rather focus around a potential lack in infrastructure and the temporary urgency arising from a crisis

- One thus should rather strive towards providing the required (public) infrastructure to fully comply with KYC (similar to AK, KS, RB, RZ, (WK))
- Potential exemptions could be lobbied for in e.g. a refugee camp, where people might be on a longer-term basis and still are dependent on a reduced KYC to access services
- Agencies however should focus on their core mandate and argue for people affected not needing to comply with KYC in the first place

#### *Humanitarian ID serving legal purpose*

- A digital humanitarian ID could potentially possess the same characteristics of a governmental ID in a certain context, hinting at the issue of governmental acceptance not only being based on the grounds of an existing simplified KYC

#### *The need for a (humanitarian) SSI*

- AL expresses normative and practical concerns, like RZ, VG, AK, KS, A. and RB, about undermining governmental sovereignty, if humanitarian agencies were to take over too many tasks of a government in the long run
- For long-term stability, the state should thus, whenever feasible, be included into longer-term interventions, humanitarian agencies should rather focus on their core mandate of providing disaster relief and the most pressing needs within a given context
- Thus, while seeing a normative desirability of giving individuals more control about their identity, sees AL a task in lobbying for governmental SSI-acceptance on an international, rather than national level, without the provider being humanitarian (AK, RZ, RB, KS (WK))

#### *The feasibility of a (humanitarian) foundational SSI*

- Generally, AL confirms the potential of protecting individual data on the one hand, while ensuring transparency to align with AML policies and ensuring accountability of the humanitarian actors in such a system
- However, a non-governmental ID being accepted for KYC might rather occur in the traditional financial (banking) context itself, implying that acceptance

amongst these stakeholders would pose the initial step towards a more foundational function of according system, not in the context of providing humanitarian assistance (AK)

- If such a system could prove utility increases for the service provider, AL assumes wider acceptance as likely, as long as the underlying system is well understood by regulators (VG, RZ, AK, A., RB, (WK))
- For a successful use case in the humanitarian sphere, a controlled experiment, e.g. in a refugee camp, could represent the first marginal step for scaling-up pilots (AK, RB, VG, A., RZ)
- Relating to an SSI utilizing blockchain as underlying software architecture, AL identifies encryption-techniques disguising the identity of an individual as conflicting the traditional AML/CTF perspective, hence urging for analytical tools to analyse the transactions in a transparent way to add value to accounting. Then, e.g. a government could accept a more foundational purpose due to being able to comprehend individual transactions, without necessarily retrieving PII
- The transparency and (alleged) immutability of such a system, however, could vice versa yield massive data protection concerns, if exploited as a surveillance tool

### **Further Points**

#### *Notification instead of free consent*

- AL strongly advocates for humanitarian agencies not to collect informed consent from people affected, as free consent could firstly not be given when dependent on receiving assistance (VG), and secondly, because informed consent would leave too much space for handling sensitive data irresponsibly, such as incautious disclosure to third parties
- Instead, AL lobbies for notifying people about the exact utilization of their collected data, as this would create a stricter definitory space concerning the exact data disclosure towards other parties etc. and thus increase obligations to handle sensitive data responsibly

#### *Context*

- AL assumes that Malawi might have a more flexible approach towards KYC-compliance when compared to Kenya and correlates that with Kenya being a more “stable” country

## Summary Interview - Vincent Graf Narbel (VG)

***“All refers to understanding data flows, because that's really what we're talking about here”***

<b>Position</b>
Advisor Digital Transformation and Data at the International Committee of the Red Cross.
<b>Key Points</b>
<p><i>KYC in the humanitarian context</i></p> <ul style="list-style-type: none"><li>i) <u>General</u><ul style="list-style-type: none"><li>- Aligning with AL and KS, does VG see a possibility to waive KYC-requirements based on humanitarian mandates</li><li>- Depending on the humanitarian disaster (e.g. war and conflict vs. responding to an earthquake), different data protection needs arise and how much priority inclusionary practices get</li><li>- Accordingly, is the consideration whether a minimum KYC can be complied with geared towards a risk-assessment</li><li>- According to VG, were some of ICRC's interventions terminated because the local, regional or national authorities' requirements for data disclosure were deemed too dangerous</li></ul></li><li>ii) <u>Context – Kenya</u><ul style="list-style-type: none"><li>- In Kenya, sharing data with the government may not be problematic in a lot of circumstances, however, sharing information with internationally active companies, such as the subsidiary of Vodafone, Safaricom, might be; data flows then are becoming more complex and third-party access may not be prevented</li></ul></li></ul> <p><i>The feasibility of a (humanitarian) foundational SSI</i></p> <ul style="list-style-type: none"><li>- Aligning with AK, does VG imply, that even within a distributed (identity) network, there would be somebody as an ultimate holder of the “truth”, e.g. a consortium serving as certifier nodes</li></ul>

- Similar to RZ, KS, AL, AK and RB, (A.), does VG express that an identity solution **ultimately will have to include a sovereign government**
- VG sees, aligning with A., AK, AL, RZ and RB, a (unlikely) pathway towards a more foundational adoption in building up on **potential pilots** deploying the technology as **functional** in receiving assistance, and then being able to show decision makers, that e.g. transparency, accountability, privacy-by-design etc. are enhanced – **and then** taking it towards a more **foundational** level
- Pointing out the complexity and yet immaturity of the technology's software backbone, VG identifies the **issue** of explaining decision makers the alleged advantages in an **understandable way** (AL, A., AK, RZ); a potential approach could be using examples from the analogue world to explain characteristics properly
- Like RZ, VG advocates for asking communities on the ground, what their most urgent needs would be; however, VG identifies the difficulty to ask that upfront, because of the **uncertainty of future technological developments**
- Besides feasibility and ethical studies before deploying any technology, even if findings would show that most of the target group is formerly able and capable to utilize a certain mechanism, will there always be the need to assure that some individuals still not able to utilize the mechanism have alternatives to receive assistance
- VG furthermore urges for **contextual adaption** (RZ, RB, AK, (WK)), as there are, for example, communities, where proxies normally receive assistance [inherently a conflict with KYC-standards]; as **nations have the sovereignty** in opposing or favouring a certain ID system, **standardization of an SSI might be difficult to implement**
- VG believes, similar to AL and RZ, that the underlying technology for SSI is still far away from reaching a stage able to produce a convincing use-case beyond greater interoperability and data sharing
- VG further has the viewpoint, that evolving technologies in general should not be tested on vulnerable people with their urgent needs, but rather "in the lab" and checked against classical do no harm principles whenever an advancement is made

## Further Points

### *Points for further research*

- VG brought up France Connect as an example, where a federated solution is based on private, trusted verifiers and distributors of individual identities
- Aligning with AK and RZ, does VG refer to E-Estonia
- Handbook on Data Protection in Humanitarian Action

### *Informed Consent*

- Like AL, does VG express, that informed consent does not apply to humanitarian settings, making a risk-proportionate approach necessary for the humanitarian agency

## Appendix 12: Full Interviews

### Full Interview - Wonderful Kunje (WK)

Discloser
WK has a lot of knowledge concerning the CBA-operations of MRCS and the relevant context of the target groups. He is not involved in the project of 510.

JM:

Thank you for giving me the opportunity to talk to you! If you don't mind, I would give you a brief overview about what we are doing [at 510/NLRC) and then I'm very happy to just dive into some questions, if that's fine. What we are basically researching here right now is that because of a new technology we might potentially be able to have a very trustworthy digital identity which we could use - once all the other problems like connectivity and mobile phone penetration are solved - to identify recipients [of humanitarian assistance] more easy and faster than currently. Once we have such an identity system put in place, we hopefully could also use this identity system for the people to apply for other services such as new mobile money, but this is really about the future. Now, coming to my questions, to my understanding, you are working around cash-based assistance, is that correct to say?

WK:

Yes.

JM:

Very good. And if I would be able to ask a very open question for the beginning, if you would need to state some marginalization or vulnerabilities normally applying to the target groups or recipients of cash-based assistance, which would in a way restrict the ability of receiving cash assistance on electronic mechanisms, would there be something coming to your mind?

WK:

I would basically say that the **difficulties to access is the network**. There are some **rural areas which have no network**. In that context, they have money in their phones and everything, but **to access, they need to travel long distances to access that**

**money** which is a bit expensive going in town. **Accessing that money might make the value of the money lower** than they are expecting. For example, if someone used to get \$100, and they're using \$30 for transport, the money wouldn't cover the needs of them. That's an issue. The second issue I would say, the people in the rural areas, if we were to distribute a massive amount of money, the **distributors might not have that kind of money** to help those kind of people. In terms of **security**, they wouldn't hold so much money with them but, the capacity of them is very low. So, first, rural areas need to have that capacity to hold some of money. Unless, if those people can be offered vouchers, so that maybe they can use **vouchers** to buy stuff.

JM:

That is very insightful. Thank you for that. Would you think, that literacy or for example, possessing a mobile phone, is an issue as well?

WK:

Yeah, that's another issue. But then, I would think in the context, that when providing them with monetary assistance, you would provide phones for them as well. **We have cheap phones disposable**, but then, we don't have a network in that place so that's why we didn't want to tackle that issue. And also, on the **illiteracy** part, we have some old people that **cannot remember their password**. It will be a need for them for accessing the money, they should maybe renew their PIN code to withdraw the money. What if it's an emergency, **they wait maybe for a day so that it can be restored**. And most of all, old people, they use maybe their grandchildren to help them access the money, just because they are not sure on the counting part or maybe about the whole system, their child or their grandchild might take money from them without their consent since they have access to it. Cause when someone is withdrawing money they would just give out the PIN code or just send through the agent and they will get money. So those issues we are mostly facing, those kind of situations.

JM:

So, given all these issues, would you currently think that a voucher system makes more sense for cash delivery?

WK:

It makes sense. It's easier, but then, to get to that place, you have to know how to talk with them. That's the first goal. The first thing, I would suggest, you have to make sure that the network coverage is there. If the coverage is there, then the second thing will be providing phones so the people will be accessing the money, that's the second thing. The third thing, **capacity of those people** in those areas, how we can increase it. **Maybe somebody could be going there once a week.** There are many ways, but you have to look at it on the grass-root level. But the first thing is just network, because I'm trying to avoid them travelling from their areas to the town to access the money, the value of the money will reduce. But then, we have to find the means whereby someone should be going to those areas so that people can get their money. But then, that person going to those areas, you also have to take care of the security of that person. That person will be carrying a lot of money. Thus, the security. So, there are so many things involved. That's what I'd say.

JM:

Thank you so much for the answers. That was already very insightful! So that's probably the reason why you're currently working together with G4S and not the mobile network operators. If I may ask, is G4S bringing the money in envelopes, or are they using ATMs? Or how exactly can I think about the system?

WK:

**They're bringing the money in envelopes.** They keep the money at the bank. So, every morning they get the money from the banks and go to the field for distribution. So, when they're going to this distribution, they take the exact money that would be distributed on that day.

JM:

And so, the people know when they receive cash. So, they go to the distribution points and just provide their identity credentials whatsoever which shows they are eligible for the cash transfer.

WK:

This is what happened. **The Red Cross staff is on the spot and we have G4S on the spot as well.** We have to call the names of the beneficiaries which are eligible to receive. We **give them some ration card**, some cards for them to receive. So, what

we normally do, we scan the card, we see the amount of money that person is supposed to receive, and we confirm in our systems, we check that person is eligible to receive that kind of money. So, if they are, we send them to G4S and G4S also has a list of people, so that's **where we normally thumb print on the sheets**. So, after they found the thumb print, they check the names against the amount of money that supposed to receive so they give the money in cash. That's the basic system we use.

JM:

And then, again, when we were talking about this digital identity we're talking about the future. When issues like network connectivity or also the agent network might be improved, literacy levels, phone coverage and so on, would you think, if these factors would be put in place, the people you're currently working with, would be able to use a transfer mechanism such as mobile money with that ID? For example, for being financially included? Because how the system sounds right now, people receive the money, but they cannot use the system to also store their money or access loans or transfer the money on the device. And ideally, I mean a lot of people might not be able to make use of such a system, if they need cash to satisfy their urgent needs; but ideally, there would have the opportunity to be financially included, would you think that is possible? [I obviously talked too long and did not narrow down the scope of my question sufficiently enough to guide the interviewee well].

WK:

In terms of technology in town, the technology is available. Transferring money in mobile phones going to banks and from banks to mobile phones is very possible right now, but the only limitation I would say, are the rural areas, the first thing is the **network**. On top of the network, it's the **sensitization of the people**, they need to know, how they can access the money and everything. That's the only limit right now, I would say. If it's a town set-up, it's easy, we have branches everywhere.

JM:

To my understanding, the Malawian government had massive efforts in rolling out a new identity system, they gave out these new identity cards, which can also be read by a card-reader. Do you know, if every one of the recipients of the Red Cross' interventions has these identity cards? [Because I felt like I misguided the interviewee with my last questions, I decided to approach the issues around humanitarian digital

ID acceptance by the government / due diligence performers by asking about the national ID system].

WK:

People have them, the identity cards, but I can't come up with the exact percentage of how many people are left [out]. But from asking around, **I think almost 80% of the people have their identity cards** and actually, it was for free and **they are still registering more people**. But then, I'm not sure about the exact percentage. **If everyone would have that identity and we would have a digital system identification system, things would be easier**. Cause also, **it was advised that everyone should register their phone numbers against their names**. At least right now, **everyone who's using a phone, their numbers are registered to their name**. Everyone will be attached to one thing. So, **you would find a phone number, that number would link to the ID and that ID would link to the person**. So, we are in the early stages of having one data base where all information of the people will be there. We are getting there. The only issue is we **haven't reached the stage of linking the customer digital ID's and the phone numbers**, but we're getting there. The mobile service provider has that information and the government has that information, but there is no link between that two information though. If this system is to work, we would work on how to link the data base of the government and the data base of the service provider. That's the approach I would see if we would meet those kinds of things.

JM:

And when are you talking about this centralized database, you mean the governmental database and not the data base for your own record keeping, right?

WK:

Yeah, this is a government data base that we have, but it's not that much.

JM:

So, you said many people already have the national identity and more people will be enrolled. Do you think, some people might still be having problems in getting the national identity because they may be don't have the driver license or maybe don't get

a letter from the chief and so on to prove that they're actually citizens of Malawi. Do you think that would be an issue for some?

WK:

Yes, it becomes an issue in places which are closer to the other countries like Mozambique and Zambia and even Tanzania. Those people, **they might not get registered**. But then, I feel like **if you are a natural born citizen of Malawi**, if you prove yourself to be Malawian **you get registered**. **If you don't get a letter from the chief or something because of political reasons, we can go to the DC's office**, the district commissioner, who may help you in dealing with that situation. But I **haven't come across the situation of being Malawian and being denied the right to get that ID**. They just ask you a few questions, "where are you from?" and everything. If you manage to answer that, you get it. I am sure. If people are having issues, if people are not having identity cards, it's maybe only because they are just lazy to get registered. But there are, from what I heard, a lot of people how are just idle to go the district office. I think that's another limitation, **people don't really know the importance of having that ID**.

JM:

And would you think they don't see the importance in having a national ID because they basically can access everything important like governmental services or a SIM card with the kind of ID they already have? So, is that why they don't seem important?

WK:

Yeah, cause **they don't really know where they could use that**. **Especially** those people **in the rural areas**. Like "Why should I have an ID? What am I going to get of this? Let it be." So that's another problem, even although the **government did a lot of sensitization** telling people that if you won't have the national ID, you might not get some free services. The government was saying you will need the national ID so you will get services, for example for a job application. So, people are like "Okay, if I am sick, I go to the hospital, I still can access the services". That's what they are concerned about. If they go to the hospital and they get services, that's cool, cause they're old, maybe they don't feel to apply for a job, and they don't think it's necessary [to have a national ID] as long as they can access the hospital with or without the

national ID. The government did a lot sensitization on the job part, but then, **people still don't see the importance of having the national ID.**

JM:

Kind of makes sense, right? Like for example, if I live in the rural area and I work in farming, so I'm not formally employed and I'm not applying for formal job, but I'm in the informal sector, I might not really see the point, for now at least, to have this national ID. But do you think, because the government rolled out the identity system so much, do you think that accessing services, like a hospital, or maybe also subscribing to SIM card, might become more restricted in the future with other identity credentials than the national ID? Because the government has put such so much effort into the system.

WK:

Yeah, for getting the Malawian passport you need to show the national ID. So, you can't get a passport, if you don't have a national ID. I'm not sure about the driver's license. But then, a person in the rural areas does not want to have a passport. It seems like people don't really have a reason why they should have the national ID. **Well, according to our registration, I think around 90% of the people had national IDs.** The government really reached every corner of Malawi to register them and it was free. They [the government] went in rural areas, to every place, you [as individual] wouldn't travel so long for getting registered; but right now, it's only in the town, the **DC's office, that's the only place where people can get registered [now] if you are not registered [yet].**

JM:

I see. So, if you are not registered now and if you are living in a rural area, it might be very difficult to obtain the national ID, for now at least.

WK:

Yes.

JM:

I see. And do you think, that a humanitarian organization if the ID is at some point needed by people living in the rural areas and if people cannot travel so far, do you think the humanitarian organizations like the Red Cross could support the government and the unregistered people in registering for that national ID?

WK:

Yeah, I think the best way to do that, is to **communicate with the government, cause they have the equipment. So, the best way is to talk to the government. Let's say you are registering in a certain district, you find out the people who are not registered you get that equipment, meet the people get them registered, do the verification and everything.** That's how you can do it. You have to follow the people.

JM:

What I was wondering, coming back to the border areas, to these people who can maybe not prove that they are Malawian citizens but they're still living in Malawi and they might be dependent for access services and maybe they are not able to prove their citizenship. So they might not have the national ID, but they also might not have other identities which I accepted for, let's say the hospital, would there be a way to support these people in accessing services, or will the government be reluctant to give these kind of people, maybe being not Malawian, but still living in Malawi to issue credentials to them as well?

WK:

I would give an example for Mwanza, it's close to the border of Mozambique. Maybe 20% of the people who would access the hospital are from Mozambique. The hospitals don't ask them for any details. If you are sick, you just go to the hospital you access everything. And I think, on the border also. I'm not sure on the border. I think they just have to get a border pass. I think it's only for applications [to governmental jobs] when you need to provide your national ID. That's the only situation I've seen they ask for a national ID.

JM:

So, I can, even with the national ID system, if I want to have a SIM card, or if I want to subscribe to, for example mobile money, I can still just basically to show any identity, whatever I have in this would be fine?

WK:

Yeah, I used my passport to register my mobile phone, mobile money, everything. [WK before indicated, that one needs to show the national ID for obtaining the passport,

thus implying the same trust proxy level, however whether this is the case for less formal credentials, is unclear].

JM:

And other people could still use any anything else, like the letter of the local chief and so on to be accepted by for example the mobile money providers?

WK:

**They use the voter's card, the national ID, driver's license, and the passport and even school IDs.** Those are the main things. Cause I feel like in Malawi, we do not have much of faking IDs. **We don't have so much identity theft** in Malawi, that's the good thing about it.

JM:

Now, being very specific. Again, what we are are looking into is digital identity for humanitarian assistance. And once we are able to have a system which is electronic, if the connectivity, the phones etcetera are there and everything is okay, but for example the people coming from Mozambique from the border region who may not have a Mozambican passport for example, so they still might need to show something to the mobile network operators. Would you think, that the Red Cross for example provides this kind of digital identity, disclosing whatever needed, like the name or the address, would you think this would also be accepted by, for example, mobile money providers to subscribe to SIM cards and mobile money?

WK:

If I understood you correctly, someone from Mozambique wants to access money from Malawi?

JM:

I mean, it's very theoretically right. Another example: Imagine there is a humanitarian crisis, a refugee crisis. So maybe, we have some refugees, for example in Dzaleka Camp, who don't have an identity card to support their claims, that they are a specific person, and to give them the chance to access mobile money and so on. The Red Cross now would issue an identity to these undocumented people. Do you think this, the Red Cross giving this digital identity, do you think this would be accepted by mobile providers for example?

WK:

Yeah, **they would accept it**, as long as they are getting money out of it. It's very possible.

JM:

So, as long as one bargains well, it should be fine, basically.

WK:

Yes.

JM:

Are you aware of any upcoming regulations maybe changing the way people can access services now, based on the roll-out of national identities?

WK:

Nothing so far.

JM:

Just a small question before I'm happy to release you. Do you have to feeling as a humanitarian organization that there's a conflict of interest between you and the government sometimes when you try to support people in need?

WK:

I've never come across something like that. **The government is a bit flexible, the only thing is, whenever we're doing anything, we have to involve the government.** The **government** actually is going to **guide us in this area**. I think you might want to help it's in this area or in this kind of assistance. That's what they told us. But it's for the good, because **they stayed longer in the districts**. So, they get to know everything. We just go in the district and tell them "We have this amount of money and we want to provide assistance, these are the people we are looking for, how can we assist them?". This is when the government comes and tells us "no, you don't have to use this approach", cause maybe they are already doing that [providing assistance to that target group]. So, we work hand in hand with the government. **We don't have experiences in terms of conflicts of interest with the government.** They are advising us on the best ways how to handle the communities.

JM:

I see. So, the government basically decides to whom you can give assistance, is that fair to say or is that too extreme to say?

WK:

Not exactly, but **they just tell us the gaps which are in the communities.**

JM:

So they already have identified the communities and the people most in need basically, and then they give suggestions to whom to...

WK:

For example, this activity we are doing for cash distribution. We approached the government since they are already doing the distributions. We were like "ok, we want to distribute this cash assistance to the people". So, **they give us the locations like maybe in this area, so and so many people are in need and in this area, so many people.** So what we actually did, **we were working with the government within the community, we would involve the community to pick the needy among themselves.** So that's the approach the government gives. So we would gather the whole village in one place and say "okay, among these people, among yourselves, who is the most vulnerable?" And the community would be like "this and that person are the most vulnerable". And we would ask the whole community: "Is this true?" And they would say "Yes", if it's not true, they say "no". And this is the approach with the government so we should adopt. But they do not have the name. We work with them primarily in the communities.

JM:

But isn't there a danger, potentially, that if you have this approach of self-selection, that the most marginalized of the community - because they may not have the social contacts in the community - that they cannot self-select them[selves] when you gather the whole village?

WK:

Okay, the thing is, if we just go in the village and start selecting people, we might not reach out to some other people that stay for in areas. All we had to do, before we

started the selection, we had to give them criteria on the type of people we are looking for. We had those people who don't have food at the moment. They maybe eat once a day, and we had another, those with small farming land, those with large families with many people that are depending on them, but they can't be able to feed them. We had those criteria. We had a whole group of people selecting the people and we had the, we call them the Village Community Protection Committee - VCPC, those are the structures in the villages, so we told them, these structures in the villages, that they should write names of the people they know in the village which are vulnerable. After that, we take the list from the community and the list from the VCPC and we should compare the two. If a person exists in both lists, we endorse them. If they are on one list, we enter the community and be like: "Ok, the VCPC selected these people - who is the most vulnerable among those people"? The government suggested we use this approach cause with this community-based approach they should choose their own people and ask. This is the approach we are using lately.

JM:

That's very interesting! So basically, the government supports you, but they are not really demanding you to pick, but you will go by this community-based approach and it seems to work out so far, right?

WK:

Yes. They just told us this approach and we were like: "ok, this sounds fair". Cause we went to the government and we told them "we need people" and the government was like "We don't have people, we have numbers. If you want people, this is the way we would select those people."

JM:

And the government, so eventually, they have the numbers, you go to the community, do the self-selection process and then you give out the assistance in whichever way, but the government does not know the names. That's what you said, right, so they don't know who will receive assistance from the Red Cross in the end.

WK:

No, we can share the list with the government, **we do share the list with the government.**

JM:

You do share the list, ok. And what is included on the list? The name and the address?

WK:

Not really, but for this exercise, the government is planning to give out maize to the people, we are giving out cash. So, what we normally do is just the name and the location of where they are. Those are the information we are sharing mostly. Because the government right now won't need so much details of them since we work with them when we are selecting the people. So, all they have to know is the names and give out the maize. So, **they have access to the names of the people and the location of where to find them.**

JM:

Do you think this will always be required in the future, or at least in the next years, that the government knows the name at least?

WK:

It depends on what kind of; if the government is planning on assisting those people, I don't think it's necessary for them to get the name. **If it was 100% Red Cross work, then I guess the data will still be with us. We have no reason to share them if they have no use for them. Since they right now want to use the data to do more distribution, they need to have it.**

JM:

Interesting. Is there maybe like an **ethnic minority which my feet be fearful about the government** knowing their name or is that not a problem right now?

WK:

**That's not a problem** right now.

JM:

Ok great. And generally, when the government does not support the exercise, then as you said, they would usually not require about the individuals receiving assistance.

WK:

We don't like the fact of sharing data, if it's not needed.

JM:

Completely agree. Thank you so much for what I took way more time than I wanted to but it was very, very interesting and enlightening from me. Is there anything else from your side if you want to state or what you have in mind?

WK:

No, I have nothing.

**End of Interview**

## Full Interview - Anonymous (A.)

### Discloser

Based on a confidentiality agreement is the identity of A. and his/her humanitarian organisation disguised, passages hinting at either identity were thus modified. A. was made aware about the digital ID-project and the according ID system currently being developed within the 510 team at the beginning of the interview. Besides having contextual knowledge, A. was aware of the concept of SSI before the interview.

JM:

Thank you so much for coming back to me! Before diving in, I would like to start with a more open question. Generally, if you would need to define certain vulnerabilities or marginalizations generally applying to recipients of humanitarian cash assistance, specifically around receiving e-payments, are there certain vulnerabilities you can think of?

A.:

Vulnerability of the people, or failures of the delivery mechanism, like risks associated with the delivery mechanism?

JM:

The latter, in which way might such a [e-transfer] delivery mechanism restrict someone's' capability in making appropriate use of such a mechanism?

A.:

In the contexts of Kenya, I would say that basically **M-Pesa is so widely penetrated** that the idea of receiving a cash transfer is **pretty well understood**. After my experience so far, for humanitarian purposes, I think the **issue is about guaranteeing**, that the person is **spending** it [the cash] in the **right way**. **Both the humanitarian organisation and the government have been working with that modality** in response for quite a while. So, I think the **community is quite well sensitized** today with that modality. I think the main issue you will hear about is that if

you give money to a man, he will take the money and "run off". People say that as a joke, but there is some underlying seriousness with that issue.

JM:

So that would mean that the primary target group would rather be the females of the households and not the men?

A.:

You surely cannot generalize, but it is an issue to keep in mind in the context.

JM: Very interesting! After your experience, is there also a problem with accessing the M-Pesa network, for example due to connectivity, illiteracy or an insufficient agent network or mobile phone penetration?

A.:

More broadly, M-Pesa is not always the default mechanism. For example, the governmental social protection payments are essentially done on a prepaid bank account, which is like a limited bank account with, I think, two of the National Bank providers. The reason for this is because they trialled M-Pesa and found it to be inappropriate because **people sometimes could be tricked** into giving their money away.

JM:

Apart from the government preferring prepaid bank accounts, to my understanding, the default mechanism of the humanitarian organisation is still the M-Pesa system, right?

A.:

It is indeed. You would better speak to them than to me though [referring to the cash delegates of the humanitarian organisation]. As far as I understand, **illiterate** people can still make use of M-Pesa, they however **rely** a bit more on the **agent**. I think you have a lot of true believers who think cash [over M-Pesa] is appropriate in any circumstance, but the limits of that modality clearly have to be defined. And there are a lot of those in Kenya, where M-Pesa is not really appropriate. That being said, M-Pesa is a bit flexible. So there is the government-mandated way of looking at it, where a person going through the Know-Your-Customer requirements, applies to a SIM-card

and subscribes to an account and accesses M-Pesa through their mobile phones, but **in reality, people share accounts**, share SIM-cards and share mobile phones or even pay other people for SIM-cards, so there is a lot of variety.

JM:

And jumping to the ID cards and the Know-Your-Customer regulations, as you said, people are able to circumvent these requirements. So, is it [not possessing ID cards] still an issue [to the humanitarian organisation] for delivering on the M-Pesa system, at least to some?

A.:

That's a bit tricky. People share M-Pesa accounts. What the humanitarian organisation does, and again, it would be better if I put you into contact with the cash team, but what they do in theory is taking the M-Pesa API of the beneficiary and validate that against the name they registered with at Safaricom, however I'm not sure whether you can take somebody else's Safaricom account to receive cash.

JM:

I'm happy to talk to the cash team of the humanitarian organisation later, as it sounds like they could give me some valuable insights! So, it sounds like in order to receive M-Pesa from the humanitarian organisation, you definitely already need to be registered with Safaricom, which implies that you need to have an ID card, because you need this to be registered for the service, or did I misunderstand it?

A.:

In theory that's what it is, but the reality could be something else. I think, you could nominate someone else to receive cash for you, but I'm not sure.

JM:

Alright. Sounds like there might be some exemptions applicable to the operations of the humanitarian organisation when it comes to registering human affected on the system.

A.:

No, not on M-Pesa, **not yet**.

JM:

Okay. So, there were no exemptions applicable in the past to the humanitarian organisation for registering.

A.:

No, not through M-Pesa. As far as I understand, **there was some in the past for distributing SIM-cards** but not on M-Pesa.

JM:

Could a registration for a SIM-card automatically yield registration for M-Pesa [without providing additional information such as an ID]?

A.:

**No.** You need to register for M-Pesa the same way you register for a SIM-card. The way M-Pesa works, you also need to register at a vendor. So, you also need to present your ID just for M-Pesa. Therefore, these are two separate steps.

JM:

Interesting. When M-Pesa was utilized as a mechanism, were there restrictions attached to the human affected, meaning they could not use the system after the intervention ended, or could people use the mechanism beyond the humanitarian intervention?

A.:

They just used the normal commercial M-Pesa. So, it was people's normal M-Pesa account. Some people might have joined M-Pesa because of this [the CBA], but the humanitarian organisation did not "distribute" M-Pesa accounts, so there was nothing special about the M-Pesa accounts that we used. **For now. In the future, exemptions might be applicable.**

JM:

Relating to that, given the issue of individuals not being able to register for an M-Pesa account because of not holding an officially recognized ID, would it be thinkable, that for example the humanitarian organisation issues an ID holding certain information about a person, collected and verified from sides of the humanitarian organisation? Could that be leveraged for subscribing to the M-Pesa system? Or is that too far away to think about right now?

A.:

This is kind of a “shades of grey” situation. The way this could be operationalised is by looking into exemptions. What's happening now is an **organisation "taking over"** the [individual] **Know-Your-Customer regulations**. So **not** what one would directly consider as **complying** with KYC requirements, but **rather an organisation using its good name to assure they will work in compliance with KYC**. For example, the way I understand it, **Safaricom is not legally obliged to take somebody's National ID. Essentially, the only way they can do this** [assuring individual KYC-compliance], **is however using the national ID at this point**. In the future, **one could convince them to accept another form of ID, but Kenya is still miles away from that**.

What you could look into now, are **exemptions, meaning a trusted organization absorbing the individual KYC**.

JM:

Interesting! So, in practice, this could mean that for internal purposes [of the humanitarian organization], a digital ID could be issued to recipients of humanitarian assistance. However, these individual recipients would not [with that ID] directly register to Safaricom, but the humanitarian organization itself would be "taking over" the risk associated with individual KYC for the individual.

A.:

Yes. The concrete nature of how that would be done exactly is a bit unclear, but one [as humanitarian organisation] **could probably provide a list of names and other required information to Safaricom**.

JM:

So that would mean, in a way, formally the Know-Your-Customer regulations would be complied with, because you would basically hand out all the information about a recipient of humanitarian cash, e.g. address, name, age and so on, but not supporting these claim with an ID credential, but supporting it rather with the established trust, a humanitarian organization has with Safaricom.

A.:

Not exactly, this is a little bit off. This is what I meant with shades of grey. But, because that's a new thing, there is no paved road for this. So, what it would be, the

humanitarian organisation would absorb the risk. So, if this happens, one would need to make sure the proper measures and counter-measures, the checks and balances, are in place. Basically, **making sure, negative consequences** potentially arising, such as fraud are **not happening**. **Either** by checking and **making sure of having a good idea about the individuals' identity, or by limiting** what they are able to do with the account. However, I think what is really important here, lies in the fine details. Probably, in the way it would be, in the framing which is done at the moment, **if the humanitarian organisation would absorb the risk**, and something were to go wrong, **the humanitarian organisation would be found of not complying with Know-Your Customer. By vouching for the individuals, it would suffer the negative consequences by absorbing the risks associated with KYC**. What you are talking about, is having a system, where the information you provide, actually comply with Know-Your-Customer. These negative consequences would then not be in the realm of Know-Your-Customer, but some other regulation.

JM:

I am very sorry, could you repeat that? [there were some issues with the connectivity]

A.:

The situation you outline, is that a humanitarian organization would provide the system providing information which fulfil KYC requirements. This is not the case with an exemption. Basically, what would happen with an exemption, and this is a very new process; so it's not the hard and past truth, for example, **if the humanitarian organisation would absorb the risk, they would essentially go to Safaricom**, and they hand out the SIM card and the M-Pesa account. If something goes wrong, if they give out the account and haven't checked, or haven't done the KYC requirements and if there is some kind of issue, so for example fraud on the system, they are not liable, because they officially have performed the requirements. So, if there is evidence of fraud or some other situation occurring, on some of the situation occurring they [the humanitarian organisation and not Safaricom] will be punished. So, this is the risk they absorb.

JM:

So, let me try to wrap this up, because I'm not sure if I could understand you correctly due to the connection. The way I understood it, is that the humanitarian organization

would absorb the risk in a way, that they would be solely responsible for obtaining the recipients data, and that Safaricom would not necessarily have individualized present of these recipients of assistance and whenever anything would go wrong, the humanitarian organization would be held accountable. Meaning, that as long as they kind of would have a good identification system put in place for the recipients and nothing goes wrong that it would be fine, basically not complying with the official KYC regulations. [Note: Due to connectivity issues, I obviously partially missed the relevant message].

A.:

Yes. Either by ensuring that the identification is good, or by limiting the account. Either can be done. **Basically, you just need to assure Safaricom, that KYC-regulation will not be an issue to their operations** [relating to the target groups].

JM:

Very interesting. Probably the more risk-appropriate approach somebody would choose, would be restricting the accounts or what you can do with it, as long as not everybody [relating to all involved stakeholders] is assured that the identification system which is put in place is very strong. Is that fair to say?

A.: Yeah, maybe, but this is all a bit up in the air. This is a maybe for now. But it's a possibility.

JM:

So what do you think, I mean, we're talking in theory here and hypotheses, that once people [I was not very clear here in hindsight, but I meant the service providers, such as Safaricom and the regulators, as responsible entities for KYC-compliance and regulations] would be assured the identification system would be strong enough that people [this time, the recipients of humanitarian assistance] actually can subscribe to the system, perform transactions and build a financial identity? And would it also be potentially sufficient for the officially undocumented individuals also to access broader financial services?

A.:

I mean, this is the hope. But this is really miles away. **Trying to bring this to the regulator in Kenya, you would not get a comment on this at the moment.**

JM:

So this implies, the best way to approach this right now, would be to have a solid digital identity system, which would be deployed to Kenya, and use that for the humanitarian identification system for now, and try to build up a certain financial history of the recipients of humanitarian assistance and with that, at some point maybe have the leverage to talk to the regulators to also enable these individuals with the digital ID, plus the financial history, to access wider financial services.

A.:

Yeah. I mean, I think this is the approach one would take. But, it's a bit more general than that, this is just **not something that's widely understood. It's a complex idea, it relies a lot on technology, that doesn't really resonate** with the idea of the people seeing these kind of things, which is more like a list of names. I had a meeting with IOM [International Organisation for Migration] this morning, I briefly discussed it with them, but they - the concept is just, I think very high level, and **people cannot really understand what it is and you cannot expect policy makers at this point to really engage with it.** And I think, people can be very resistant to what they do not understand and to what is not either public or evident.

JM:

Would you have any idea, how we could approach that problematic of people not really understanding the concept of, for example, a self-sovereign digital identity? If we would for example present some nice power point slides [inappropriate polemic from my side], or a running app, with an illiterate-friendly interface and so on and just like, guiding people through the process, or what would you think would be helpful?

A.:

Honestly, I think what **you need**, is a cold, **hard statistic**. You need to show that it works, and you need to proof it. People want to see evidence. I think people won't buy into a power point. People need to see that it's working and something they want to engage with.

JM:

So, the approach would be deploying this kind of digital identity system, seeing if it's working out well, and then showing the use-case to government officials and proving

that it's working. So basically, start deploying, and then using that as leverage in the future [towards the government].

A,:

Yeah, so, I mean, I think this is really context-specific. I mean, there is technology, which is comparable in some ways, like Red Rose [a digital ID provider officially utilizing blockchain technology, however only focussing on one part of the humanitarian funding chain; for more information relate to Appendix 1 - glossary] for example. Red Rose, they've seen it, they've seen the gains, but when you look at the kind of decision makers in an organisation, they don't necessarily need understand how it works. They just need to know it works and that they can see the benefits. And they can also see the clear negatives, for example a 2% flat rate on it [relating to the transaction fees on that system]. So, we're talking about some very conventional decision making. In this way, **I think you're not going to be engaged in this idea of the humanitarian imperative around a foundational ID, because you need to deal with the practical decision making of humanitarian programming**, what the governments see, and they [the government] also have their own agenda, and **they do not necessarily want to see this fluid border, people being able to bypass the government**. This is not necessarily attractive.

JM:

Again, I had some issues understanding you due to connectivity issues, after you talked about Red Rose having already established a use case, which allows people to see the gains of such a system, after that you, if I understood you correctly, implied that if another system such as a self-sovereign identity, would be able to communicate these gains relating to efficiency for example, that this could be leveraged for convincing decision-makers, but given the current political economy in Kenya - we currently have strong movement towards centralizing an identity system where everybody, not only the nationals in the country, basically should be registered, that this might counteract might kind of counteract even if you would have successful use case. Did I understand you correctly? [Note: I obviously did not, as A. was primarily referring to decision makers within the humanitarian sphere, while I assumed A. was talking about decision makers within the Kenyan government, which A. only mentioned as a side note].

A.:

So, basically what I was saying, is that with this kind of technology, that the technical level is almost separated from the decision-making level. People making decisions of whether or not to use Red Rose, they do not have to engage so much with how it fundamentally works, they will look more at conventional, traditional decision-making indicators. So, when the decision maker at the HQ can look at the pilot from Red Rose, they can say, "ah yes, there is this much more efficiency, it is this much easier, we reached people with these and that gains of efficiency", they can see this, and this is clear. And they can also see, for example what Red Rose does, is a 2% flat rate, you cannot customize the system, and then it's the same conventional decision-making process, like it's not really scalable. So, to this level, you cannot really bring the argument of bringing something that has this moon-shot change with this fundamental imperative behind it, this is secondary to the conventional decision making. So, you can say, we have this digital identity of this firm, that can provide the benefits of Red Rose but also solve the issues we have had last time, then it's something which will be adopted. You can then also say, this solution furthermore provides essentially a backdoor to other humanitarian organisations [relating to the interoperability of such a system] providing assistance, beneficiaries having some kind of fundamental digital ID which may be useful for them in the future, this is good, this what they'd like to see. They like this kind of thing; however, you need to have the conventional decision-making indicators put in place first. Decision makers are not solely going to engage with the technical elements and the technical potential. They also need the benefit in terms on which they can base their decision without just looking into how the system works.

JM:

So, the first step would be about proving the benefits to the decision makers within the humanitarian organisations and then using that as a leverage to talk to the regulators

A.:

Yes. **You cannot do anything without a good pilot. Unless you have a use-case, no one will look at it.** And once they [the humanitarian agencies] have a bit experience with it, they can see, what they can do [relating to involving in discussions with the regulators].

JM:

Interesting! Then, talking in hypotheses again, assuming such an identity system would have become foundational in the future, say, 10, 15, 20, years from now, would you think it's possible, that a humanitarian organisation could serve as sole collector and verifier of an individual to include him or her on the system, or would you think that a government official always would be required as an information collector?

A.:

15 years is a long time as a time scale, you don't know what the state of technology will be, you don't know what the state of the government will be. I mean, I think you can come in on what you'd like to see. **For me, I really see that this is a decentralized system, and for me it's not about a particular humanitarian organisation being the sole executor of identity. For me, having a proper identity system, it's decentralized in every way, where you can have certain standards and a code of conduct which one can sign into, numerous humanitarian organisations and civil society actors, and make them all verifiers of digital identity.** Maybe you would need to be verified by two, three different actors. So, I think, I can't speak about what will happen, but you can talk about the things that I think would be ideal for the system. **And I don't think that the ideal situation is having one humanitarian organisation as sole executioner of self-sovereign identity.** But if you're working in a country, a hundred percent, **all of the time, what is ideal and what you should always aim for, is a fair and willing government. I think that any system, which does not have the government involved in it, is inherently unsustainable.** I can't see any time in the next 15 years where the government is going to say they don't mind a sovereign identity being given out that they don't have a saying in it. I realistically cannot think of any scenario where this would be going to happen. You need to see it as a march of progress you need to see how these organisations work. For me, the way I see it, is for an organization, like an UN agency, any organization in the humanitarian sphere, to "buy in" into such as system, they need to see clear gains in terms of coordination, operability, in terms of inclusion for the beneficiaries, improving the kind of assistance you can deliver, that should really be at the heart, and once it is adopted, I don't think that anybody will roll back from it. I think it will be continually growing, it will be continually adapting, and with every organisation, with every incident of organizations' adaptation, the system

should improve. In this way, if you have the system developing, we won't have to roll back. Rather this way, we would have a system which will be mainstreamed, and then you will have the government needing to engage with it. But, **the government might just ban it**. That is also possible, but I think that, **if you had enough influential backers behind it**, who really say "we like to use the system, because we like the concept behind it, but first and foremost, **because it makes our operations better, it makes us better in what we're doing**", I think this is really how such a system could bring a meaningful change.

JM:

Thank you very much for these interesting insights! If I understood correctly, the way you would aim for such an identity system to grow, or even become foundational, it would rather still start with the functional purpose of delivering humanitarian assistance more efficient. Reaching foundationally would firstly be rather a secondary, more implicit purpose. Then, once more individuals and organizations adopt that ID, it would become foundational.

A.:

Exactly.

**End of interview**

## Full Interview – Raúl Zambrano (RZ)

### Discloser

At the beginning of the interview, the regarded digital ID system of 510/NLRC was briefly introduced. According part of the interview, based on a confidentiality agreement, is not displayed here. Furthermore, were some subsequent passages, based on their confidentiality or informality, excluded. RZ was aware of the concept of SSI and has working experience in both relevant contexts.

JM:

So, what I also initially said, what I liked about your whitepaper, is that you pointed out that digital divides in the developing contexts, oftentimes mirroring analogue inequalities, could undermine, uhm, the potential utilization, or an inclusive utilization of such a complex and yet not very well, obviously, well understood technology in certain contexts, and I would, I mean that's very basic, but I would like to ask you what could be core exclusion factors for such system deployment in a certain country?

RZ:

Well that's a big question. So, let me give me an example. 20 years ago, 25 years ago, when the internet first came, it was actually 93, 92, the same issues came up, right? So, the internet was supposed to be this wonderful, decentralised equalitarian blablabla, all this nonsense which never happened. We had the same sort of, atmosphere, claims and stuff and so on and so forth. And you then found two schools of thought. One is what I call the "techy", the "techies" which will tell you that my technology is going to solve everything. So, it was gathered, buy it, you know, drop it, airdrop it and that's it. People will come. So that's what's happening in blockchain in part. And the other one is more the, our approach, which is, I mean, "our" meaning, the government, the humanitarian, which is "Wait a second, it's not so simple". When you go to Malawi, I've been in Malawi, you have never been there, then you should go because it would be so difficult for people to use anything, cause they're lacking basic stuff. Communication, income, health, education. So, dropping things on people doesn't work. We need something else. So, what you need to do, and this is my approach, **you need to connect technology to development, suppose ID**. People

have no ID. Ok, so can technology help get me an ID? So, the question is, is not a new issue, it's being on the table for centuries, ID, specifically in the modern society is very important. I am no one. I have no rights. I don't exist with no ID; a legal ID. So, it's a very old issue. So, the question you need to ask: "Does blockchain contribute anything new to ID?" And if so, tell me what, which we couldn't do before. **So, is it only the need for Self-Sovereign ID, or is it my access to ID is limited?** And you think, just like Kenya, being there, people take kids, they have no ID, birth-registration. So, they don't exist as citizens, you know, as children. It's terrible. So, can you give a blockchain to children to solve this and that's what you have to wonder, is this really the solution? But maybe it is, but maybe it's not. So, we need to really take a look at this. So again, connecting technology to development is really important, cause I don't want to add a new dimension. "So, in all, you guys, you're so old fashioned, you don't use the internet, you're obsolete" - Well, that's not the point. The point is, that we have so many needs on the ground and if you want to bring something new, please, connect that innovation to our needs. You say "Oh, yes, yes, this gonna help us advance, you know, the solution". Development field is actually a long-term, it's been in place for so many years. So, these guys working on governance human rights, humanitarian aid, they have expertise, they know what's going on. And I find this **gap between practitioners of development and technology is getting bigger. Blockchains are so complicated. So, explain that to a government's expert.** So, what happens, either they're saying "Forget it" or they get overrun, right? So, they're saying "Whatever you want to do, we do" which is what happens in most cases. It's like artificial intelligence today. So, you need to close that gap. You need to, you need to get in touch with the practitioners. People have been doing this for many, many years and are saying "**What are you guys facing every day? What are the challenges?, right? Then, me as the innovator, you know, supposedly, I could think "How can I help?" But what is happening today is the opposite.** These guys would tell you "Oh, I have the solution for everything. You come here, I don't have to come to you, come to me, right, and I have the solution!" That doesn't work! That's what I said in my paper, right? You cannot do this. It will not work. It's like the internet. You know, it didn't work. Which country has developed since the internet? Not a single one! Mention one! Not one! They haven't developed as, you know, like, Korea, Taiwan or Malaysia, happened until the 1990. Those countries were developing countries 50 years ago. Name one country since 1995 which has developed like Korea. Not one! Why? So,

that's, that are the challenges, right? And we then made the claim that, with the internet approaching, or AI, ID solution, for advancing, contacting, I think the answer is "yes", a qualitative yes, right? But if you tackle the right things, not because it's new, it's going to, somehow magically soar. The answer to your question is: It's **important** to get **context** into the equation. Every country is different. Even developing countries are not all the same, right? I mean, Malawi is not Sudan. Sudan is not Nepal. Nepal is not Myanmar. So, there are different shades of grey here. So, you have aware. But, they share a lot of common things. Which is lack of education, lack of services, lack of public services, lack of health and so on and so forth in different degrees. So, my job as a, as somebody who embraces both technology and development, is to see which technologies can actually help us improve such conditions, right? So, that's one part of the answer. The other one is when you mentioned that humanitarian aid you guys want to make become **more sustainable**. Meaning that the, meaning **that if you do something in country X can we make it part of the country itself once we leave?** That's a very old discussion we had in the UNDP years ago. So, in the UNDP, or in the UN, they have this twofold strategy, which is, okay, if you have a situation in, let's say, I don't know, in Yemen and we deploy smart communications for peacekeeping operations, which we had all the time in the UN, **how can we then leave that infrastructure**, so that the country when it's, when it's in the post-, **post-conflict situation, can leverage that and then use it for development**. And that's a very old discussion. And the answer is: You can, but you also need to build when you're doing the peacekeeping operations, or whatever the humanitarian operations is, to **build capacity in the country**. Cause if you have this, suppose you have this AI, smart, you know, platform to communications, who are you gonna hire when you leave the country? So, who's gonna run this, you know, **security and maintenance, governance you know, you need to build those things, while** you're doing all this **humanitarian** thing. But what you find, is that **people doing humanitarian aid don't do development**, they're used to their own thing. Now they want to help people and, you know, get your, use your cash, buy stuff and then I leave the country. So, there's a gap and you need to also try to find the institutional connections, too. Because it's not people, it's institutions. **You need to build organizations, public and private, who can then take this on in the future**. And this is a **challenge**, because when you have a war, people are moving out of the country, they will come back, or, there's **no capacity**. So, that's a challenge. Probably **they should be connected**. So, in the case

of blockchains, when you do your analysis, ask the same question. If you deploy this in Malawi, which is a very different country, to **ensure capacity**. Red Cross and sort of, say, **take this on to the government** of Malawi. **If you don't factor these issues in from the beginning, it won't, it will not work.** You must check that the pilots are thinking about these very basic issues from the beginning. If the government is to make this sustainable, then we need to see what do we need to do from day number one, so that in day number X, final day X, we can call someone in Malawi and say "here guys, it's yours, take it". I could do the easy thing, but it's not realistic. I need to build, you know, it's like a wave, it gets bigger and bigger and then it goes to the beach and then dissolves, right?

JM:

Thank you so much for that substantive and comprehensive answer! I noted down some core points I would like to come back to in a few minutes. As you have indicated, Malawi is currently not a digitally very connected country. You have basic access and input [factors] such as access to hardware, access to electricity et cetera pp, agent liquidity and so on massively lacking behind, so a current deployment of the technology on the state-level does not make any sense. A pilot in a very controlled area might. I remember reading your blog posts today, that you made the argument that - I am rephrasing a bit but you, you more or less stated, if I understood not incorrectly, that based on, on the expectation of future Innovations around the blockchain sphere, for example, in the next years, some of the current complexities and issues might become irrelevant in the developing context in the next years. So, relating that to an obvious assumption of the project here, or why we are investigating that even in the context of Malawi, where it's currently, as you said, not really feasible to talk about some inclusive deployment, the assumption kind of is that, uhm, factors like connectivity, literacy, electricity and so on might, or will increase in the next year's and that like now, it's maybe already a good time to already investigate a potential deployment, given that these factors improve. Sorry for that long monologue. Do you have anything to add?

RZ:

Let me give a context for the comments. **Blockchain is still evolving.** I see this as a very, actually terrible technology. And I met people from South Africa, from other

countries, locals, saying "it is **expensive** to run and it is **complicated** to get people to help us developing". This was actually told by start-ups in a couple of countries in Africa. The guy told me: "it's expensive and I'm losing money. And when I try to hire somebody in Cape Town", this is Cape Town not Malawi, "I find no one, there is no one who know blockchain". So, it's **difficult to sustain the effort**. So, an example to tell you that blockchains are, as they are today, they're not very advanced. I'm sure **in five years, we're going to have a very different technology** running on the blockchain, which is gonna be **efficient, scalable** to use. So, that's what I meant with my comment. Remember the telephone? The telephone, when it first was invented, almost all of the people didn't want to speak to a machine, right? So, in the US actually they have, radio, you know, commercials, they are telling the people "please talk to the machine, talk to the phone." Because people were like, you know "I talk to people, I don't talk to a thing, you must be crazy", right? It's the same thing. Sort of similar, right? But, in the case of blockchains, the technology is still primitive, it's not - that's why "deployments". I mean, you must know about **the Illinois SSI experiment**, it didn't work! So, Illinois couple of years ago they launched "Oh, we're gonna use blockchain and SSI", you know, for birth certificates and whatever. **Two years later, they haven't done anything because they faced issues of scalability**. 10 million people. **How do you mine 10 million people in a blockchain?** In Bitcoin, you can probably do 3, 4 per second, which is really bad. And in Ethereum it's like 7, 8 per second. I have a blog on that, based on real data. So, the real world is, when you do a pilot, you have to say "Listen, we have something we do which is still evolving" Don't say it sucks, because they will kill you, but say this "It is evolving", and things like IOTA might be better than Ethereum. Cause if you say Ethereum, they will probably lynch you, cause they have like a religion-based approach on Ethereum. **In a few years, innovation will actually help address most of these issues, but not the issue for being a technological determinist**, right? You still need to be able to do things on the ground, people have their own needs. So, that's the importance. **The closer the technology, the ICT-use, the better for you to succeed** on the ground. I recall, when we started pushing email in the UNDP, in Malawi by the way. So, you know, the government ministers. "Do I need to type?", you know, type-writing used to be for secretaries, right? E-mail entails that I do my writing, right? I had to take a keyboard and become a typewriter. So, people said "I don't want to use that, why should I use that?". So, I heard this from ministers and many people in the government, saying "I don't want to, I don't

know how to type, my secretary types" Think! We approached it by forcing people to think "Oh no, now I have to type. I don't want to do my own typing." So, I had a boss in the UNDP who had all his emails printed, right, so he can read them. And he wrote his replies be hand and then the secretary typed on the email the replies. That's how it works. But that's not what somebody wants to promote. So again, technology historically has become easy to use and will be, you know, I think with AI, voice-driven things, is probably becoming more easy. So that's my comment. **Blockchain should be as easy** to use as Alexa. I don't like Alexa, but people love it. I don't know why, because it's a spy too, but anyway. That's what **people like**, you know, **simplicity**. They see, you know, I don't have time to discuss AI but I can say "Alexa, get me a Hamburger" and then, I'm happy. Anyway, blockchains and keep that in mind, Jan, they are still evolving, not ideal. I mean, compared to AI, blockchain are in the prehistorical stages. AI is so powerful when you see a guy working, it makes you wonder how we can have such a bad thing going on in blockchains. People don't tell you this but I'm working on both fields and I recognized the difference, how AI is mathematically, of course, I am also biased, but it's really, really powerful. You know, and it can be used by almost anyone; if you have access to some basic tools, whereas blockchains sort of are difficult to use and so limited. It makes you wonder, the correlation between financial gains and technology. Which on the internet never happened. In the Dot-com boom, this didn't exist, right? You only, they were hoping to have an IPO, and with the IPO to raise funds, now, if you have a Bitcoin, you become a millionaire! So, easy money, and I think those guys are doing a great job trying to tell all of us "oh, that is the future", because they created it. And my argument is, that in my paper like I said, **this sort of financial incentives, might actually go against innovation. Because of stars will not want people to innovate to change the rules of the game so we have a more equal financial inclusion**, or big bank. Bitcoin and blockchain, which I think is the future. **You have to de-link blockchains from cryptocurrencies. I think, that's the future.** I mean, any entity who is working on blockchain should know this. Why do I need to have a token, why do I need to have a cryptocurrency? And that's probably one of the answers. Of course, if you say this in public, you get lynched, because, anyway. So, for a developing country like Malawi, I think that's important. If you can have a ledger, which is sort of secure and transparent and offers services to people, where do I sign, right? That' the issue.

JM:

Alright, thank you so much for that answer again. So, I think that's a very straightforward question based on your previous columns. But, so, you are obviously strongly advocating for not focusing on any new fancy technology but sticking to what works best in a given context, or basically what works best to deliver assistance on an inclusive basis, right?

RZ:

Yeah. Let me give you an example of this. Back in 2012, we launched, in the UNDP, a network in Africa, specific for mobile applications. So, we did a workshop in Kenya, Malawi, Tunisia, Senegal, Rwanda, Ethiopia and so on and so forth. So, I was in a couple of workshops. So, it was nice. We had like 200 innovators. So, I asked them, you know, the innovators, "Are you guys, have you ever seen Ethiopia's National development plan? And they all said: "We have no idea, what he is talking about" So, I had a slide. So, I took the five or six areas of the plan and said, "This in the plan, so, how do you see you supporting this plan?" And they said "We cannot support it. We don't work on development, we work on technology". This is young people, right? So, they told me, one of the guys told me "Development is not a business. Development is just, you know, wasting money." Development is a 100-billion-dollar business, so it's probably more than you have seen in your life. So, they had this idea, so that development is sort of a waste of money. And the other things that they told me, when I asked them "So, what apps are you working on?" And they told me: We are working on taxi apps and you know, buying things" and I told them, "Ethiopia, you know that Ethiopia, your country, is 70% rural population, right, people don't live in cities, they live in the countryside. So which apps are you developing for those people?" None. None. This is local people, this is not some foreign consultant. I was shocked. And I think I convinced them, **that you need to be aware of this development things also the SDGs**. And that's why I think **this gap between development, technology exists, because people who do technology don't see development**. They are not even aware. They use to follow the Silicon Valley thing, right, you know, they want to be like Uber, they want to be like, you know Facebook, WhatsApp, so I guess they want to make the same amount of money which will never happen, by the way. So, that goes to back to your question. You need to, to create awareness. You can actually be living in one country like in the case of Ethiopia, or, you know, Rwanda, and not be

aware, that there are indeed some key priorities that need to be addressed. And I find that a pretty simple gap, a reason for this sort of "I have the solution for all of your problems, show me the money when it comes to ID" and that's what you have to reply to me. The policy of India is you know, Aadhaar. Ok, can blockchain do that? No! 1.3 billion people, no way! That would never work, right? So, we know the answer. You cannot use blockchain for India, cause it's 1.3 billion people and that would never work. Try to implement this on Ethereum, it's going to be a disaster. But if you say this, in the future, it might be the solution.

JM:

I mean, I mean, uhm relating for example to Bitcoin and Ethereum in relation to scalability, I mean, there are already some solutions which are a bit faster, right?

RZ:

Not as fast as the other ones. And I heard that **ID2020 has dropped the interest in Blockchains, because of the limitation of scalability.**

JM:

Interesting, I didn't know this.

RZ:

They actually have a, you know, call for proposals for anything for IDs, not only blockchains. Because, what is the blockchain solution, what is the solution including blockchain? There is a **paper by the UNF, also offering different solutions one being blockchain.** There are other solutions. So, you have to wonder, why it's only one being pushed, but anyways, that's a different thing. So, in the end, Jan, be realistic, I mean, there is nothing wrong with saying "Yes, this is limited, this is just a pilot so we can see if it works" So, I can give you examples of, in the US or places, it has not worked. In an average context. This is not, Illinois is not Malawi. And the issue in these places is mostly technological.

JM:

But mostly related to scalability if I understood you correctly, right?

RZ:

**Scalability, and easiness of use and, you know, wallets**, you have to have a wallet, I mean, with your private key and...

JM:

And if you lose it, oh my God. Yup, yup, yup.

RZ:

If you lose your private key, then you become no one.

JM:

Exactly, exactly. I mean that's currently one of the key concerns going on, especially if you look at, let's say Malawi, and already given that to you...

RZ:

I could see a black market for private keys.

JM:

Yeah.

RZ:

Imagine, I will give you my private key so you can do whatever you want.

JM:

Exactly, and then the question is, how do you kind of, uhm, save or, or like how do you implement a recovery of that private key and then, would you do biometric hashing and store that biometric data in some centralized database [510 is not doing that] and...

RZ:

Which is even worse.

JM:

Exactly. So, apart from that, we obviously face a lot of, uhm, current issues, implementation issues, which need to be solved in order to, to get to something, uh, like, to some solution which actually makes sense to, to be utilized. However, that's part of my research, investigating that system. or the potential use case of such a system, before it's completely developed. I would very much like to ask, given the assumption that we at some point would have, uhm, an identity system, which is

scalable, which is sustainable which is, also illiterate-friendly, human-centric designed and so on and we would hand this identity system to, for example, in Kenya, to the Red Cross, and ideally, what also Self-Sovereign Identity entails, is that individuals are ultimately in control of their own identities, can decide with whom to share data and so on, I mean, that's the shiny ideal, right, and the question I would be having, after your opinion, can we, for example in the circumstance of a humanitarian disaster, when this identity is handed and then the individual is dependent on receiving assistance with his identity, so sharing his or her unique identification details with some organization, can we talk about, actually can we talk about self-sovereignty, because in the end, I don't really have the free consent to share my data, if I have to choose between sharing my data or dying, uhm and relating to that, because I mean, even, if, if I have this kind of Self-Sovereign identity system put in place, in the end, for yielding, assumingly for yielding governmental regulating acceptance of such a system, I would still need had to have a third-party involved verifying my self-asserted needs on that system, so, in that context would it be fair to actually talk about a Self-Sovereign Identity in the end, or is that kind of going away from the truth? Sorry. That was a very long question.

RZ:

Is this like, cause you say that you already have the utopia, so, is utopia good? The question to me, for me is, what is the goal here? I mean, if you are happened to be in Malawi, we're looking at a poor person, **is your goal to get self-sovereign identity or is your goal to get a basic service?** Then I think, that's the issue. I don't give a hell, I mean, about SSI, if I need to get health. Please give me health, and then I will discuss having my own identity. Because today I have nothing. So, and I find this, if you want, I may go a bit beyond our discussion, this is between, **the fight between, within human rights, right, the economic and social rights vis-à-vis the political rights.** And you find this all the time. So, they are in conflict, right? So, we need to connect those two. There is not such a thing to guess you need human rights. These are political rights. You have two sets of rights. So, how do we balance these two? And now, there is, even the humanitarian experts, are wondering **how come human rights "won" in age of neoliberalism?** Ok, **we have an age of inequality, we consider human rights throughout the agenda.** How is that possible? And what is the connection? And the answer they gave, these guys, is **because they forgot about**

**the other side of rights, social rights**, which are basically, you know, rights to have education, all these things, working rights, obviously. So, that's another point of the issue you need to keep in mind, when you hear this. So, **SSI seems to be more adhere towards the political rights**. Because in the North, in the global North, this is the issue, right? You know, we have the NSA spying on us, and I agree, it's terrible, that should never happen. **But in the South, that's not even an issue because in the South, I'm not even connected**. I don't have anything. So, for me it's more important to get those public services. Have you ever been in a country, Jan, where you have to get a birth certificate? I have been, I've seen mother's trying to get a birth certificate, how difficult it is, nearly impossible. Would you want to have an SSI, or would you want to have a process where I can get my son registered in two seconds. No-brainer! I want to have my son registered in two seconds, first and foremost, not SSI. They are both relevant, but you need to balance this thing. So, how do we balance this? Of course, **when you talk about surveillance and things like that, you need powerful states**. Powerful in the sense of having the tools to spy on you. I mean, the NSA is a very powerful entity, with a budget of 20 billion dollars, which is more than the GDP of Malawi. Think about it. So, they spend on surveillance what Malawi spends on the whole country. Anyway. So, spying, thinking that Malawi is gonna spy on me, the government, how? They cannot spy on me. Anyway.

JM:

I mean, I could imagine some context, where you could, uhm, persecute some ethnic minority based on their last name or something, which also likely would have....

RZ:

I agree. I'm not saying; I'm saying with technology, it's difficult to spy on people. Alright? It's easy for me to do it, if I look at your name. "So, you're from the North? I don't like you". But imagine a state in Malawi that is like the NSA. They know about encryption, they now about eavesdropping. I don't see that happening in 25 years, no. That's why they use force, cause they cannot spy on me. So, they need to use force instead of, you know, possible revolution, or whatever you wanna call it. So, what I'm saying, is that going back to Malawi, when you're advocating for human rights in that sense, how do we, and I think people should decide, not me. So, you go and ask them "What do you want, what do you need?" I should not have this prejudice saying "You

must implement the development agenda based on Article 19". I think that is a great principle, but when it comes to poor countries, we should tell people, or ask them, we have different options, we can do this, we can do that, there are many things you can do with the community and every option is wonderful and what shall we do? So, it's basically, a community would tell us. "In our community, our main challenge is to register our kids into school, how can you help me?" And that becomes a platform for other services. And I will give you a real example about what we did in India, with the UNDP. So, birth certificates. So, we needed to study in a northern part of India, small island, very poor, so, the island has, you have to take a ferry to go to the mainland and then go to the capital city of the state to register your kid. So, if you're a mother, living in that island, or a parent, you will have to travel from the community, go to the ferry and take a bus to go to the capital city and then apply for the birth certificate. So, we did a follow-up on a few families and we found that it took them about six days to apply, just to apply for a birth certificate. And usually, when they went to the office of administration, there were these people called "black coats" which is a real name, which are facilitators. So, if you pay them some money, they would expedite the service. So, more people actually used those black coats to expedite the service. And those guys, I guess they have somebody inside the office who was corrupted and they would expedite. So, you will get it, instead of one year, you will get it in six months. Six months. So, anyways, it will take you quite a bit of money, because you have quite a bit expenses, cause you have to pay the black coat to get your certificate, which can take a year, to come back to you. So, what did we do. We set up a couple centres in the island, dial phones at that point, and we have one private and one public, so one run by an entrepreneur, one run by the government. So, now people can go to a centre and they actually gave the details to the operator of the centre, who then was studying the computer and then he send this request by email to the, to the office in capital city, and then they got back, it took only a few hours, saying "It's being processed, we're getting a copy in 48 hours." Ok? So, look at the example. We never said "You need to be connected to the internet." We never said "You need to use a computer to get the certificate". You don't need to know English to apply for this. You don't need to learn Windows, right, or use a mouse. It improved to 48 hours. So, this became a model for doing many other services. Licenses for marriage, land titles. The same mechanism became the entry point to create many services. From that pilot this became the state as a model to replicate in every single town of this state, in Andhra

Pradesh. So, when you go to, I went a couple of years later, actually privately, to another place, poor place. We went to the centre and it has 5 C's computers from the operators and people from the South come to the centre and they, again, the model is not that they use computers, they actually said "I want to pay my bill. I want to get my bank-payroll." The same model was working throughout. So, again. We never emphasised the divide. That's not my job. My job is to get people, through technology, services. And that was working. And now, they use iPhones today, of course. Since it's evolving with technology, but the principle was **"We focus on the need, find the technology that can help me make this happen."** So, I didn't need to use the latest, if I can I will, but I keep in my target the core goal, right? Which is not blockchain, or internet, or, you know, Facebook, but how can I get to the best service so they can get the document they need in a short period of time. And that should be your solution. So, you have to answer that question "Is blockchain the answer?" No. It could be, but many others could also be, including some old technology. But this is not common, right? If you use something which is old, you don't get this, sort of, socially exposure. But who cares? But people care today about reputation. And also they want to have media followers and 20.000 likes, so I find that funny. But anyways. So, my example is to illustrate, that when you do the pilot in Malawi also **try to explore that question on the ground. Is this the best way to do this?** Are there any other ways that we could actually deliver this service to people? I think the potential of this is, there are actually so many great options that you can actually deploy, but in the end, you have to keep in mind that, **is this gonna be left behind and we need to think that way when we exit this pilot, what's going to happen.** An ideal would be, as you said, in the beginning, **ideally, people, local people should be able to take over. That should drive me design from day number one.** So, **if you make it too complex, you make it difficult** for them **to embrace** this. So, when you design the initiative, have this target on your mind. Then, that's gonna drive to a point where you have to decide "I want this to become a stable, something which is going to stay there for the next ten years." Don't go in and go out. And that should drive the way you design the initiative. Because many "development", humanitarian agencies don't think like this. So, help people and go out! I give the example of building houses. So, I know how to build a house, and I go to Malawi to build a house. But Malawians know how to build a house. Why should they not build it? But I feel great because I built a house in Malawi, right?

JM:

And maybe, people need sanitation and already have houses put in place. Thank you so much again for that, uhm, comprehensive reply. So, uhm, relating to some comments you made, so, I mean, the underlying principles, or the underlying concept of a Self-Sovereign identity is quite an anarchistic, if that's fair to say, so, uh, decreasing the dependence on intermediaries, decreasing the, the, the dependence on the sovereign, maybe more centralized state, uhm, if I understood you correctly, you argued that, persecution, data protection issues, would apply to a more "developed" context and that these are relating to the use of technology, not really emergent, or not really immediate problems in the context of Malawi for example, uhm, and the question I would you have to you, and I think you already answered it implicitly, is about the normative desirability of deploying such a system anyways. Both Malawi and Kenya for example, have had a massive roll-out of their national identification system in recent years, so, uhm, Malawi claims universal ID coverage, Kenya still has some, some spots, uhm some communities, where you can maybe have a coverage of 20% not more, but they also, after my understanding are increasing their efforts, so the only argument for, for me would be deploying a Self-Sovereign identity based on the data protection, it could potentially provide, in Kenya might see some persecuted individuals who don't like so much to be included in the centralized governmental database, but beyond that, I'm happy for your opinion on that, I don't really see a desirability of setting up a parallel systems, besides the governmental one if we don't have the, like the urgency to protect people from, from prosecution and violence based on their identity, or based on the belonging to a certain group.

RZ:

Think about the Rwanda genocide. Was that, because people had identities? No. That's actually an interesting case, because people knew who was who and who was not. It's binary. You are, you are not. So, if you were my neighbour, I know you are a Houthi, so I'm going to kill you. I don't need your ID. Cause at the local level, in that case, I know, who is next to me. I don't care, if you have an ID or not. And that's an interesting country, country example of a government using ID for oppression, because in this case, like many other civil wars, people have any IDs, but are not the enemy, cause you're different, you look different from me, or you are; religion, but in the case of conflict, **even SSI won't help me, because I know, who you are.** So

that's sort of an interesting discussion on the relevance of IDs in conflict. So, even if I have an ID card, you actually know who I am. And if you know how I am, you will probably kill me. Anyways, that's just a side-example.

[Subsequently, RZ and JM engaged in an informal exchange of opinions about the WFP's Building Blocks project, the statements are not displayed here. Basically, the Building Blocks project claims to utilize blockchain for its eye-scanner verification system for some camp-based closed-loop food voucher transfers and according to RZ, part of that implementation included cutting local intermediaries out of the assistance delivery chain.]

JM:

I think the refugees you were mentioning, or the camp context, is actually quite interesting, also relating to my research. So, coming back to the example of Kenya where we have, also in Malawi, we have some refugee camps, Dzaleka camp for example, but especially in Kenya, you have a lot of, uhm, displaced populations from around the neighbouring countries in some camps and now we, we have these Refugee populations, which do not possess legal identity documents, the Kenyan authorities recently, in the recent years restricted the foundational purpose of the UNHCR-mandated ID in these contexts, some years ago, I could kind of, seemingly according to the literature at least, access wider public services with this UNHCR-mandated card, this got now, this influence got now reduced, the state increasingly asserts sovereignty in issuing, also to refugees, identity documents, uhm, kind of, uhm halted issuing, I forgot the exact the exact name of the identity card, but basically halted issuing an identity card for refugees, which would support accessing these services, these wider public services, and also saying "Hey, I am a refugee and I'm eligible to stay in this camp." So, uhm, the basic argument for and I don't necessarily agree with that, I agree with a lot of points you said regardless of my questions, uhm, so one argument you would find in the sphere of providing a Self-Sovereign identity or maybe even another identity from a non-governmental institution, is "Hey, we have this global ID challenge. we have people being undocumented, under-documented, therefore not financially included, let's, because the state for whichever reason excludes them from their public or governmental ID scheme, let's provide a Self-Sovereign Identity, whatever, for, for these people so they can build up their own identity and be included. So, let's kind of circumvent [connection interrupted], because

the state arguably does not include everyone into its scheme." So, would you, would you agree with, with, this viewpoint of providing a Self-Sovereign Identity as an alternative to a national governmental one, or would you rather say "Hey, okay, setting up parallel structures, working out of the [scope of the] sovereignty of each state kind of undermines what humanitarian actors should do."?

RZ:

I think, I still; that's probably not the right question. What you need to think is, again in a development and humanitarian context: "What are the priorities?" And then, the other question is "Who decides?" Normally governments. **Look at the development plans developed by the governments.** I think those two questions, one is "**What are the pressing needs?**" and then, "**Who is making the decisions on my behalf?**" That's very important. And, of course, **people should be informed.** Cause **you cannot have these discussions in a back-yard.** So, you should, also need to **share information with people who might make the decisions.** But in most developing countries what you see is that governments speak for all of us, right? Especially in developing countries. You have no way of asking average citizens to influence such decisions. So, that opens the door for, for you as a humanitarian practitioner of asking "So, what if we ask the community we actually engage in about such needs, such priorities?" And that should be informing on how to proceed. And I think that is very important because if you do it the opposite way. What if somebody comes to you and says "Jan, you know, I think you need SSI!" So, you say "Wait, wait, a second!" You're educated, you know what you want, you will say "Wait, wait. Please, **before you tell me what I need, you need to ask me what I do need!**" So, it's the same. So, we are now going to the Southern World saying "You guys need this! Cause I think it's great." Well, yeah, it might be great. **But, why don't you ask the local people "What do you really need"?** You know, **without being biased, and we don't do that very much.** Especially, **the "techies",** since they **believe they have the answer, but they don't have the questions, right?** So again, it's not that either or. So, that's one answer. The other answer is, let's think about what is the purpose of development? As such. So, if you look at the history of Western Europe and partly the US, these guys took 150 years to develop what we have today. They built states, institutions, which are the places I can go to, to either get information, services or complaints. And those places have rules of the game, by a code of law. So, if I don't play by those rules, they

come after me. That took a while to develop. So, it didn't happen, you know, look at Swiss, Swiss is supposed to be the maker of democracy, but these guys were in civil war for 50 years. From 1798 to 1848. I think they got the agreement they have today. You know, the canton, the cantons. So, they have war. So, are we calling them savages? No! So, it takes time, it takes conflict to, to address this. So, you go to a developing country, and you tell them "You need to be developed." So, in theory, I mean, you should be sort of, like we are in the North and these institutions which have clear rules of the game, rule of law... it took us a long time to develop this and we ask them doing this in 5 years. So, would that be realistic? No, probably not. So, how do we advance? So, I think that's the question. So, how do we compliment to this long-term process? They might, they might take 75 years, or maybe 50. But, it will take a long time. It's not my, my contribution to the process is going to be a grain of salt into this, you know, heap of salt, right? And you should be aware of this. So, how can we help? **We are not in a position to decide for them, what works best. But so, in an ideal world, I'm all behind having my ID in my own hands.** Nobody, no one will say no, of course. Why should I, why should Facebook have all my information? Why should these guys sell all my information? It doesn't make any sense.

JM:

Uhm, relating to these comments, may infer from that, that you are implying that humanitarian agencies should rather focus on their core mandate - providing immediate disaster relief, for example, rather than focusing on for example providing a Self-Sovereign Identity or even, on a more broad level, a legal identity for a certain state because that would kind of deter from...

RZ:

No, no. What I'm saying is, whatever you do, make sure you know, there **are three principles for development**. One is, it has to be **demand-driven**. That's the first thing. People want it. Somebody has asked me from Malawi. Second, it has to be **owned by the community**. So, they have to own this, because if I want to leave this behind, it's actually their initiative, it's not mine. I'm just facilitating. And the third it has to be **participatory**. That means they have to be engaged in processes from day one in the end. So, these three principles apply to everything within developing countries, humanitarian or not, in the return. Now, of course, in the case of a war, it is much more

complicated. In the case of, say, humanitarian natural disasters or, you know, extreme poverty, hunger, this is not the issue. So, **excluding war** and civil wars and stuff like that, you can actually do this, **you can follow those principles**. Because **then you link to development**. Demand-driven, owned, participatory, you can hand over this to the development agencies, because they follow the same principles. So, that's the connection. So, I'm not saying, you guys aren't supposed to do this. I'm saying you can do whatever you want, as long as you follow these ideas. Of course, it doesn't work in all the cases, but in most cases, it can work, it should work.

JM:

Ok, then relating to that, thank you for the answer, I completely agree, relating that to; imagine the Red Cross would go to some community in Kenya where there's an apparent need for identification, or a lack of formal identification. And the people there are saying, or most of their community is saying "Hey, we lack the formal identification, we cannot enrol our children in school, we cannot vote, we cannot access health services etc." we have a need for identification." [example made up]. Would then the approach be rather lobbying, or the humanitarian agency, lobbying or advocating the identification, or the inclusion of these people into the national identification system, or trying to provide a humanitarian ID, to kind of circumvent that problem...

RZ:

I guess, the answer depends on "ID for what?" I mean, I don't know about the Red Cross, but in the case of WFP for example, ID was for giving cash to people, right, so it's very limited, which is not done by the government, so you don't cope with the governments. It's clearly, governments don't want to enter the business of; cause the cash is coming from the UN, so they are not in the picture. So, the answer would be "ID for what?" ID for getting health services, or ID for Red Cross help? So, that's a very different thing. So, the **ID, probably by the Red Cross, will not give me access to governmental services. Unless you make a connection. But does the ID provided by the government give me access to Red Cross services? Maybe.** If I can check your ID, right? So, think about those factors. **You might have a case, where Red Cross ID might coincide with public services, but then, you need to connect. Cause government will not offer a service based on a private ID.** How do I know, you know, **even if it's blockchain-based, I don't know who you are. You**

**never registered in my database, you don't exist.** So, we need to make that connection. So yeah, ID for what? Because the WFP you see it's clearly ID, iris scan IDs basically for their own recipients, but government has nothing to do with this, cause they would not want to use that for banking. Because of the Red Cross, I don't know, if people give them access to medicines, or help or, but that will not give me access to getting a birth certificate. Cause RC doesn't exist legally. And this is a famous discussion between private IDs and sovereign IDs. But **there might be a case, where you can work out with local governments. There are situations, where IDs are common to both, so any ID issued by the Red Cross with our, sort of, oversight, might work for both Red Cross giving private medicines and doctors provided by the government. That should be ideal.** But again, because it goes back to "IDs for what?" so, ID for my own purposes then yeah, you can whatever, but **don't expect them to be adopted at the national level because it's not a national ID. But if you make the connection with the national ID authorities, then you might have a case where you can actually provide some changes in the national ID systems and then use your pilot to entice such change.**

JM:

I agree with that. So, but that sounded a bit like you would have the opinion, that whenever you would provide an ID system as a humanitarian organization, which is not solely meant for accessing humanitarian assistance, but guaranteeing whatever it is, by the way, whether its mobile money or whether its health, or whatever, but guaranteeing more, wider foundational purposes with that ID, that the ID-characteristics of a given to individual would not only needed to be verified by the humanitarian institution itself, but also by the government in order to, to achieve that credibility, of that ID being accepted, is that fair to say?

RZ:

No, no, no. Okay. Think of the issue of legal ID. So, of course, if you go to Facebook, you have an ID. That's a private ID. But I cannot accept your ID in Facebook to give you wider benefits, it doesn't make any sense. I don't know who you are, I don't know, Facebook is a different animal, different rules, so that's the issue. It's the issue between legal IDs in the country with any other kind of IDs. So, there many different types of IDs, there's Microsoft IDs, single IDs, all those things. So that's my question:

"When does it become legal to a public level? **Should a private organization give public IDs?**" **I don't think so. It should be a public organization, right?** Hopefully, a public, democratic, open, transparent organization. But not a private organization. So, Facebook cannot be a national ID provider. I'm sorry. Facebook is a US-based company residing in California. It doesn't make any sense. Legally, I cannot even sue them as a citizen from Malawi. Okay, so that's the issue. So, I'm not saying that, I'm saying it's a difference between public IDs, legal IDs and any other ID which companies love to do now, because they make money from my IDs. So, what I'm saying is, how do we, how do we make, the question is how do we make these public IDs, legal IDs more, of course there are different dimensions, access is an issue, people do not have access to IDs and then, the quality issue. How do I protect my ID? So that's the question. Whether it should be done by a public entity or a private entity, or the UN system. It should be done by a public, a national institution, which is so hopefully independent, transparent and democratic. Which is a lot to say, but, that's the answer.

JM:

Maybe I expressed myself a bit confusingly then. Because I think that's, what I asked. Whether any ID in the context could become legal without the public entity backing it, or verifying personal identifiable information et cetera pp on that system. And I think, you answered that with "no", if I understood you correctly. Just to make sure that we didn't even talk about the different.

RZ:

Yeah.

JM:

I think that we are on the same page there right?

RZ:

Yes.

JM:

Thank you by the way so much for sacrificing so much time for me. I really enjoyed the conversation so far. It was very enlightening. So, I think, uhm, I'm mostly done

most of the questions I had. Is there anything else from your side as a comment or question, you wanna follow up with?

RZ:

I have a lot of interest on the pilot. If you could keep me abreast...I work on both Kenya and Malawi. Actually, Malawi, I was in 1995. And we set up on of the first e-mail nodes of the country.

JM:

Cool!

RZ:

And I know, how; internet actually is still a bit lagging and it's really, really a poor country which has not developed in, actually, the last 25 years. So, I know a lot of people in Malawi and; Kenya, I also have some friends in the government. So, I'd like to follow-up on your pilots, because I'm following blockchain. So, and my theory is that blockchain is still not delivering what is possible at this point. I wrote another paper for a journal on this, on blockchains and I made the same point. It is not, I mean compared to other technologies like machine learning or...compare if you read the books of the press on AI and impact on people, it's happening now, that people are being affected by, you know, this stuff. Blockchain is at nothing. You're going to invest money. Billionaires! They are more talking about the Bitcoin price than anything else. So, that's, so, think about it, it's so soon, it's so funny. Hopefully, it's gonna change.

JM:

I hope so as well and if not as you said in one of your blog-posts. I mean, eventually, it's not about solutions looking for problems, but it's about trying to find the right solutions for the problems which are there and if it does not provide a solution for the problems we face...

RZ:

Look, if it doesn't work, you should conclude that. There are so many limitations. People need to hear this.

[JM and RZ engaged in a more informal exchange subsequently, which is not displayed here. During that exchange, did RZ suggest checking Fordham University's Humanitarain Blockchain Summit.]

**End of Interview**

## Full Interview – Kokoévi Sossouvi (KS)

### Discloser

At the beginning of the interview, the regarded digital ID-system of 510/NLRC and the research were briefly introduced. According part of the interview, based on a confidentiality agreement, is not displayed here. Consent for recording the interview was given after 20 minutes during the interview, as KS expressed some initial concerns relating to deploying the system unconsciously. The non-recorded part of the interview was not included in both summary and full version of the transcribed interview.

JM:

Are you a supporter of this general idea of the „humanitarian development nexus“, meaning are you a supporter of this idea of linking long-term sustainable development, uhm, efforts to humanitarian assistance?

KS:

What I, my point is that, governments are the ones legally responsible for the well-being of the population and the **role of a humanitarian community is to support them fulfilling that mission, but not to take over from the government.** A lot of times, I find that the **humanitarian community is working outside of the government structures.** For example, and maybe that will speak with to you on the social protection side, there is definitely a lot that can be done using the existing social protection structures. And a lot of times, **humanitarian assistance works in parallel.** These days, we're talking about the so-called "shock-responsive social protection" that is looking at how we can scale-up vertically or horizontally in all sorts of forms in Social Protection, so that it can meet humanitarian assistance needs. And then, that's an example that shows that we, we are sort of inventing this terminology because of the humanitarian sector is not really linking properly within, with the existing structures. So, I mean, that is already, sort of, for me, the **main issue is the lack of the synergy**

**sometimes between the humanitarian action and the action that is more rooted in the long-term development goals.** And so, you know, on the ID-side, if we were to sort of develop, **foundational IDs**, maybe **generated by the humanitarian community**, that's again **another example of something that will be taken away from the governments and not building the capacity.** So said like this, it [deploying an SSI serving a more foundational purpose] doesn't sound like a, like a strong proposition and it doesn't yield the capacity of the government and that's **the main issue we have, when trying to intervene in crises situations, that the capacity of a government is, is not strong enough for us to be as efficient as we can** and as fast as we can.

JM:

So, would you see an acceptable pathway for deploying such a system, would be solely for supporting the humanitarian agency in its, uhm, its own assistance delivery?

KS:

At the moment, cash is, cash is king. We're using a lot more financial assistance in crisis situations. And so far, in my experience, **we've been able to deliver cash to the most vulnerable people because we have found ways to work within the existing regulations in terms of KYC.** A lot of countries, especially when it comes to mobile money, have the so-called "tiered KYC", it's a risk-based approach, and because the amounts that we provide to the humanitarian community are small enough that we can still work in the legal systems, you know, legally accepted transaction limits, amounts, those kind of things, we have been able to deliver the money, even though not everybody has sufficient, you know, sufficient ID levels. **So, you know, it didn't seem to me, that a lack of ID was preventing assistance to the poorest.** Now, you know, like what I'm saying, progress is a great thing and if we can do things better then, by all means, let's look at it. But, I would say, that the **client for this technology should be the government and not the humanitarian community.**

JM:

And, uhm, linking that approach of a tiered KYC back to this, uhm, humanitarian development nexus, in this case, financial inclusion, so one of the more explicit aims of, of, uhm, this nexus is to link humanitarian assistance to wider financial inclusion

efforts and there my question would be, does this tired KYC approach, which is applicable to some recipients of humanitarian assistance also apply beyond a humanitarian, uhm, uhm, crisis, thus yielding this kind of financial inclusion?

KS:

Yes. I mean, these are sort of guidelines or regulations that are applicable to the entire country. So, you know, we just plug-in to this existing mechanism. So, an old grandmother in the top of a hill somewhere in a village is our target, you know, recipient, because we, we anticipate her to be vulnerable to, you know. But this person irrespective of the fact that she would be receiving financial assistance with a scanner, can access the financial services based on the regulation, what we find is that once we, you know, if she becomes a recipient because she's been affected by crisis she will be using the financial tool that will be made available to her, **but once the payment stops, she's unlikely to continue using it, because at this point of time she's got no more income.**

JM:

Yeah, so, I mean, I completely agree with that. I've read various studies which were already, uhm, kind of showcasing that there's not really a substantial financial inclusion impact of, of, uhm, deploying a kind of e-transfer system, because people, as you said, people simply don't have the financial means to, to save or, or, or transfer money beyond the, uh, beyond receiving humanitarian assistance. Uhm, but would it be for, when we're talking about this old, uhm granny, uhm, somewhere, uhm, sorry, that grandmother, living in this rural area - now she has been included onto, without any identification card, onto the M-Pesa system, to receive humanitarian assistance - now or the intervention stops, uhm, and given that she would have, uhm, some, some Shilling to, to, which she now wants to store or send, with this, this e-transfer mechanism, without the ID, that would not be possible, right?

KS:

Yes, so, I mean, what happens is that, we normally, you know, like, best practice, there is always some exceptions, but **best practice** is that we will facilitate the humanitarian agency that is providing assistance to her, we **facilitate her obtaining an ID**. So, for example, you know, what you need to register for a SIM card, is different from what you need to open a bank account, right? Depending on the amount of

money that you want to transact, the things that exist is what we've been calling a mini wallet, a mini wallet being, you know, a mobile wallet that has a reduced KYC. So, you will be able to transact just based on the ID she gave when she, when she opened the bank account. So, sometimes you can open your bank account with just a birth certificate. Your picture is not on it. What the humanitarian community has been able to do, is to, you know like, provide proxies for identification. So, we know that is grandma, she's been living in that village for almost forever, or at least for a very long time. The neighbours know her, they know her under a certain name, they know her, and they can maybe identify some of her children, some other relatives, so the chief of the village is always the go-to person, so at some point, somebody's about to verify that indeed the information she provided is true. And so, if she is a refugee, it will be a different situation. She has no community, right? Here, we are able to, by means of using proxies, confirm her identification and get her a SIM card with the humanitarian agency acting as the, kind of, vetting her, so you know, so under the, I wanna say under the **tutorage**, but that's not the right word, of a **humanitarian agency, she's able to have a wallet opened for her. And that normally is permanent. It is permanent to the extend she maintains, she maintains the phone line active.** The problem being, you know, these guys, so the mobile operators would keep your line open if you use it, if you make phone calls if you - and the issue is, is that this person may not be making phone calls. She's probably isolated now. The people she knows are living around her. They live around her, so she doesn't have anybody to phone. **At some point, a phone line will be disconnected and when she doesn't have ID, she can't open it again. So, this is, this is where financial inclusion ends.** First of all, she may not transact and then, so there will be no financial activity although she is included. Or, if she loses access to financial instruments, it is difficult for them to gain it again when they don't have official ID. So that's where you, where we, where there is a breakage in the financial inclusion kind of loop or chain reporting or whatever it's called.

JM:

However, you said something very interesting, I haven't heard so far yet. Uhm, that's a humanitarian organisation in a certain case at least, could serve as collector and validator, or vetter, of certain, uhm, information required for KYC-purposes without having a government official directly on the ground, on the site, including that person

at least for a temporary time, into a, for example, mobile money system [is possible] if I understand you correctly there?

KS:

Yes. Basically, what happens a lot of time, is when we, when, let's say NGO A, so, when NGO A goes in, what they would do is that; and they decide to use mobile money; they will acquire a number of SIM cards and as if, and that would work as a, as a float. So basically, it's like they're collecting all the SIM cards and then they choose who to distribute the SIM cards to. So, in the system, the SIM-cards are, you know, recipient A under the patronage of NGO A. That's how the person is recorded. **So, they got their name, but they are also associated with a given programme of the NGO. So that creates the sort of, you know, a risk-based KYC for the mobile network operator.** So, you have a lot of people who get a new SIM card for being part of a programme. We don't always use the existing ones, because, say for example NGO A is working with MNO A, and this person has a SIM card with MNO B. And it's just easier for the NGO to manage one relationship with one MNO as opposed of having to deal with others, **so we kind of always tend to start from scratch and issue new SIM cards with a process of being a guarantor or whatever, vetter, for for the recipients we distribute the cards to.**

JM:

But, uhm, you're more or less automatically obliged, when we're talking about minimum KYC in this case, uhm to use, to use a closed-loop payment system. So that the transaction amount will be limited, the amount which can be - or maybe the storing value on the device et cetera pp, these kind of things will always be restricted, right?

KS:

Well, so at this stage, because it's a, it's sort of a proxy-KYC system or whatever, it's, well, like I said, it's kind of a mini-wallet, so the amount that you can transact is likely to be limited. It's not always the case, it depends on the agreement you have with the MNO. So, I'm not speaking universally here, but the **limits are there most likely. But the limits also align with the transactional capacities of the population.** I mean, you know, if you are poor and don't have lot of money to move around, you know, to spend to, to transfer to purchase with, so these are very small amounts. What we also see in terms of financial behaviour is the "**cash-in cash-out**". So, we give you money

and you finish everything. **Because also the areas where we work are not themselves digitally connected** the way in the most kind of, in the way **that sort of meets the potential of an ecosystem**. So, for example, **there are no merchants from which you can purchase, you know, digitally anyways. So, your only option is to withdraw.**

JM:

Coming back to one interesting thing you indicated, which I highly appreciate by the way, is that humanitarian actors should be very aware of not taking over, uhm tasks from the government, in this case, providing a more foundational ID-system. Now, the question relating to that, if we're looking into a context where there might be discrimination, persecution, violence against a certain minority for example, or a certain religion, whatever, and the government would only issue foundational ID credentials, which kind of indicate if you are belonging to a certain minority which might be persecuted. Would you then have, after your opinion, would you then see a normative argument in providing a foundational ID system from sides of the humanitarian sphere, which kind of protects, by its characteristics, disclosure of sensitive information, which my yield to persecution?

KS:

I'm not sure I fully understand what you meant, are you saying that in some cases, the government does not want to issue IDs to some population, or they issue ID but distinguish them as belonging to certain populations?

JM:

The latter. I mean, the other thing could also be, could also create kind of the basis for a more compelling argument for a humanitarian agency providing foundational IDs, but for now, the case of persecution would be quite interesting to me.

KS:

Well, I can give you the example of the Refugee ID that UNHCR produces and that definitely, you know, spells out to everyone that this person holding the ID is a refugee. To the extend that it can be stigmatising to the refugee and you already have a situation. You know, if a government is already kind of, you know, wanting to stigmatize its population you know, members of its population, I don't think that, I mean, there is

nothing we can do, like, I mean as humanitarian actors, I mean, you know. There are things that can be done internationally, you know, within the UN Security Council. But, if a **government is already deciding that it wants to, you know, apply different rules to various communities, then we're dealing with a problem that is way bigger than what, you know, humanitarian actors can handle.** So, so that's an issue. I mean, we, we have situations where, you know, some nationalities are financially included, because the government wants them to do so. So, for example, I give you a very concret example, if you're Sudanese in Egypt you can not open a bank account. Like, it's impossible for you. If the government doesn't want Sudanese people to have bank accounts, if you, you know, Sudanese is an example, but there' a number of countries where you cannot have a bank account, even in Egypt. So, the decision already has been made. And then, as humanitarian actors, there's nothing we can do. When we provide the Sudanese with a, with the UNHCR Refugee ID that we have been lobbying, so that the government accepts this, as a regulator, accepts this for KYC-purposes, that still, doesn't, you know, because Sudanese are not eligible for financial access of that magnitude. So, there's nothing we can do, when the government doesn't want to. This is why collaboration with the government is super important. Egypt is an interesting example, because I don't even think they signed, the Refugee convention of 1952, so, they are not held accountable, on that level. So, you know, some countries have, yeah, specific circumstances, that just undermine any effort that we want to make. This is why I mean working with the government is essential, I mean, it's their country, they can do whatever they want. So, **collaboration is always stronger than coercion.**

JM:

I see, I see. Thank you so much for the example. That was very enlightening and also the answer to my question. So, I'm just, because, uhm, that kind of deviates from my research, but out of interest, uhm, the discrimination in Egypt took place because for subscribing to some financial services, you would need to disclose an ID which always, kind of, provides information on your, your nationality. So, that's why is the Sudanese were automatically excluded.

KS:

Yes.

JM:

Ok. So, in the second case, or the first example you mentioned, when we're not talking about discrimination based on nationality, or not accepting certain nationalities, but rather the government excluding some, some minorities in the country from their ID-system. Would you say, the same issue applies, that humanitarian actors anyways can not kind of, circumvent or, or, uhm, fight this obstacle when the government already decided to to exclude these minorities?

KS:

You lost me a bit, but...

JM:

Sorry, I talked too long.

KS:

I mean, if I don't want some people, let's just say, for example, even gay people you know, some countries can come up with nonsense like that, where gay people don't have the same right, you know where it's considered a crime in many countries, then it's very difficult for us to intervene. You know, in some of the countries where we were, we had to, I would say, you know, we had to expatriate some of the refugees because of their sexual orientation. Cause we knew they couldn't stay in the camp and they couldn't stay in the country. We had to, they had to be prioritised, you know, for being transferred to another country. **Especially if they are known in the community as activists, wherever, in that case, it is nothing you can do. You know, humanitarian actors work within the national legislation, they don't supersede the national laws**, so, yeah, especially in terms of ID, which I think is a very sensitive issue, it's very difficult to negotiate.

JM:

Thank you so much for the input, that was very enriching! So far, is there anything from your side you want to mention or clarify?

KS:

Well I think, there is a lot of initiatives that look at the, at these ID situations, I mentioned before the **ID4D** with the World Bank and if you could speak with someone

in that team and see, you know, and kind of, just understand their process. What is it that they do and what hurdles do they come across, when trying to do the things? I mean, understanding why a lot of people don't have ID, you know, but that, I think that would be useful for you and we need for - look, I'm just saying, in my experience, we have had the need to, you know, to create a new ID. But even, though, like, in a way, we, we, the UNHCR ID provides a **DID to the, to the refugees in many many many countries and a lot of times, we've been lobbying with the Central Bank, so that the refugee ID is considered for complying with KYC-purposes and sometimes, it has worked, sometimes it hasn't worked. But that's, you know, so that's been good enough for us.** We haven't, you know, needed something else. In terms of the national population when it's in the interests of a government that everybody is identified, you know, I mean, the biggest thing with ID, further down the road in a, in a number of years is, it's always been to **tax collection, so it's in the interest of a government that they know who their population is**, because it'll be easier for them to have a government to enroll these people into into the tax-system later on. So, it's never something that the government says "I don't want to have an ID" and when they do, yeah, that's very suspicious and then and then it's, it reflects a bigger problem than the ID-situation itself. It's related to discrimination of certain groups, because of religion, ethnicity or whatever, and that becomes another conversation all together, it's not an ID-conversation. So, in my experience, I have seen the government keen to which gaps in terms of ID. A lot of people have voter's cards, they don't have ID cards, just, you know, on the election side, I mean, if there is no argument why the government wouldn't want to be able to provide identification to the entire population, so **if you come with a solution, that helps do that faster, kind of more cost-efficient way, they are keen and on the contrary, when they, when they see this, you know, responsibility taken away from them, I don't know that it's pleasing, because how do they get this population back. You know, you can't give thousands of IDs to the same people. You know, if somebody says "Ok, now I have a foundational ID from these humanitarian organisations, well I don't want to get the national ID no more", what do we do then?**

JM:

Good point, yeah.

KS:

So, it's kind of a; and then at some point, you just have to, the government has **to say: "This kind of thing that we said was ok, is no longer ok". You know, this humanitarian foundational ID is no longer** - so, I mean, it's just like, like I said, I keep repeating myself on this, if a client of this solution is the government, **I think it's great, because governments have issues, you know, in providing IDs to the entire population and that's a problem they don't want to have.** Humanitarian actors, **we just have to be better at working with the existing structures and providing solutions to the government** as opposed to only saying "Ok, the government can't do this and so we do it for them." So that's a challenge, that the project, you know, sends to the community, instead of saying "We're gonna come up with something else", "How can we work better with the government? How can we work faster under the circumstances, when we have emergency response and people cannot be financially included because they lack foundational ID, they don't have the ID for the KYC-purposes?" So that's a challenge, **and in terms of us wanting to provide assistance more in financial terms** that's the question that we need to be asking, but within the, **within** the, you know, **national legislation, not outside.** I think, there is just too much happening outside of the government structures and we need more alignment, need way more alignment and we need more capacity building. But the issue we always mention, is the urgency. You know, it's an emergency response, we don't have time. Maybe, **humanitarian agencies need to find ways** to fund more, kind of **preparedness working with the governments before.** I mean, you know, some countries are more prone to disasters than others, so we need to be working way ahead of the emergencies, so that the emergency response is softer. And **it could be on the ID-issue perhaps.**

JM:

So, I think that's also a point, or an issue you raised, when, in your guidelines, that disaster preparedness should be, uhm, quite emphasized when setting up any kind of e-transfer, just to make sure that assistance can be timely delivered when an ongoing, or repeating disaster occurs. So, uhm, lobbying for that, that disaster preparedness in relation to the ID-challenge would, wrapping everything up, not mean that, humanitarian actors set up parallel systems, but it would mean support and an increased support of governments in setting up universal identification systems.

KS:

Yeah, absolutely, that's a good summary. There was also, at some point, I think it was Action International that was working on a mission, an initiative called FAB, it's called "Financial Access at Birth" and I can't remember when, it was some years ago, when I was talking to a really nice lady about this, and I think, what they were trying to do, was to make sure that, you know, people begin their financial life on day one and so this financial access is not something that comes up years later when, you know, when your crisis affects you or whatever, but like, you know, from birth and also, I think it's linked to something that's quite dear to me, when you begin your financial life with savings as opposed to credit, like many people have in the developing world when micro-finance has been the first thing to, you know, the first financial experience, and it's about acquiring a loan and having to pay back when, I tell you that at least 90% of people living in the West would begin their financial life with savings, we have [connection interrupted] at least, you know, our parents open savings accounts for us and obviously, our financial outcomes are different, because your financial outlook in itself is different, you know? So, the kinds of services are differently and this type of initiatives, I think, are very powerful to shift, you know, the situation in this direction and then, they love the concept of financial citizenship which I also quite like, you know, making financial access right. On a personal level, I believe that financial access is paramount, is quintessential to the life. You know, the reason why you don't have basic services up in the mountain where we left the granny, why she doesn't have running water is, because somebody couldn't figure out a business model where they could be paid for providing clean water. Because these people don't have access to payment services, they don't have financial access. So, **the more financial access with the local ties, I think the more we are likely to reduce poverty or at least to bring basic services to the people who need it the most, or the people who lack them the most.**

JM:

I completely agree with this. We should always have a very critical eye on market-based approaches in general, I would say, and not, kind of, close the eyes in front of, let's say, supply-sided interests too much, but I completely agree that it can, if done properly, can be an equitable tool to reduce poverty and I hope we're incrementally getting there a bit more. Thank you so much for all the input!

**End of Interview**

## Full Interview – Prof. Avner Levin (AL)

### Discloser

At the beginning of the interview, the digital ID-system of 510/NLRC was briefly introduced. AL asked several questions, suggesting personal concerns and awareness about the potential exclusivity as well as arising data & information-protection issues when utilizing some sort of ICT with CBA-mechanisms.

According part of the interview, based on a confidentiality agreement, is not displayed here. Furthermore, were some subsequent passages relating to 510's system design excluded.

AI was aware of the concept of an SSI before the interview.

JM:

Firstly, I would be interested, when we are looking into this issue of KYC-compliance, what you have indicated in your paper and what used to be the case in a lot of contexts, is that, given a humanitarian crisis, governments are willing, sometimes at least, to accept certain simplified KYC standards for the recipients of humanitarian assistance.

AL:

Yes.

JM:

Relating to the underlying question of my research, that the identity component of the system here aims to provide for a long-term impact, are you aware of any contexts, where these **reduced KYC-standards were also applicable beyond the humanitarian crisis?**

AL:

**No**, I'm not aware, actually. And I thought, I think this is a very good interesting question that you might be able to see, for example, in your two countries Kenya and Malawi, if there is a different kind of attitude on behalf of the government with respect to KYC. It seems like in **Malawi** [connection interrupted] to **the more simplified way**

and in Kenya, maybe not so much, right? Because it's a **more**, like a **stable country**, even though they have like these places where they need the Red Cross and others to assist them, but I have to take you back also to the paper because to me, what I tried to say to the aid agencies, is that you're really, sort of **giving up almost half the battle when you start engaging in the conversations over "should the beneficiaries actually be required to comply with all the KYC to begin with?"**. Because there is typically, I think you know, the **entities that are directly regulated by KYC, are the banks** that give the money to the agencies, so, there is like at least, I would say, one or two levels removed between the entity that is KYC-regulated, and the first thing that is getting the money. So, if I'm a person in Malawi getting some aid from the Red Cross, it is not the same as the Avner, the customer of the Canadian Bank, doing a financial transaction. **And I think, the responsibility of the agencies, and I don't think that they've done enough on**, is to really push that awareness, that **KYC** there is sort of, in my opinion, you know, a certain **context** that is **appropriate** for it. But I don't think that **the humanitarian crises** certainly and even the ones where they're giving perhaps aid in camps on a **longer-term basis**, even those, **I don't think that you can really say that the beneficiary has to comply with KYC**. So, I'm a little bit, you know, a little bit, **I like to push against this idea you have to have some KYC-standard that will apply to all these people** that are lining up, whether it's in the aftermath of a crisis or whether it's a longer issue to receive aid, to treat them sort of like as the bank customer in the Western World, right? So, I think there is a bit of a problem there. And I also, if I can just say one more thing, I also think that, when you look at the policy purposes of **KYC and anti-money laundering, I think it is typical to see the problems like**, you know, it **could be at the level of aid agency employees**, but **I don't think, it's necessarily at the level of**, you know, **individual beneficiaries** that, you sort of, **if you're looking at where is the greater risk**, who has greater access to the funds, who has the ability to manipulate, I think those are the issues to the extent that you have a camp in a situation where you think, well there some kind of negative elements controlling a camp instead of directing, you know, sort of, ceasing the money that the agency is giving two individuals; again, I see that as a problem that KYC is not necessarily the answer for that problem. I think you have a kind of a social, criminal, political problem in the context of that particular camp which, you know, about really, and you can solve it in whatever kind of method, but you don't really need the KYC, again, to sort of do

that. So, that's my challenges with the whole kind of "let's make sure we're in compliance with KYC". That's what I would say.

JM:

Thank you so much for that answer. That's..., I completely agree with that sentiment. But, uhm, relating to, uhm, that possibility of having, we already talked about, uhm, the possibility, uhm, of providing assistance in a longer-term than solely within the scope of a crisis, meaning that the humanitarian organizations, if they want to make a use case, or have an argument for their beneficiaries or recipients not directly being included into that KYC-, uhm, KYC-compliance, uhm, discussion. What would you think, how could humanitarian organizations argue for that, because it kind of goes away from their traditional mandate right?

AL:

Yes. And I think it's more difficult for them as a result to make a compelling argument, to exclude people, and I think there's a very interesting debate in the field, in which I don't know enough about, you know, sort of like, the permanent refugee status and the permanent aid giving in that context of refugees in this discussion in the refugee, sort of, literature about it, but it's not my field of expertise. But I'm aware that this this poses like an intellectual problem for people that are studying the idea of a refugee to begin with or anybody, that is in the need of aid. And I think that the **aid agencies really have to look at their mandate** and sort of see what's the core, what's essential to our mandate? What are we all about and what are things that we're just sort of like doing maybe because slowly we started doing it, but if we step back, why are we doing it? I'm, I can understand from the state's perspective why there would be **increasing tension** when they feel that the **agency** is sort of **encroaching** doing things that **the state should be doing**, and sort of **excluding the state** and if you're already a state that is politically not very - and socially - not very kind of a stable, robust country, right? Because that's why the aid agencies are there. It **doesn't necessarily always help create long-term stability, having the agency there on a long-term basis**. So, I see all kinds of difficulties with that and if, you know, if I were looking at it from a, I guess, a neutral perspective, I **don't know why I should be receptive to an argument of that you need to be exempting people from KYC, if it's something that is going on, for years**, let's say, right? I can very much understand the rationale

for, you know, we have a crisis we're in and we need to help people. That makes a lot more sense to me from a KYC-policy perspective, but I, I don't know and that's why I haven't seen, again, that to my knowledge, I have not seen simplified KYC in places where there is like this longer-term aid, kind of, relationship or delivery.

JM:

Thank you so much for that reply, again! And, uhm, relating to that, uhm, KYC policy perspective, but, wouldn't you say, a compelling argument in favour of a reduced KYC or a KYC- exemption is, a situation, let's say again, a refugee camp, here people don't have the means to formally comply with KYC in the long term. Would that, would that be an argument for you, after your personal opinion, would that be argument enough?

AL:

I think, it really - I guess I hate to give you the lawyer-answer of it - depends, right? I think for me, it would depend on, you know, people can be, let me think about the example that we did. For example, let's say in the **context of the Syrian refugee camps in Jordan and in Turkey, I think I can accept that argument.** There is still some kind of conflict going on in Syria and you can say **they're in a refugee camp, but they still need some kind of simplified KYC-approach that would allow them to still get services**, the countries in which the refugee camps are based, still see them as like, sort of, temporary, whether it's Jordan, whether it's Turkey. So, I can see the rationale why you would want to say, you know do something that is simplified for those people. I think it's a question though, what happens if they're still in the refugee camps ten years from now and I think, you know, I, you know, I think the classic example of the long-term refugees are the Palestinian refugees and the question to, it's a very politically loaded question, but they are considered refugees. But then, the question is do they still when we're talking about, let's say, from 50 years or maybe more than 50 years that there in a refugee status, can they still claim that they need a simplified KYC, when we're talking decades? I think, I would have a bit more difficulty, seeing, even with somebody who is legitimately internationally called a refugee, to say "well is there not an infrastructure in place already, that would allow you to, you know, be in compliance with whatever the KYC is." So, I think for me, if you want to distance it from, you know, this political conflict with that political conflict, the issue is, is there really **an opportunity to create the infrastructure that we need to support** the, the

regular, let's say the **regular KYC-standard**. If there is an opportunity to do that, I have a hard time in arguing while you shouldn't do it. **If there isn't an opportunity** and if it's still like, sort of like, or kind of a **temporary refugee**, then I would say you can still, **should argue that you need that simplified approach**. But can I say maybe one more thing about the simplified versus the regular, which is I don't necessarily think that whatever you're proposing or developing, or other people are, are developing, necessarily has to be called "simple". I mean, if it's its own identity, I think the governments, there might be some kind of, or even the agencies, uhm, there, perhaps, perhaps there should be the recognition that just **because it's digital and distributed it doesn't mean that it's more simple or more rudimentary or lacking the features that the regular government-issued photo ID** would have, right? Because you could have all those components into whatever it is you are developing, and whatever other people are developing. So, so I don't necessarily see, why the kind of, I don't see that this is the same division between simple and regular than digital and traditional, right? Let's put it like that.

JM:

I completely agree with that. So, we, as indicated, if we would have a certain infrastructure, for example, the identity infrastructure in place, there's not really a compelling case to make for simplified KYC. But, given the assumption, that we're looking into some context, not necessarily even at the refugee context, but maybe at some ethnic minority for example, who, officially has access to a certain ID infrastructure. Both is the case in Kenya and Malawi. We have had massive roll out of national ID systems. However, certain literature and certain people from the field indicate that not necessarily everyone, although being a national in Malawi or Kenya [note that this seems to be more of an issue in one of these contexts, I purposely decided to keep it on a more general level, however] has had the chance to obtain such an ID, thus automatically is excluded from, from, accessing public services.

AL:

So, this is along, like ethnic lines, groups within the, sort of country, that the majority and the minority...

JM:

For example. It's not only ethnic minorities in the case of Malawi and Kenya, it's just for example, hard-to-reach areas, rural areas, people failing to, to see the added value of the national ID initially, not signing up for it. So, there might be some people still being under the radar, while universal ID coverage is claimed. So now, the question is, okay, these people are not included in that ID infrastructure, could the humanitarian organization, such as the Red Cross having an identity system, which potentially is highly trustable, inter-operable and brings along some nice features, could that replace the governmental infrastructure to yield formal KYC-compliance or not? And I mean, that's a very contextual question right now, but I mean...

AL:

I think it is contextual, but I think it's also going to be a **question that's resolved not necessarily in the aid agency context**, but it'll be resolved in the, really, **first**, I think in the more financial, **traditional financial context**, because you're seeing the same conversations with the digital ID with again, with traditional banking, with traditional customers in the Western World. Those are the issues that the banks are struggling with and that, you know, initially, the attitude I think, on behalf of governments and banks was absolutely not, right, this would never be like some kind of an alternative to whatever we need. Again, even in the, I think, starting from the context of, let's say, the West, and things like, customers and pressure, from the business perspective, I can see that perhaps a little bit softening, that banks have an interest now and sort of started trying to, you know, get a jump on like, the Blockchain platform and try to experiment with things. So, I wouldn't, I wouldn't necessarily rule it out. **But I don't think that the compelling case for them will be the case of the, you know, aid circumstances.** I think if it happens, I think it will come about from the traditional banking, from the traditional customers, the traditional sort of, kind of competition pressures between banks in a country or operating in other countries. That's where I think you might see both those pressures. But I don't think like, I mean, **I don't see that as an immediate development.** I think, I think a lot of, there is still, this technology is so far, you know, in terms of the current, to be adopted, right? So that I really don't see it happening in the sort of, short-term, right? That's to the point about how and when it'll become available, **but even just from the perspective of individual end-users**, you know, so I don't think that we're there yet.

JM:

Uhm may I re-phrase, or try to re-phrase, something you said while making an argument. I'll just make sure I got to right, because I'm not sure exactly. So, what you, to my understanding, implied is, uhm, sorry, let me think about how to, how to put it.

AL:

Sure.

JM:

If, relating to what you wrote in your paper. So, there you wrote, that ultimately, it's the responsibility of the service provider to comply with KYC, it's not the individual...

AL:

Exactly.

JM:

So, it's not the individual, but it's the service provider's task.

AL:

Yes.

JM:

That means, if, uhm, a service provider would see risks as massively with a deployment of the [potential digital ID] system, that even out of the aid context, it could yield acceptance of the service provider? And this is kind of apart from whatever the direct regulation concerning KYC-compliance says.

AL:

I see, yes, that's correct. And I think, I would maybe add to that. I think, it goes back to blockchain and understanding blockchain, right? Because there is this kind of, for individuals, like this paradox about blockchain. Because it is supposed to be an open ledger system, right? That you see all the transactions that sits on all of the computers. From an accounting perspective, what better mechanism would you wish for if you wanted to see sort of where the money is going back and forth. The problem of course is not in the blockchain. It's in the hashes that maybe you and others are creating that are protecting from, I'm saying a problem from an AML perspective and a KYC perspective, if you are protecting the identities of the, of the individuals or entities, that

are involved in every transaction that appears on the ledger right, because they have this kind of - so, so it's, to me that part really goes back to a discussion that's not really about blockchain. **It's about encryption. It's about confidentiality. It's about anonymity.** It's something [connection interrupted] before blockchain was around, and the question really is and that I don't know that I'm willing to understand, but the question is will there be analytical tools to analyse what happens with transactions on the blockchain to sort of see that at the end of the day, we don't really care who has the money but we can see for example, the Red Cross, took 100,000 dollars, distributed them to, you know, a thousand individuals, and we can see in terms of the money flow, all the transactions on the ledger. We don't know who those thousand individuals are, but we know that nothing sort of is going to open at least for other purposes. **If we're able to sort of analyse the blockchain, the ledger right, to that extent, I think the bank would be a lot more at ease with not knowing who each person is.** I think, **the challenge right now is the banks feel that they cannot do that, or governments feel that they cannot do that. So, the ledger is there, but we can't really sort of, analyse it in that kind of way, that would help their anti-money-laundering purposes.** So, **they crack down on the encryption-piece,** because they want to sort of see, who is doing what. So, I think, I think we need perhaps some more analytical tools about the ledger, or that would deal with the ledger, and that would help perhaps with respect to my earlier comments. But I agree. I think you re-phrased in the way that I understand, yeah.

JM:

Uhm, so, if I understood correctly, you're suggesting, once the banks would be able to see, that, even though personally identifiable information are not necessarily inside the system, as long as they are able to have that transfer and record of transaction and understand how it works, that they would be very likely or at least more prone to accept such a system.

AL:

Yeah! And this is the risk, because, actually, the, you know, the interesting thing about blockchain, and, and if you go back to Bitcoin and cryptocurrency is that it's sort of right now, used by, you would say perhaps, slightly more criminal elements, right? But if you look at the technology in terms of having an open again, if you focus on the **open**

**general ledger** part of it, then you could actually see a day, where this **could be quite a surveillance tool, right?** Cause if you do it, like, sort of, you know, you have privacy concerns of a different nature. So, if every transaction is recorded and you got all the information you've got the algorithms that are able to crunch all this data, you're actually in a situation, where there's a lot more transparency to the extent maybe you then start worrying about it as a citizen in a democratic society as to what this all means and how this could be abused by a more totalitarian government, right? So, there is tension here, right, between the between the two. I think, we're like, because we're at the stages that everything is developing, we don't know how it would go, right? But, there is room for caution, I think, on both sides, that's what I would say.

JM:

Also relating to what you wrote in your paper, you said that, uhm, aid agencies should take care that KYC-compliance is not used as an argument by, by governments to actually retrieve sensitive information about potentially persecuted minorities etcetera.

AL:

Right.

JM:

But if, so uhm, if you take away, that, that bad potentially bad, intention what you just said, is that as long as government and service providers understand the system and, and see that it's transparent and that AML-risk would be reduced accordingly, or at least, to a certain threshold, that governments would generally be totally fine with accepting not accessing personal identifiable information, right?

AL:

Exactly, exactly! And then it also would be a way for the agencies, to really, at that point, for itself, understand more, what is a legitimate government enquiry? And what is the government requiring that is, really, based on some kind of political conflict motive or some kind of other, other issue, right? And I think, that that's the role of the values of the principles of the agency there, right? To what extend does coping with the government on the ground because it wants to deliver the aid to the people that are suffering, at what point does that kind of collaboration become a little bit too worrisome because of the repercussions the people are facing. So there really is

promise in the kind of, you know, kind of open general ledger that while the identity of the people is protected, so people don't worry about the individual kind of repercussions. There is the ability to show the government: "Look we're in compliance with whatever it is in terms of AML". You don't really have a case to, and it sort of helps the aid agency and its relationship with the government at that point.

JM:

Interesting, very interesting. Uhm, may I infer, or, did I then understand correctly, that, uhm, you're suggesting implicitly, that whenever the government has more questionable intentions in relation to obtain KYC-related information, that humanitarian organizations should not use a mechanism of delivering assistance, which would require giving out all this KYC-related information.

AL:

Yes, and I think, to some extent we talked about it in the paper a little bit and this is what one of my [in the deleted part of the interview] questions to you is, like the movement to, like the set of cash delivery is going to in aid, maybe one solution in those particular situations is to not deliver cash and to set aside, kind of, the whole KYC-issue and deliver aid in other forms, right? Whether it's food, whether it's assisting with infrastructure, whether it's shelter, whether it's clothing, you know. Do some of those activities and not necessarily go into the cash, kind of, problem. You know, there's always going to be the potential for corruption anytime you are offering some kind of a resource, right? Somebody might take control of all the food and then redistribute according to whatever criminal system they devised in the camp, that's always possible. But, I think for some reason, this kind of KYC and the set of issues that come with anti-money-laundering has become very prevalent, very prominent in the aid agencies, because of the pressure that their financial institutions are exerting on them, and because of the pressures for accountability that the agencies are facing in terms of showing what they do with the money that they receive as donations, or from other, other sources in their home countries or in other countries where they sort of raise funds. So, there is this push, you know, for aid agencies to be more business-like in several ways. And part of that is saying, "well, why are you not complying with KYC-standards?" And this goes back to more of the things we were saying earlier, I think, the agencies should be quite proud in saying, "you know, we're not a bank, we're

not a business, we are an aid agency, the standards which do apply to those institutions in those functions don't necessarily apply to us." And again, I think open ledger, could help that, you know, whatever it is that you're registering on the ledger could help agencies demonstrate to people, that sort of, have criticized them for not being very, perhaps, transparent, or that it's not very accountable to sort of show "you know, here, you can take a look at the ledger, you can see whatever happens to whatever resource that you want to track". So, there's a lot of potential, actually, in the open ledger idea when it comes to the accountability of aid agencies and enabling them in that way to sort of, you know, resist the pressure that exists right now.

JM:

Would you, I mean, that's really going away from, uhm from your expertise maybe, or I'm just assuming that, but would you, uhm, have a personal opinion on how to make a successful use case for, for showing the banks, "Hey, okay, we, we have a system and it works and yes, it's complicated. But here it is" and uhm...

AL:

Yeah ,you see, if I, I mean, if I'm the aid agency and I have to sort of say "well, what should I be focusing on", **I would probably still tell the agency focus on making a case that you should not really be subject to all these standards to begin with, rather than spending a lot of energy and trying to show, because I think it's too early right now and I think the banks, for a number of reasons, won't accept it.** Maybe if we talked ten years from now, and the technology is more widely, sort of, accepted in society, it will be easier to sort of, show, instead of like the development of, you know, the payment card industry standards, right, that sort of started off with things that are less familiar. The credit card was not as known, all the standards were sort of like not clear, and then, now we have all these very robust standards with technology with these pieces of plastic in the chips that are on them. **So, I think you need to see the technology becoming a little bit more widely acceptable** and then more routine uses, right. We sort of don't really have right now this basic kind of widespread use by individuals, that would allow the banks to be familiar with it. Even at the level of individuals that are working in a bank, right, because you sort of have to bring it back to the human being of all, right, and like you say, every time you talk to people about blockchains, so well, do you understand what it is and when you go and

talk to a few of the people that are working on blockchain, again, you can have very interesting conversations about, really, what's the definition of blockchain, what's fundamental to blockchain, what do you see as the essence of blockchain, you know, all the kinds of issues between experts and those who are working in the field. So, I think, I think, **the ability to make a successful pitch, or use case, maybe if you do a very kind of, controlled experiment, in one camp, that you can sort of, try to, it would really be more like, I would say, more a social experiment and less like a real life situation.** I don't know how well the banks would sort of buy that, as like "okay, well, then they can use it in any context, at any time", but it'll be a very interesting, like, research project. I have to say, I haven't thought about it like that, but it would be, from a research perspective, very interesting to sort of see how, how that would work, and I think everything as to start somewhere. So, I don't want to dismiss it, I mean I just don't know, if it will happen overnight.

JM:

[Some parts are deleted here, because of a data-non-disclosure-agreement].

AL:

Maybe we didn't talk enough about that, but I think, that's also a role that the agency should play. It shouldn't just be like a conduit saying "Okay, well, let's just push this all on the beneficiaries, and make sure that they've got some kind of form of ID", but to the extended that the agency, and I think, **it also requires the agreement of the provider**, right, because some providers would agree, and some providers might say absolutely not, because they understand it differently, but I certainly think, having looked at the laws and the regulation, **I really think that there is a legal basis for an agency to always say "you know what, I'm your customer, I'm vouching that what I'm doing is in compliance. You don't have to worry about what I'm doing with my beneficiaries."** And I wish actually that, more agencies would do that. **Even if it's not in the context of a pilot, just in other ways of delivering aid, because I think that, that's, that's probably the best that could be from the beneficiary perspective**, I think.

JM:

[Some parts were deleted here]

I had the, at least that's how I interpreted it, you're not the, let me say, biggest fan of that idea of the humanitarian-development-nexus. You're more, I had the feeling, that you rather would see the tasks of a humanitarian agency in providing immediate relief, or maybe even in a protracted crisis, so, ok, supporting for a longer-term, but not necessarily chasing long-term development impacts, which would be rather, uhm like, a task of development corporations and not humanitarian assistance.

AL:

Oh, I think it's fair to the extend, that I don't focus really on who else, who is doing the development, but I think, the agency has to step-in with a state that is failed. That's my understanding of it. So, if there is a failed state, or a state in crisis that is just overwhelmed, you come in from other parts of the world and you assist them. I think, the question is, to at **what point do you stop assisting and start taking over things that the state should be doing? And then, leading to sort of an increased dependency on foreign aid** and as you know, there's many prominent scholars from Africa, that are saying "you know what, actually all this aid over the years is just a result of the failed states. We need to become more independent and build our own infrastructure and take the risks of corruption along the way". And I am very sympathetic to that. I think that, I think, I think that, you sort of hear the voices, you know, the authentic voices of the people that are in there and their experience the way that they've lived it and that's what they're saying. Not somebody who's looking at it in that in that detached kind of anthropological way. I think, you have to listen to them. So, I think, I think, yes. To me, that's the best way to understand, what a relief agency is, an aid agency is about. And I wish, longer-term, that there would be like some kind of a transition mechanism, right. So that you could start handing over things to the state along it, to become more independent, more robust and having ultimately a situation, that you know, we are, you know, if you're looking at the first world, the Western World, there is always going to be role for disaster and relief agencies, but by and large, most of the other stuff happens through the regular government and I think, that to me is how hopefully it comes about other parts of the world as well.

JM:

Thank you so much for that input! Relating to the identity system the Red Cross would aim to provide, would you then argue, that the ideal case of such a system being

deployed would not be necessary solely in the sovereignty of the humanitarian agency, but ideally support for the national identification system, as long as a certain responsible usage of such a system was given?

AL:

Yes. So, I think, I mean, I think you have to be a little bit careful here and I mean, also, as people that are sort of, like you mentioned, starting up and developing into that space, there is a debate over what's the preferred form. And it's a very lively debate in the blockchain community, as to what is the preferred form of identity in the world, right. Should we have sovereign national identities, or should we move away from it. And I think, you have to be careful to not confuse that debate, which I can, you know, certainly see the rationale why you would not want to have, you know, state-controlled identity and the appeal of having individuals control their identity. There's a lot of it that's very appealing to me, but I think that should not be confused with how aid agencies interact with governments on whatever it is that they are doing. In other words, **you can have an argument**, that at the end of the day, **everybody should sort of have an individual identity that they control and still not say that the aid agency should be the one providing its own identity as an alternative to a government identity. Perhaps, the lobbying should be on governments worldwide**, to say move away from the things that you were traditionally doing, but **I don't think, that necessarily means, that the alternative identity provider should be the aid agency**, as I still **see the role of the aid agency** starting at the beginning, from the, from the **primary purpose of providing aid. It's not in the business of providing identities**. So, in order to provide aid to people that has to come up with some kind of mechanism and it has now maybe the ability to do it in a technologically very savvy way, but that doesn't mean all of the sudden, that again, that in sort of like, a business that is now offering like kind of "here's my identity product for you country X or country Y, why don't you take it and use it". Maybe a start-up to do something like that down the line, and I think that would be really, perhaps neat, but I don't think that that's, to me, central to what an aid agency should be doing. So hopefully, that's clear.

JM:

Thank you so much for that! Coming to a small question I noted down. It goes away, it kinda interrupts the flow, I'm sorry for that, but, uhm, making use of you being the

legal expert. So, Malawi and Kenya both are not part of the FATF, still, I would assume, not being a law student, so that's probably a first semester question, I would still assume that, when we're talking about this relationship between the aid agencies and the countries they are operating in, that aid agencies would still need to adhere to the FATF recommendations.

AL:

It's not a beginner question. It's actually a very interesting question. Then, I think, I'm sure the cautious lawyer, will still tell them "Yes, you should comply", but I think you have to look at it the country has jurisdiction over the laws and its territory and the banks that or financial services providers in its territory. Whatever rules at Kenya or Malawi have been placed if they exist at all, in some cases, there are no rules, that's primarily what those banks or service providers like you mentioned with the mobile provider, that's what sort of they have to comply with. It gets a little bit more complicated when you were talking about an international agency, because then, they might be operating in other countries, right, not just in Kenya. If we're talking about a bank, that has the ability to, sort of, operate in other countries, then they have the standards of Kenya, or no standards in Kenya, but then they also have standards in other countries. And that's how indirectly perhaps they might decide that we are going to do the task force's recommendations, wherever it is that we operate. But that doesn't strictly mean that they have to do it in Kenya. It means it's a decision that they made, and you mentioned the GDPR [in a non-disclosed part of the interview], right, so it's a good, data protection is another good example. Different places have different standards and then the businesses make their own decisions, right, and like the Europeans they, you know, "it doesn't matter to us where you operate, if you're a European entity, we want you to follow GDPR", right? So, the same thing could happen with respect to financial standards, if they were telling you "hey we don't care where you operate, we want you to follow", but the obligation doesn't come from Kenya. It doesn't come from Malawi. It's comes from another place in which this organization is doing business. So that's the best way that I would describe it, it's really not a simple question.

JM:

Because I really don't want to steal more of your time, I would like to ask you, if there is anything from your side, based on our discussion, which you might want to add, or any other concern you want to address, or any other question you want to ask to me?

AL:

It was a very interesting conversation. I would maybe only add one point to you, which is, you started off, and we talked a little bit about it, you can look it up at our report, about this need, or not needing to consent. To me, again, this is, this is a question that I, what I don't like about **the idea of consent** is that it **actually does not capture people's agreement in a meaningful way. It serves more as a risk management tool** for whatever the entity is instead of say, you know, I have a piece of paper or some kind of a digital version of a piece of paper, that I can sort of show to the people up in the KYC-chain that this is all okay, and according to the rules. But I would be much happier, from a data protection perspective, in not discussing this in consent-terms at all. Saying, again, because it's a vulnerable population in a time of crisis. Even if it's a longer-term **refugees** in a refugee camp or people that are receiving aid for other reasons, we **cannot really** sort of, at least not the way that I understand it, say that they're **providing their free consent** in a way that I decide to use Skype or Facebook or something like that, that I can sort of, walk away from it, if I don't really want to use it. And these people require that aid, so I think it's much better from the perspective of data protection, and again, whatever the identity that we're trying to protect, the basic notions of dignity [connection interrupted], give people the opportunity to provide consent, we're going to respect their identity, and we're going to tell them what we're doing. So, it's more like notice, **you notify people about what you're doing**, uhm, **because they don't really have the ability to decline it "Yes or no"**. Now, I don't know enough about the solution that you're developing. Maybe it's more relevant when you're developing this new kind of a solution than what we were looking at in the past, but I would certainly not automatically think even with the GDPR, that "Oh, I have to go to sort of, tick a box because people are consenting to whatever it is that we're doing". I think I, you know, **consent** is, to me, a concept that the more we have, like, ongoing digital information collection and, and digital identities is a concept that **is losing**, you know, from its, I would say, **explanatory power**. Like it's the principle of data protection and it's hard because all the **regulators still want to see as the corner stone about what we're doing, but I don't necessarily agree**

**with that.** So, all I'm saying is, you might want to take a look and see whether consent is actually a good foundation for what you're doing, or maybe you should be focusing more on saying "well, we really need to notify people about what we're doing with this, but then, we really need to be strict about how we're going to be using this information, what's going to happen with the digital identity." Those kinds of situations down the line, you know, when a government comes and asks for some kind of a [connection interrupted] more helpful to the individuals, to think about, than it is to say "well I've got their consent which means that down the line anything goes". So that's the one thing I probably would want to add.

JM:

Thank you so much, that's a very brilliant point, actually, you're making. But what I would, sorry, I need you to clarify that quickly, so, this, this notification for you, uhm, from, from a normative point of view, would, uhm, because I think I also failed to get that argument completely in the paper, would basically be, for you it would be more honest in a way?

AL:

Yes.

JM:

But is that the only advantage?

AL:

No, I think notification does not, you have to recognize that what you're doing is notifying people and not getting their consent, but that doesn't mean that that's the end of your obligations. **Your obligations do not end by notifying people, your obligations, then are even stronger, because you have to take care of that information. You have to be a responsible information steward and you have to have all the protections in place particularly, when it comes to secondary potential uses and disclosures of this information down the line. So you actually have a greater responsibility and that's the reason why, if you want to be cynical, most companies don't do that and they just choose to take consent,** because they write legally in these things that I agree to them doing whatever they want with that information so **it actually frees them down the line with all the secondary**

**purposes and disclosures** and I would feel, so I think, by no means this is just about notice. It's very much also, then what do you do with the information, once you have it you have to, and I would say **as part of notifying people, you** should actually be saying to them **quite clearly what you will and what you will not do with the information that you're getting from them**, because that's always a concern for refugees right, that's a concern that you've seen with the traditional systems, like are you going to take my information now and hand it over to the government, so that they can come and chase me right down the line, right, you know, while I'm fleeing from them. So that's always going to be the case, that **you have to clearly promise them what you can and cannot do with the information that you are collecting about them**. So that's what would complete the picture.

**End of Interview**

## Full Interview - Vincent Graf Narbel (VG)

### Discloser

VG is aware about digital ID-system of 510/NLRC, the surrounding research and the concept of an SSI.

JM:

I would very much like, if you don't mind, start with a more open question, which does not necessarily relate to your background, but uhm, if you don't mind, ask a question and you can answer to it, which, like, like, however you deem necessary or important. So, regardless of a certain context we're looking into, if you would implement a digital ID system would there be, after your opinion, some potential hindrance towards some populations or some individuals of making adequate access to such a system or making the appropriate use of such a system?

VG:

Can you just tell me what you mean by hindrance, like in...?

JM:

Sure. For example, let me say, in the context of sub-Saharan African country and I am a woman who never has been to school, maybe he has issues with reading texts, maybe I don't have access to a smartphone and now I'm handed this potentially ground-breaking Self-Sovereign Identity in digital form, would there be some exclusion factors you can think of?

VG:

Good question. I think, as far as we are concerned, we, there are two things we're looking at. The first one is with regards to digital transformation, which is something we're starting to really, you know, to invest seriously on. So, digital ID thought and all that general transformation, so to speak. With, so **digital ID** obviously, you know, obviously, is going to be **one of the cornerstones of providing new digital native services**. Cause we also make a difference, we also make a big difference or not a big, but a form of **difference** between, you know, digitizing existing services. So, bringing **new digital tools to keep doing what you do** a bit faster, quicker, cheaper,

and designing, really, **new services that are digitally native**. Now, CTP, so **cash transfer programming, lies a little bit in the middle**, because you definitely, I mean, **it isn't digital native** to, actually, you know, bring piles of cash and distribute, but, **so it's more than falling into digitizing it**, so making sure that you have tools that speed up in and then, you know, actually increase the efficiency, essentially, of the service. In the other end, **if you think about either mobile money**, or, you know, even people thinking about **cryptocurrency** type of distribution, then **these are digitally native**, right? And **then if we, we go into different ball games, because while and when the first one, the former way of distributing cash, will lead obviously to the problem you initially mentioned in the question, that second kind of, doesn't make sense because if you're saying, you know, we do implement mobile money, then of course people not having a mobile phone are anyway excluded from your initial design**. So, I suppose, that it's probably okay for, whoever implements the program, to discard this, this, gap, right. In general, though, we cannot really discount the gap. But again, if we put the people, and that's what we're really striving to do, if we put the people in the centre, so the customers, the beneficiaries, the affected population, at the very centre of all the design, then I would argue, that if your community, **because one size would not fit all anyway**, right, if the target community of a given programme, is not educated enough and not connected enough and not whatever enough to, you know, get the service through super, you know, super fun technology kind of things, or let's say, these kind of technology advances in general, then I would kind of argue, that probably, **the programme is missing the point**. And that, that you have to find other ways, because if you, and many, not many, but a few, a few people are designing fairly nice solutions, stats, that are capable of bridging physical and digital, you know, in the forms, of even sovereign, kinda have whitepapers, where you can print things and sort of have a digital wallet, not wallet, but let's say, digital ID printed, so, that it kind of works et cetera. So, this is necessary to have these thinking, in order to, when your programme, has gone through a proper ethical and feasibility study, et cetera and you go for it, digitally speaking, **even if your, again, your finding shows, that the vast majority of the, or your, target population will be capable of using an understanding the solution, you still need to have ways by which you not gonna exclude a given individual that can't get it**. But again, in general, if we kind of say, you know, "Oh we're going to design a solution which is whatever you say et cetera, et cetera", but then, what are we going

to do? **Because 60% of the target population is not going to be able to either use or understand it, then why do you do it digital?** Why, really? Who is it for? Is it for the donors, for their transparency and shall we all have pressures by donors, to have that transparency? But perhaps, we also have, a, an obligation perhaps, not to resist that kind of pressure but at least to, either counter, or balance, and sort of, you know, sort of explain why, you know, in certain cases it doesn't apply. Now, I want to make kind also, something kind of clear here and emphasis on something that, ICRC is different from others. It's that by mandate and actually, in reality as well, we do essentially operate in **conflict zones and war-zones right, and there, I suppose the risks of kind of, persecution**, typically, coming or stemming from, you know, having, so well identified a given community because of nationality, status and, and religion, and God knows what, you know, having that kind of classification or identification of the community, brings **a lot more risks** than say, for example, when you are an **early responder to an earthquake** and where, basically, where you wanna look at, is to say it's not about giving your aid, to, you know, people based on their the status with regards to, you know, violence, but it's about saying who really needs and then, the devil is in the detail and it makes a big difference, really.

JM:

Alright, thank you so much for that substantial answer! There are a lot of points, I would like to come back in the process of the interview. So, let me start with one interesting thing you said about, uhm, kind of relating to the principle of impartiality under which the ICRC, to my understanding is also operating. So, you indicated that any digital solution, would only or should only, be deployed to a certain context, if the majority, or if all people, could appropriately be included into that digitized solution. Did I, I was not completely sure, if you said that any individual needs to be included, or, if we have a certain threshold after which we can say, "OK that digital solution would make sense".

VG:

Well, I mean, right. I don't think I have a definite answer to that, but, to consider, first there is the conceptual aspect, and then there is the pragmatic and you know, sort of, operational, but from a philosophical perspective, you know, really, there are so many different contexts and talking to some of my colleagues in implementing these programs in the fields, you have things such as, you know, some communities really,

and it's not a small number, but like, communities where you know, **the notion of a proxy for gathering aid, at a family, or sub-community**, or whatever. They have ways by which they represent each other in some communities. And, and so that's just one aspect that could make the program fail, if you're kind of requiring every people to be physically present to identify themselves. **You might factor that into the design of your solution, so that, you know, you can, sort of, have enough proxies for your own identity.** But, it just highlights that there's so **many different local characteristic** to, to how people behave to that. So, for sure. I mean, if, I don't know what the magic number would be, in principle, it should be all of them, right, it should be a total inclusion, with all kind of, exception handling possible et cetera, et cetera. I suppose, that in general, it depends also a bit on the emergency of the situation, where you know, if you, if really, literally, your colleagues in the field are literally saying that people are dying now, because there is no foods, drugs, whatever health kind of things, and you know, you can in hours deploy something that at least is going to help a majority, or a large number, then you know, that would take precedence over, you know, the concept of inclusion, I suppose, so there is not one solution to that, but it's definitely an element to take into account.

JM:

Alright. Thank you so much for the answer again. Uhm, now coming to ICRC specifically. You mentioned that, uh, ICRC would mostly, when compared to other crises or other humanitarian disasters, would mostly operate in a conflict zone, where any deployment of a digital solution, or any revelation of personal identifiable information might yield further persecution, stigmatization, violence etcetera. So, if, how, is any kind of identity system or any kind of digital uh, system deploying an identity in such a context when third party or even a second party, such as the government, might access such data?

VG:

So, you mean what are the different alternatives, or...

JM:

In a way, yes. Automatically, is this kind of issue automatically yielding the need for an alternative?

VG:

Yeah. Uhm, I don't think I have a 100% overview of the different ways, we do, we implement in general CTP. I know, that in certain areas we did cancel programs because the requirements of the, you know, **local or regional, national authorities, the requirements to get access to some of the data were deemed too dangerous for the populations**. That's for sure. So again, it has to really be spoke to the situation and so, the situation from geopolitical level. You know, what, are the forces in presence, or typically, what is the risk? Say, a IDP [internally displaced] population, you know, is going to be, today, they don't risk much to be in a way, if we share their, you know, names and a minimum KYC so that they can benefit from the existing financial service provider and have capacity, but if, if we kind judge again, that yes, but the thing is, you know, the front line moves so quickly, that potentially, **two weeks from now, all this information will fall into the hands of the wrong person. Then, we might also take a different approach**. So, that is for sure. Now, the **risk assessment is, is very much geared towards classical data protection discipline**. So, you know, documenting and checking as much as possible of the data flows, and an understanding which one is mandatory to achieve the result of saying, distributing cash versus distributing vouchers, versus distributing in-kind, and, and again, you know, how much, similarly, registering, registering beneficiaries with digital ID also has, as we're saying initially, values for efficiency. So, this is all so very much balanced. And there are, there are places, I suppose, now in East Africa where, the sufficiency guarantees in regards to the secret of the people are met, so that you can even optimize looking at efficiency. But there are other places, where even, the modality to provide cash, specifically the last mile, would bring so much burden, that we would definitely not going to go there. So, again, the reason of one size does not fit all, but if you allow me to refer back to the initial comment: Then, I think, I'm really convinced that we are still **quite far from having, really working solution for Self-Sovereign, or digital ID, you know, these kind of things, that were a bit further, of course, from having interoperability and data sharing**. But that's actually, you know, perhaps some people will say, "Oh my God, why are we so far away, cause technology works" so we can debate, whether technology works, **I think technology doesn't work, personally, very well, typically blockchain things today doesn't work, or not well enough**, and, but the second is again, we're talking about, you know, **most vulnerable people on earth, and you do not test on these people**, right? You **test in the lab**, you, you daily or weekly, whenever you make an advance,

you know, let's **check against classical** you know, **do no harm** kind of **principles** and then, you know, with that in mind, the good thing is, you know, it's fairly okay, if rather than having a shiny press release for a pilot you did in the field, you kinda take your time and you go, you actually do fundamental research and trials in the lab and kind of see "look, because we are aiming at 5 years from now on", then, you know, **I suppose, it's okay to have an assumption, that says, when we will be ready enough people would have access to digital Infrastructure, so that they can be included in the programme.** That's another way to look at it, I guess.

JM:

Yes. Thank you so much for that answer again. I very much appreciate your viewpoints relating to do no harm and representing a more cautious voice in uh, a time of hype, if that's fair to say. Uhm, so, uhm, relating to, uhm, before I'm, I'm happy to, to narrow things a bit down and dive a bit more into the contexts, I'm working on specifically, you mentioned a minimum KYC, uh, which, which would be applicable to humanitarian organizations, and then, in the face of disaster, where, where a humanitarian organization, would be, kind of based, to my understanding, maybe or maybe I misinterpreted that, but based on their bargaining power and mandate, would be able to, to argue for minimized KYC, for, for their recipients of cash transfer programming, uhm for [towards] a government and, uhm in the face of, regardless of a very current disaster, but maybe looking into rather protracted crisis response. Would you say, that a humanitarian organization has a mandate, to, to have these minimum KYC standards applicable?

VG:

To be totally frank, that thinking I had, after I had read your one-pager, really, was to actually, you know, think about it, in the, the exact sense, you just mentioned. Is it bargaining power, or just a call to, you know, basic humanity, or something like that. But, you know, I was reflecting about, we have something in the ICRC, which we call, we have the ability to create one-time use travel documents. In certain cases, we can issue travel documents. The process does require, we are present et cetera. But, basically what it means, is that undocumented people, we can ship them through even, and not even, through mostly flights, to reach a safe destination, right, so people without any documents, because we have, you know, discussed, and got an

agreement with the countries, of course, you know, countries of origin and countries of destination, but also with organizations, particularly, like IATA, you know, the international air transport organization, which basically says, "look, yes, in general you have to have passport, biometric data", to you know, reach the airport terminal, etcetera. But, we were capable of having that, for a long time, you know, long time. Just thinking about it, I thought "why isn't the same possible for typically, yeah, KYC-regulation". So, whether it's the, as I said, it's the bargaining power of, you know, something as broad as the movements, or even bigger, if we bring up some of our friends from UN or the large NGOs. Now again, ICRC has - we believe - and I don't wanna look like, cocky or egocentric, but one of the biggest differences between ICRC and other NGOs, uhm, is that we, you know, we, our mandate is an international mandate, which is, which is essentially the Geneva Conventions, and that in hand, we also were capable to bilaterally, get, what we call "Headquarter's agreement", in these countries, so, with this in mind, again, when you think about what is the, what is really about helping victims of armed conflicts, uh, I guess it makes, it would really make sense, to say, you know, in this case because of our mandate and because of, and it can be extended to other organizations that, we do have a way by which, might be temporary, might be under a conditions, technically limited to an amount, or I don't know, what, but I, yes, I do believe that **we should have a way by which we can get, you know, the capacity to deal with less stringent requirements.**

JM:

Ok, cool. Thank you so much for that answer again. So, if you don't mind, I would dive a bit more into the exact topic I'm researching on in the exact contexts, thank you so much that we could have this this discussion on the broad level beforehand, so, basically what I think [was] already indicated a bit in my emails to you and in the research abstract, is what we're looking into right now with the 121-system, uhm, which you're aware of, uhm, is, how the system could be deployed, for example in the context of Kenya and Malawi, and how it ideally would not only support, besides the open cash ledger and so on, would ideally not only support individuals in, in, or the humanitarian organizations, in sending and receiving humanitarian assistance in a more transparent and efficient way, but, ideally having this identity component in the system, ideally supporting un-documented individuals, or under-documented individuals in these two contexts in accessing wider public services and, uhm if I might give a brief overview

about [the] countries; both countries had a quiet substantive identification, national identification system roll-out in the last years, in Kenya there is a very strong push from a federated system towards a quite centralized system if that's fair to say, Malawi went from, from also a more federated system to a more centralized system, but has, uhm, seemingly a bit more, a still more flexible approach towards the previous identity credentials they had, and the question now, which I kind of am analysing through the lens of, or the analytical lens of KYC-compliance, or satisfaction, is how this identity system in these both contexts, could yield service providers, or regulating bodies, to accept the KYC-compliance. Are there any questions so far, was there anything unclear? Cause I might have rambled a bit.

VG:

No, I think that's so far so good, yeah.

JM:

Ok, good! Great, uhm, so, uhm, now looking into these contexts, but again starting, though narrowed down to the contexts, a bit it more general, as a personal opinion of yours, would you, knowing the system, and knowing potential characteristics of the system design, see a normative desirability in having such an identity system being provided by a humanitarian agency, potentially serving a more foundational purpose?

VG:

Yeah, so, uhm, it's really a tough one. And I understand it's at the heart of your research, that's why it's tough. I, I've seen, a while back, not so long ago, but a few months back, we were talking to a couple of governments that have made advances with regards to their digital identification things, so, Switzerland, France and a little bit in **Estonia, who is in principle the most advanced**. So, for example in France, they have something they call "France Connect", where the government provides, this, kind of the federation level, or layer, of, of identification. So, because there are, or the hypothesis is, they are trusted, it might not be this much as we speak, cause of the Gilets Jaunes, but anyway, they are trusted as a, as a government by their citizens, so they can play that role of oracle where they verify and grant some identity providers a super status, which says, you know, it might be the post, it might be tax office, it might be different, so with this guys, they have done the due diligence, et cetera, et cetera, certification and they kinda say, you know, in this service, these one two, three,

four, five service providers are good enough, so whenever you want a national digital ID authorization, authentication, you know, you go to us and so you don't need to, you know, multiply the number or places where store information etcetera, etcetera. So, anyway, and when we think about it more globally, I think, **I couldn't come up with an example** of something that is working at around the world, **that actually does implement this, this level of distributed trust** or, or even, I mean, even when you go on internet, right, and you have your https-connection validated, it still relies on the consortium of web browser editors, to have accredited a few top roots, you know, nodes as sort of certifiers, for saying that, you know, they verify whoever you are. So, what I'm saying is, if we take the examples of, so 121, I think, if I'm not mistaken, it has been some time since I talked, or got into contact, if I'm not mistaken, the ambition would be to create all the capabilities so that could be used by different actors, right?

JM:

Yes.

VG:

Okay, so there's no way I guess, that's an end. And I know that, it has been taken into account, because all the architecture essentially targets existing, big initiatives, such as [deleted due to non-disclosure agreement] and others, **but nobody would be able to, I suppose, to force in, with the identity, and sort of force a standard, standardization of this identity, because,** again, at the end of the day, **nations, states, will always have the power to either favour one or shut down another**, or, or do you know, but again, if, if, **if through usage**, you know, you, you can and then we can and **the humanitarian sector demonstrates that, uhm, by implementing in the right way, our functional identity, you know, we can demonstrate accountability, transparency, privacy-by-design and this kind of things**, uh, I'd say that the only way, the **only realistic ambition is that, you know, people are just going to see it's working and try to bring it to the, to a foundational level**, but, I don't know, **I don't see it**. It's really a hard question. What have you found out so far, anyway?

JM:

Uh, if I might give you a quick overview. I am also not able to produce a, uhm ultimate answers to the underlying question, because in the end we are still in the process of

developing the system and deploying the system, so, you can only gather opinions on, on the subject matter and cannot really rely on cold, hard facts obviously, uhm, for me, uhm as it is right now, and this might change in the process of my research, to my understanding, specifically in Kenya, where the government has these claims, this huge sovereignty in, in issuing and, and verifying and controlling identities, regardless of whether it's only Kenyan Nationals, but also refugees or stateless people, the only way how, how such an identity system would serve, or would incrementally serve a more foundational character, would be by, uhm, deploying the system in a very controlled, uhm, uhm, let's say experiment, following do-no-harm principles. Uhm, uhm, based, but this experiment would be rather based on an exempt status of the humanitarian agency, not so much by officially aligning with regulation, and then with this exempt status and then provided that the pilot is successful, or given that the pilot is successful, that decision-makers seeing certain cold, hard, uhm. decision-maker metrics, such as efficiency increases etcetera pp satisfied, having an incrementally increasing operability among various humanitarian actors and then, still in this in this kind of exempted status, and then basically, uhm, going to the government and saying "we have a system which is widely used among various humanitarian actors" and then, obviously, because the government still has this huge claim on sovereignty, for example the UNHCR-mandated identity, uhm, got quite restricted in their [its] foundationality recently, uhm, still any effort of including people into that system, would kind of not, uh, replace the need to also put a person's identity into the national identification system of Kenya, would not replace the need for, for a person putting his or her biometrics into that centralized database. Uhm, in Malawi, this recent push for a more centralized system, based on that it's so new, regulators seem a bit more flexible, I would say. So, that might be actually a chance to, to deploy a system, which could, could, quite, let's say not directly, but quite quickly yield a more foundational purpose without needing to operate based solely on an exempt status. But there are, obviously, I mean we're talking about a country having a Least Developed Country-status, so, very basic factors, network connectivity, electricity and so on, are undermining, obviously, a huge exclusion factor, are undermining that potential in the short to medium-term.

VG:

But then, just to clarify, in Kenya in particular, what you're saying is that, perhaps because they're more advanced, they kind of, they would require to, sort of, they might value, let's say, the existing, how would I call it, reputation of a given individual based on the activity with the Red Cross, but they will still require to get data into their systems, so that they can decide who has an identity. That's what you kinda say.

JM:

More or less. It feels, I mean, that's just my personal opinion, that's not a fact and that is definitely something that might change in the process of my research. But I kind of, and that's why I initially asked about the normative desirability of, of setting up parallel structures in a country, where you already have a certain identity system put in place, the question is whether, uhm, even if the system itself, or the system design allows for, for, for privacy-by-design principles and so on, if you cannot, and I mean that's a whole ethical discussion whether you should anyways, if you cannot, kind of circumvent the state's requirements of, like, putting individuals into the centralized database, then the question is, what added value does such a system actually provide in such a context, which, which makes me wonder, how, even if, especially if you don't have, okay, maybe you might, might make humanitarian assistance more interoperable, more efficient and so on, but it leaves me wondering, which argument, based on the mandate, or based on whichever argument, we would have, or we could use for yielding a foundational character of such as system.

VG:

Well yeah, because again, if we apply typically, uhm, data protection principles and concepts such as minimisation or fair, you know, fair usage and purpose et cetera, I guess, that every, every person then should be able to totally free decide, how much of the data, but also, transaction history perhaps, perhaps sort of the, the situation of a given network [connection interrupted]

Ultimately, generally speaking, it's about the individuals to decide, what they wanna do with the data. But while we shouldn't ever have the hypothesis, or the assumption, that in order to help someone to, you know, be included into financial blablabla, things and et cetera, we are going to discard information to the local governments, now that the acute crisis is over and then they can, you know, we, **we cannot assume that without asking people, it might be difficult to ask that upfront, because you**

**never know what's going to happen.** So, I guess you know, again whatever goes to other direction of Self-Sovereign Identity is to be really extended to data, perhaps in general. Because, in the other end, if someone specifically wants, you know, to take advantage of all the, the "credits", you know, that the individual got by behaving properly with regards to cash transfer and who knows what, and say "look now, you know, I want all the things you learnt **about me to be transferred to this XYZ-authority, so that they are more willing to trust me and include me into other type of programs**", **we should also be able to do it.** Uhm, so yeah, it's a tough one, really, cause you have different ways to look at the, it's a lot of things to take into account, and I don't have a, again, by far not a final answer to this, but, uh...

JM:

That's completely fine, I'm also not seeking final answers, and we have to see, just where the process eventually takes us in the next years and just, as you said, try to do no harm, apply the highest data protection principles possible, and if it doesn't prove to be feasible, than we go back to distribute food and clothing and drugs. Uhm, so yeah, relating to, uhm, this kind of, uhm, because I'm not sure if I understood you correctly. So, you said, if I understood you correctly again, in the aftermath of the crisis, you would normally share certain information with the government anyways. Did I understand you correctly?

VG:

No. In general, we would not share anything.

JM:

Alright, I was already wondering, sorry for the misunderstanding. So, if we, in the context of Kenya and Malawi, if we, like, want to deploy the identity solutions being built here, and the government specifically asks, the Red Cross Society which is operating in these contexts, in order to, in order to yield the acceptance of that system, whether it's for mobile money, whether it's for something else, is specifically asked to, to be to be aware of the individuals and then get all the personally identifiable information to be included on such a system. Uhm, what would the, what would the societies, the Red Cross Societies then be supposed to do?

VG:

Yeah, I mean, if we take this **particular case of Kenya**, I guess, that there are many, many, there are ways by which it **is not a problem at all**, right, to **share with the government**, and then, following normal KYC is just, it's just okay, and there are, we have places, where, as I was saying, we have shared with governments a fair amount of data, because the assessment showed, for that given community, for the kind of information they ask, for the given time we'll gonna do it and with regard to the benefit expected by implementing the programme, you know, to locate, to share information, in our case, **Kenya**, again, most, most of the cases, it's **not going to be an issue to share a list of the beneficiaries**, but of course, you know, minimisation and understanding data flows, so for example, if you, if it goes through, say, a **financial service provider, that is actually a subsidiary of an international group** and that has offices that are going to process data, say, in another country such as Middle East somewhere and you know, then the mobile network operator will also get its share of the data because we need to verify, because, you know, SIM cards already have kinda KYC, so we gonna share that with the mobile operators, and the mobile operator belongs to a large international group too, and these guys will store the data into a centralized database somewhere in Asia and you know, the **data flow process becomes complex**. Even then, even then, there are ways by which you can probably document and assess the different data processes in a way which are not going to, shouldn't, shouldn't make that...are going to let us do it anyway, so that's, that's okay. But at the same time, we may have, in Kenya we might have, been in contact with certain population in certain areas, which are at high risk of some kinds of persecution where it's not okay at all. So, again, I don't think that we can rule out saying "government is asking data, oh my God, we can't do it, so we need to find another way"; in several cases it's going to be fine.

JM:

I see. And now relating to, to sharing data with the service provider potentially, for example in the case of Kenya, for example, Safaricom is a subsidiary of Vodafone, to my understanding, so also an international cooperation and uhm, if we would have assistance, such as the 121-system put in place in, that context and if we somehow I would be able to, based on whichever mandate or other argument, would be able to lobby for, for the government to the acceptance of, of such a system, would you assume, that we could make use of the system for having undocumented people

subscribe to, for example Safaricom's services, with the system; being able to rely on the fact, that for example anti-money-laundering risks and so on would be sufficiently reduced, based on the transparency of the ledger, based on the trust-ability [trustworthiness] of the verifier of the individual' information in the end, which is included on the system, with a verifier, for example, being the Red Cross?

VG:

That still **depends on proportionality** of what we're doing, right? So, cause yeah, if, if, if you can achieve distributing aid and you know, having financial inclusion objectives satisfied and that's the data that, well, first thing is, you know, we tend to say that in data protection, **informed consent doesn't apply in general into humanitarian settings, because the - you don't have a freely obtained informed consent, right, so it's really our duty to assess, things such as proportionality** and so forth. So, you know, if we kind of say, if you have someone who, I guess it totally makes sense for someone to understand that in order to be included into a programme that relies on mobile money, you need to have a mobile phone and because your partners are Safaricom which anyways probably has 60 to 70% of the market shares, you know, that's not the worst thing on earth. But again, you know, and making sure that, and getting some mitigation measures which go through, I guess so kind of contractual clauses, you know, with the providers to say that you know, as you said, Vodafone is a Spanish company, so they get all this information and then, you know, next waves of migration from Africa to Europe and you get from Kenya to Spain and you know, they all of a sudden pull out the list and they say "these guys are actually not refugees because see, last year, they got, you know, so many shillings in aid, so they should be sent back". So, yes, there you obviously gonna have, if that happens, then we obviously failed proportionality and we failed, you know, due diligence and these kinds of things. But we can't account for everything. One thing that's right for lack of better tools is really the law and **this is about the law and lots about complying with some of the local regulation, but also taking advantage of more international body of regulations**. Such as typically the GDPR nowadays. Even though you don't have to comply with it in Kenya, obviously, it might be a good approach to start with.

JM:

That is a very interesting point you're making! Not having a background in law, I would very much like to ask stupid questions relating to that. So, when you say, you could have arguments, or compelling arguments around, uhm, international law, or maybe humanitarian international law in relation to data protection concerns, would there be a specific clause or a specific book of law, you would point out, besides GDPR?

VG:

Yeah, actually, I mean, I suppose I would really advocate for using "Handbook on Data Protection in Humanitarian Action", which was core sourced by our team of data protection guys and also by the Brussels privacy hub. So, yeah, these kind of things make sense, and some other kind of report, that I know, because we didn't write that, but we published a report not so long ago alone go, around the metadata problem in humanitarian settings, so also which deals with the extra risks that we might introduce, when using digital tools and the specifics on looking into metadata **but it all refers to understanding data flows, because that's really what we're talking about here.**

JM:

Thank you for that. Do you have a based on, I feel the variety of topics on various different macro- and meso-levels we've covered, any comments to add so far to our discussion?

VG:

No, so far so good so far so good.

JM:

So far so good, alright great. Uhm, so, you being not only an expert obviously in the operations of ICRC and humanitarian law, but also being an expert in, uhm, the technology itself, would you think that, coming back to, to this, this acceptance of an identity system for KYC-compliance, would you think that the likelihood of a service provider of accepting such a system, which is not disguising personal identifiable information, but rather using the characteristic of distributed trust, uhm, could yield a higher likelihood of acceptance, if the service provider would understand the underlying prospects ,or the underlying characteristics of such a technology, and if so, how would you think could that be communicated?

VG:

It's a good one, because as we were initially talking about the maturity of the technology, when you test it. I guess, this is a follow-up question on that, and you're right. I mean, wherever infrastructures are so damaged or malfunctioning that people don't have IDs bringing that kind of new technology - it's a good point, I never thought really about that - my initial gut feeling is that right now is like it's really **gonna be a challenge**. Yeah. It's really gonna be a challenge. In the case, I'm kind of trying to find an angle. So, you were mentioning the pilots, or the governments in Malawi and Kenya and I can imagine that, yeah, going in and telling even volunteers who participate to the projects, you know, **explaining** to them what this **decentralized system** means and what is the **protocol** which make it more trustable. It kind of remembers me another kind of discussion we had which was around security and people, you know, sort of asking as to why aren't you yet using Microsoft Asia's cloud, or AWS [Amazon Web Services] cloud, and you know, everybody's moving there and from a security standpoint, anyway, they're better than you, cause ICRC, we have our own data centres and most of the things from there and they say "anyway, you know Amazon is much better than your team in cybersecurity", and that's I would say, hopefully true because with the regards to the amounts of money they put for that, I hope they can get something higher. But then, you have the legal aspects. So, you know, we're not under a US arm reach for having to provide information to prosecutors, uhm, and the third one is really about perception. So, there as well, I think that, **one of the good assets for the Red Cross in general, is** precisely the Red Cross and the **reputation and the perception of that, that is being brought with it**. So, I am, again, my sort of feeling would be that really going into the nuts and bolts of explaining why certain, such system, brings trusts, it's going to be tough and, and we got to probably eat our own dog food first and, you know, really demonstrate while likewise all the other things we have done over the decades, you know, that most likely people are not questioning whether the drugs we bring, are legit or good quality. They might argue about some of the food because we source it locally most of the time, like the things that are branded, you know, are fairly trusted and then, perhaps, **perhaps we can learn from the physical world on how to propagate**, uhm, you know, kind **of trust with the new systems**. That being said, even if we would try to embark into explaining the nuts and bolts of the technology, the debate is still raging, right, around the blockchain and you know, public, permissioned, and which one, and you know, why are we keeping investing in Bitcoins, which is consuming so much energy and, and, and. So...

JM:

I think that's actually very interesting point. I haven't thought about using, basically the examples from the analogue world, to maybe make this super abstract concept of, of, let's say, blockchain and Self-Sovereign Identity, decentralized networks and public-permissioned vs. whatever, a bit more tangible to people, who might not have been exposed to a wide range of sophisticated digital tools yet. Because in the end, we need to, in order to convince people in like a context that is less exposed to these digital factors, we, we need to come up with, I think, as you said like a good idea to how, how to make things understandable and relatable in a way. Thank you so much for the interview!

**End of Interview**

## Appendix 13: Anonymized Cover Letter & Informed Consent

### Cover Letter

*Concerning: Research on Financial Inclusion*

Dear XX,

thank you for giving me the opportunity to talk to you!

With your support, I broadly want to find out, if a non-governmental digital ID could and should sufficiently satisfy Know-Your-Customer regulations to allow for inclusion into open-loop mobile-based payment systems. For that, I would like to conduct an approx. 30- to 45-minute-long interview with you. Broadly, I seek answers for following questions:

- Could and should the collection and disclosure of KYC-information in another than a national ID yield financial inclusion into open-loop systems?
- Could and should a humanitarian organisation serve as collector and validator of information for that ID?
- Is setting up such a foundational ID system as a humanitarian agency normatively desirable and which individual exclusion factors need to be considered?

A more detailed interview-guideline will be sent to you before the interview, if desired.

Your contribution is extremely valuable to my research, so you will be, if desired, honourably mentioned as crucial contributor in the final version, which will be sent to you.

Kindly note:

Ideally, the interview will be recorded for exact transcription, but consent for that can be withdrawn any time before and during the interview. You will be asked for consenting again at the beginning of the interview. If consent is given, the records will be kept on a secure database and deleted 30 days after transcription, unless you want to have a copy.

Disclosure of name, position and any other information relating to your identity in the final research document can be freely determined by you.

You have the right to check the written version of conducted interview for desired adjustments, or to give overall disapproval. If you do not respond for over two weeks after receiving the written version of the interview, your approval will be assumed.

Before the interview will be conducted, you will be asked to sign a statement of informed consent, which will be made available to you prior the interview. If you prefer to express your informed consent in verbal form, you will be asked to do so at the beginning of the interview.

If you have any further questions, do not hesitate to reach out to me! Thank you in advance!

With kind regards,

A handwritten signature in blue ink, appearing to read "Jan Meyling", with a long horizontal flourish extending to the right.

Jan Meyling

*NLRC Researcher*

## **Informed Consent Form**

### *Research on Financial Inclusion*

I have read the information disclosed in the cover letter for this research project. I was given the opportunity to ask additional questions. My questions have been answered to my satisfaction. I have had enough time to decide whether or not I want to participate.

I understand that my participation is completely voluntary. I understand that I am free to withdraw at any time, without giving any reason.

I understand that some people have access to my personal details. These people have been mentioned in the cover letter, unless I agree to full disclosure in general. Additionally, Maarten van der Veen, project leader and initiator of 510, has access to my details.

I consent to the use of details relating to me as determined by myself, for the purposes that have been mentioned in the cover letter.

I agree to take part in this research project.

Name of participant: XX

Signature:

Date : XX / XX / XXXX

-----  
With this, I confirm that I have fully informed this participant about the above research project.

Should any information become available in the course of the research project that could potentially influence the participant's consent, I will inform him/her of this in time.

Name of researcher: Jan Meyling

Signature: 

Date: 28 / 01 / 2019

---

## References

510. (2018, August 02). CBA: Cash Based Assistance. Retrieved 10. October 2018, from <https://www.510.global/the-future-of-cash-based-assistance-2/>
- Agboola, A. (2005). *Information and Communication Technology (ICT) in Banking Operations in Nigeria – An Evaluation of Recent Experiences*. Retrieved 03. October 2018, from <http://unpan1.un.org/intradoc/groups/public/documents/aapam/unpan026533.pdf>
- Airtel. (2018). *About Airtel Money*. Retrieved 09. November 2018, from [http://africa.airtel.com/wps/wcm/connect/AfricaRevamp/Malawi/Airtel\\_Money/Home/Personal/About\\_airtel\\_money](http://africa.airtel.com/wps/wcm/connect/AfricaRevamp/Malawi/Airtel_Money/Home/Personal/About_airtel_money)
- Airtel. (2018a). *What is Airtel Money?* Retrieved 09. November 2018, from <http://africa.airtel.com/wps/wcm/connect/AfricaRevamp/Malawi/home/personal/airtel-money/about-airtel-money>
- Airtel. (2018b). *Kutchova*. Retrieved 09. November 2018, from [http://africa.airtel.com/wps/wcm/connect/AfricaRevamp/malawi/airtel\\_money/home/Kutchova](http://africa.airtel.com/wps/wcm/connect/AfricaRevamp/malawi/airtel_money/home/Kutchova)
- Airtel. (2018c). *Terms and Conditions*. Retrieved 22. November 2018, from [http://www.africa.airtel.com/wps/wcm/connect/AfricaRevamp/Malawi/Airtel\\_Money/Home/Personal/Terms-and-Conditions](http://www.africa.airtel.com/wps/wcm/connect/AfricaRevamp/Malawi/Airtel_Money/Home/Personal/Terms-and-Conditions)
- Al Mahdi, M. (2016, August 24). *Digital Financial Inclusion, Scope and Policy*. Retrieved 28. September 2018, from [https://www.itu.int/en/ITU-D/Regional-Presence/ArabStates/Documents/events/2016/DFI/Pre/ITU%20Presentation\\_%20Mustafa.pdf](https://www.itu.int/en/ITU-D/Regional-Presence/ArabStates/Documents/events/2016/DFI/Pre/ITU%20Presentation_%20Mustafa.pdf)
- Alliance for Affordable Internet. (2018). *Mobile Broadband Data Costs. Price of Broadband Data (1GB mobile prepaid) as % of GNI per capita, 2017*. Retrieved 09. November 2018, from <https://a4ai.org/mobile-broadband-pricing-data/>
- Allen, C. (2016, April 25). *The Path to Self-Sovereign Identity*. Retrieved 06. October 2018, from <http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html>
- Arun, T.; Murinde, V. (2010, June 17). *Microfinance Regulation and Social Protection. European Report on Development*. Retrieved June 23, 2018, from

[https://ec.europa.eu/europeaid/sites/devco/files/erd-socpro-financing-arun-murinde-20100617\\_en\\_0.pdf](https://ec.europa.eu/europeaid/sites/devco/files/erd-socpro-financing-arun-murinde-20100617_en_0.pdf)

Baars, D. (2018). *Towards Self-Sovereign Identity using Blockchain Technology*. Retrieved 25. October 2018, from [https://essay.utwente.nl/71274/1/Baars\\_MA\\_BMS.pdf](https://essay.utwente.nl/71274/1/Baars_MA_BMS.pdf)

Bailey, S.; Harvey, P. (2015, March). *Cash transfer programming and the humanitarian system - Background Note for the High Level Panel on Humanitarian Cash Transfers*. Retrieved 10. October 2018, from <https://www.odi.org/sites/odi.org.uk/files/odi-assets/publications-opinion-files/9592.pdf>

Bailey, S.; Harvey, P. (2015a, March). *State of evidence on humanitarian cash transfers - Background Note for the High Level Panel on Humanitarian Cash Transfers*. Retrieved 10. October 2018, from <https://www.odi.org/sites/odi.org.uk/files/odi-assets/publications-opinion-files/9591.pdf>

Bailey, S. (2017, March). *Electronic transfers in humanitarian assistance and uptake of financial services: a synthesis of ELAN case studies*. Retrieved 19. September 2018, from <https://www.odi.org/sites/odi.org.uk/files/resource-documents/11424.pdf>

Bansal, R., Mburu, S. Porteus, D. (2018, August). *Malawi Digital Financial ID Feasibility Assessment*. Retrieved 13. November 2018, from [http://finmark.org.za/wp-content/uploads/2018/10/Malawi-Digital-ID-Report\\_Final-Draft-25-Sept-2018\\_CB.pdf](http://finmark.org.za/wp-content/uploads/2018/10/Malawi-Digital-ID-Report_Final-Draft-25-Sept-2018_CB.pdf)

Barr, M. 2004. *Banking the Poor*. Retrieved from University of Michigan, on June 20, 2018, from [https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1049&context=law\\_econ\\_archive](https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1049&context=law_econ_archive)

Barrow, G. (2012, December 17). *Malawi: Poor Farmers Get Cash Through Mobile Phones*. Retrieved 08. November 2018, from <https://www.wfp.org/stories/malawi-poor-farmers-get-cash-through-mobile-phones>

Bemo, V.; Aberra, D.; Zimmerman, J.; Lanzarone, A.; Lubinski, D. (2017). *Enabling Digital Financial Services In Humanitarian Response: Four Priorities For Improving Payments*. Retrieved 18. September 2018, from

<http://www.cashlearning.org/downloads/enabling-digital-financial-services-in-humanitarian-response-four-priorities-for-improving-payments.pdf>

Bemo, V.; Lubinski, D.; Martin, C.; Tholstrup, S.; Zimmerman, J. (2017a, August 8). CaLP. *How We Built a Global Action Agenda to Enable Digital Payments in Humanitarian Response*. Retrieved 30. October 2018, from <http://www.cashlearning.org/news-and-events/news-and-events/post/469-how-we-built-a-global-action-agenda-to-enable-digital-payments-in-humanitarian-response>

Benson, C.; Goosen, R.; Tellez, C. (2018, July). *Achieving Development and Acceptance of an Open and Inclusive Digital payments Infrastructure - Guidance Note for the G20/GPFI Markets and Payment Systems Subgroup*. Retrieved 30. October 2018, from <http://www.gpfi.org/sites/default/files/documents/BTCA-GPFI-OpenInclusivePayments-.pdf>

Blake, M.; Propson, D.; Monteverde, C. (2016). *Principles on Public-Private Cooperation in Humanitarian Payments*. Retrieved 30. October 2018, from <http://www.cashlearning.org/downloads/weffiprincipleshumanitarianpayments.pdf>

Bold, C., Porteous, D. and Rotman Parker, S. (2012, February). *Social Cash Transfers and Financial Inclusion: evidence from four countries*. Retrieved 04. October 2018, from <https://www.cgap.org/sites/default/files/researches/documents/Focus-Note-Social-Cash-Transfers-and-Financial-Inclusion-Evidence-from-Four-Countries-Feb-2012.pdf>

Bradley, M.; Slim, H. (2013, March). *Principled Humanitarian Action & Ethical Tensions in Multi-Mandate Organizations in Armed Conflict*. Retrieved 30. October 2018, from [https://interagencystandingcommittee.org/system/files/legacy\\_files/Slim,%20WV%20Multi-Mandate%20Ethics%20FinalDraft.pdf](https://interagencystandingcommittee.org/system/files/legacy_files/Slim,%20WV%20Multi-Mandate%20Ethics%20FinalDraft.pdf)

Brand Engel, M.; Scher, J. (2014, December 19). *Four Barriers – and Four Solutions – to Financial Inclusion Through Payment Innovations*. Retrieved 30. October 2018, from <https://nextbillion.net/four-barriers-and-four-solutions-to-financial-inclusion-through-payment-innovations/>

Buckley, R.; Greenacre, J.; Malady, L. (2014, March). *The Regulation of Mobile Money in Malawi - Project Report*. Retrieved 09. November 2018, from

[https://www.clmr.unsw.edu.au/sites/default/files/attached\\_files/the\\_regulation\\_of\\_mobile\\_money\\_in\\_malawi\\_project\\_report.pdf](https://www.clmr.unsw.edu.au/sites/default/files/attached_files/the_regulation_of_mobile_money_in_malawi_project_report.pdf)

Buckley, R., Greenacre L., Malady, L. (2015). The Regulation of Mobile Money in Malawi. *Washington University Global Studies Law Review*, 14 (3). Retrieved 20. December 2018, from [https://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=1536&context=law\\_globalstudies](https://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=1536&context=law_globalstudies)

Cash Learning Partnership [CaLP]. (2011, April 4). *Glossary Of Cash Transfer & Voucher Terminology*. Retrieved 18 November 2018, from [http://www.cashlearning.org/downloads/resources/tools/calp\\_ctp\\_glossary-4-april-2011.pdf](http://www.cashlearning.org/downloads/resources/tools/calp_ctp_glossary-4-april-2011.pdf)

Cash Learning Partnership [CaLP]. 2017. *Glossary Of Cash Transfer Programming (CTP) Terminology*. Retrieved 20. September 2018, from <http://www.cashlearning.org/downloads/calp-updated-glossaryfinal-october-2017.pdf>

Cash Learning Partnership [CaLP]. (ND). *About us*. Retrieved 19. September 2018, from <http://www.cashlearning.org/about-us/overview>

Cash Learning Partnership [CaLP]. (NDa). *E-Payments In Emergency Cash Transfer Programming*. Retrieved 22. September 2018, from [http://www.cashlearning.org/downloads/resources/calp/E-payments\\_in\\_CTP.pdf](http://www.cashlearning.org/downloads/resources/calp/E-payments_in_CTP.pdf)

Campos, N.F.; Coricelli, F. (2010). *How to Maximize the Development Impact Of Social Protection Policies In Africa? The Role of Financial Development*. *European Development Report*. Retrieved February 22, 2018, from <http://erd.eui.eu/media/BackgroundPapers/Campos%20-%20Coricelli%20-%20HOW%20TO%20MAXIMIZE%20THE%20DEVELOPMENT%20IMPACT%20OF%20SOCIAL%20PROTECTION.pdf>

Carant, J.B. 2017. Unheard voices: a critical discourse analysis of the Millennium Development Goals' evolution into the Sustainable Development Goals. *Third World Quarterly*, 38, (1), pp. 16-44. Retrieved 03. February 2018, from <https://doi.org/10.1080/01436597.2016.1166944>

Cavoukian, A. (2009). *Privacy by Design - The 7 Foundational Principles - Implementation and Mapping of Fair Information Practices*. Retrieved 22. October 2018, from [https://iab.org/wp-content/IAB-uploads/2011/03/fred\\_carter.pdf](https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf)

Central Bank of Kenya. (2013). *E-money Regulation, 2013*. Retrieved 20. November 2018, from <https://www.centralbank.go.ke/images/docs/NPS/Regulations%20and%20Guidelines/Regulations%20-%20E-%20Money%20regulations%202013.pdf>

Central Bank of Kenya. (2014). *National Payment System Regulations, 2014*. Retrieved 18. November 2018, from <https://www.centralbank.go.ke/wp-content/uploads/2016/08/NPSRegulations2014.pdf>

Central Bank of Kenya. (2018, March 23). *Banking Circular No. 2 of 2018. Guidance Note on conducting money laundering / Terrorism Financing Assessment*. Retrieved 17. November 2018, from [https://www.centralbank.go.ke/uploads/banking\\_circulars/985992065\\_Banking%20Circular%20No.%202%20of%202018%20-%20Guidance%20Note%20on%20Money%20Laundering%20Risk%20Assessment.pdf](https://www.centralbank.go.ke/uploads/banking_circulars/985992065_Banking%20Circular%20No.%202%20of%202018%20-%20Guidance%20Note%20on%20Money%20Laundering%20Risk%20Assessment.pdf)

Chauwa, A. (2018, August 02). Reserve Bank of Malawi say mobile money is the way to go. Retrieved 08. *Nyasa Times*. Retrieved 09 November 2018, from <https://www.nyasatimes.com/reserve-bank-of-malawi-says-mobile-money-transfers-way-to-go/>

Chifaba, K. (2014, September). *Why not digital? Technology as an interagency tool in the Central African Republic*. Retrieved 17. October 2018, from <https://odihpn.org/magazine/why-not-digital-technology-as-an-interagency-tool-in-the-central-african-republic/>

Chibwana, C.; Kanjo, K. (2015, November). USAID. *Feed The Future Malawi Mobile Money Program*. Retrieved 11. November 2018, from [https://mstarproject.files.wordpress.com/2015/11/mmap\\_ftf\\_final.pdf](https://mstarproject.files.wordpress.com/2015/11/mmap_ftf_final.pdf)

Clark, J.; Gelb, A. (2013, January). Identification for Development: The Biometrics Revolution. *CGD Working Paper 315*. Retrieved 02. November 2018, from [https://www.cgdev.org/sites/default/files/1426862\\_file\\_Biometric\\_ID\\_for\\_Development.pdf](https://www.cgdev.org/sites/default/files/1426862_file_Biometric_ID_for_Development.pdf)

Cohen, L.; Salaun, V. (2017, November 01). *E-cash e-vouchers: The digitalization of the humanitarian aid and logistics*. Retrieved 22. September 2018, from <https://hal.archives-ouvertes.fr/hal-01627418/document>

Communications Authority of Kenya. (2015, August 14). *Kenya Information and Communications (Registration of SIM-cards) Regulations, 2015*. Retrieved 22. November 2018, from [http://kenyalaw.org/kl/fileadmin/pdfdownloads/LegalNotices/163-Kenya\\_Information\\_and\\_Communications\\_Act\\_\\_Registration\\_of\\_Sim-Cards\\_\\_Regulations\\_\\_2015.pdf](http://kenyalaw.org/kl/fileadmin/pdfdownloads/LegalNotices/163-Kenya_Information_and_Communications_Act__Registration_of_Sim-Cards__Regulations__2015.pdf)

Communications Authority of Kenya. (2018). *Fourth Quarter Sector Statistics Report for the Financial Year 2017/2018 (April-June 2018)*. Retrieved 16. November 2018, from <https://ca.go.ke/wp-content/uploads/2018/10/Quarter-Four-sector-statistics-report-for-the-Financial-Year-2017-18.pdf>

Consultative Group to Assist the Poor [CGAP]. (2010). *Update on Regulation of Branchless Banking in Kenya*. Retrieved 16. November 2018, from <http://www.cgap.org/sites/default/files/researches/documents/CGAP-Regulation-of-Branchless-Banking-in-Kenya-Jan-2010.pdf>

Cornish, L. (2016, December 02). *DevExplains: Open vs. closed loop systems for humanitarian payments*. Retrieved 30. October 2018, from <https://www.devex.com/news/devexplains-open-vs-closed-loop-systems-for-humanitarian-payments-89216>

Costa, A.; Ehrbeck, T. (2015). A Market-Building Approach to Financial Inclusion. *Innovations*, 10 (1-2). Retrieved June 20, 2018, from [https://www.mitpressjournals.org/doi/pdf/10.1162/innov\\_a\\_00229](https://www.mitpressjournals.org/doi/pdf/10.1162/innov_a_00229)

Cracknell, D.; Atluri, V.D. (2017, September 04). *Digital Finance in the Field - Progress and Challenges with KYC and Digital ID*. [blog post]. Retrieved 10. December 2018, from <http://www.helix-institute.com/blog/progress-and-challenges-kyc-and-digital-id-venkata-n-atluri-and-david-cracknell-4>

Crosmann, B. (2018, November 21). Fintech MyBucks brings banking to African refugee camp. *American Banker*. Retrieved 22. November 2018, from <https://www.americanbanker.com/news/fintech-mybucks-brings-banking-to-african-refugee-camp>

Dahan, M.; Gelb, A. (2015, July 01). CGDEV. *The Role of Identification in the Post 2015 Development Agenda*. Retrieved 01. November 2018, from [https://www.cgdev.org/sites/default/files/CGD-Essay-Dahan-Gelb-Role-Identification-Post-2015-ID4D\\_0.pdf](https://www.cgdev.org/sites/default/files/CGD-Essay-Dahan-Gelb-Role-Identification-Post-2015-ID4D_0.pdf)

Davis, B.; Handa, S.; Hypher, N.; Winder Rossi, N.; Winters, P.; Yablonski, J. (2016). *From Evidence to Action - The Story of Cash Transfers and Impact Evaluation in Sub-Saharan Africa*. Retrieved 24. October 2018, from <http://www.fao.org/3/a-i5157e.pdf>

Datta, D.; Ejakait, E.; Odak, M. (2008, September). Mobile phone-based cash transfers: lessons from the Kenya emergency response. *Humanitarian Exchange Number 40, September 2008*. Retrieved 17. November 2018, from <https://odihpn.org/wp-content/uploads/2008/10/humanitarianexchange040.pdf>

Decker, C.; Gelb A. (2011). Cash at Your Fingertips: Biometric Technology for Transfers in Developing Countries. *CGD Working Paper 253*. Retrieved 05. October 2018, from [https://www.cgdev.org/sites/default/files/1425165\\_file\\_Gelb\\_Decker\\_biometric\\_FINAL.pdf](https://www.cgdev.org/sites/default/files/1425165_file_Gelb_Decker_biometric_FINAL.pdf)

Demirgüç-Kunt, A.; Klapper, L.; Singer, D.; Ansar, S.; Hess; J. (2018). *The Global Findex Database 2017 - Measuring Financial Inclusion and the Fintech Revolution*. Retrieved 23. June. 2018, from <https://www.openknowledge.worldbank.org/bitstream/handle/10986/29510/9781464812590.pdf?sequence=15&isAllowed=y>.

Demirgüç-Kunt, A., Klapper, L.; Singer, D.; Ansar, S.; Hess, J. (2018a). *The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution*. [Excel File]. Retrieved 14. November 2018, from <https://globalfindex.worldbank.org/sites/globalfindex/files/databank/Global%20Findex%20Database.xlsx>

Denyes, L. (2014, December). *Digital Financial Services in Africa: Beyond the Kenyan Success Story*. Retrieved 17. November 2018, from [http://www.eib.org/attachments/country/study\\_digital\\_financial\\_services\\_in\\_africa\\_en.pdf](http://www.eib.org/attachments/country/study_digital_financial_services_in_africa_en.pdf)

di Catri, S. (2013, August 01). *MMU releases infographic on the Kenyan experience with mobile money*. Retrieved 20. November 2018, from

<https://www.gsma.com/mobilefordevelopment/programme/mobile-money/mmu-releases-infographic-on-the-kenyan-experience-with-mobile-money/>

Donner, J. (2018, December 19). *The difference between digital identity, identification, and ID*. Retrieved 24. December 2018, from <https://medium.com/caribou-digital/the-difference-between-digital-identity-identification-and-id-41580bbb7563>

du Preez, M-L.; Lee, S. (2017). *Determining our focus: A scan of the financial inclusion measurement field*. Retrieved 24. August 2018, from [https://cenfri.org/wp-content/uploads/2017/05/Measurement-framework-note-2-Determining-our-focus\\_i2i\\_2017\\_WEB.pdf](https://cenfri.org/wp-content/uploads/2017/05/Measurement-framework-note-2-Determining-our-focus_i2i_2017_WEB.pdf)

Dubus, A.; van Hove, L. (2017, September 21). *M-PESA and financial inclusion in Kenya: of paying comes saving?* Retrieved 21. February 2019, from <https://hal.archives-ouvertes.fr/hal-01591200/document>

Dumas, T.; Frisetti, A.; Welcome Radice, H. (2017, September). *Harnessing Digital Technology For Cash Transfer Programming In The Ebola Response - Lessons Learned from USAID/Office of Food for Peace Partners' West Africa Ebola Responses (2015–2016)*. Retrieved 28. October 2018, from <http://www.cashlearning.org/downloads/calp-ebola-case-study-web.pdf>

El-Zoghbi, M. (2016, December 05). *Financial Inclusion - Can Reduce Inequality and Bring Peace*. [blog post]. Retrieved 23. June 2018, from <http://www.cgap.org/blog/financial-inclusion-can-reduce-inequality-and-bring-peace>

El-Zoghbi, M. (2017, May 17). *Bridging the Humanitarian and Development Divide*. [blog post]. Retrieved 24. June 2018, from <https://www.cgap.org/blog/bridging-humanitarian-and-development-divide>

El-Zoghbi, M.; Chehade, N.; McConaghy, P.; Soursourian, M. (2017). *The Role of Financial Services in Humanitarian Crises*. Retrieved 18. November 2018, from [https://www.cgap.org/sites/default/files/researches/documents/Forum-The-Role-of-Financial-Services-in-Humanitarian-Crises\\_1.pdf](https://www.cgap.org/sites/default/files/researches/documents/Forum-The-Role-of-Financial-Services-in-Humanitarian-Crises_1.pdf)

Evans, D.S.; Pirchio, A. (2015). *An Empirical Examination of Why Mobile Money Schemes Ignite in Some Developing Countries but Flounder in Most*. *Coase-Sandor Working Paper Series in Law and Economics No. 723*. Retrieved 16. November 2018, from

[https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=2413&context=law\\_and\\_economics](https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=2413&context=law_and_economics)

Fabre, C.; Aggiss, R. (2017). *Cash-based response*. Retrieved 30. October 2018, from <https://www.oecd.org/development/humanitarian-donors/docs/cashbasedresponse.pdf>

Financial Action Task Force [FATF]. (2012-2018). *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation - The FATF Recommendations*. Retrieved 26. October 2018, from <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf>

Financial Action Task Force [FATF]. (2019). *Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG)*. Retrieved January 12 2019, from <http://www.fatf-gafi.org/pages/members/easternandsouthernafricaanti-moneylaunderinggroupesaamlg.html>

Fearon, J.D. (1999, November 03). *What Is Identity (As We Now Use the Word)?* Retrieved 02. November 2018, from <https://web.stanford.edu/group/fearon-research/cgi-bin/wordpress/wp-content/uploads/2013/10/What-is-Identity-as-we-now-use-the-word-.pdf>

Financial Inclusion Insights. (2018). *Kenya*. Retrieved 17. November 2018, from <http://finclusion.org/country/africa/kenya.html>

Financial Inclusion Insights. (2018a, June). *Kenya Wave 5 Report Fifth Annual FII Tracker Survey*. Retrieved 15. November 2018, from [http://finclusion.org/uploads/file/kenya-wave-5-report\\_final.pdf](http://finclusion.org/uploads/file/kenya-wave-5-report_final.pdf)

Ford, E. (2017). The Potential of Digital Cash Transfers to Strengthen the Link Between Humanitarian Assistance and Social Protection. *Bath Papers in International Development and Wellbeing (54/2017)*. Retrieved 26. September 2018, from <http://www.bath.ac.uk/cds/publications/bdp54.pdf>

Food and Agriculture Organisation [FAO]. 2010. *The State of Food Insecurity in the World. Addressing food insecurity in protracted crises*. Retrieved 04. October 2018, from <http://www.fao.org/3/a-i1683e.pdf>

Frydrych, J.; Wasunna, N. (2017, September). *Person-to-government (P2G) payment digitisation: Lessons from Kenya*. Retrieved 19 November 2018, from [https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/09/P2G\\_Report\\_Final.pdf](https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/09/P2G_Report_Final.pdf)

Galetta, A. (2012). *Mastering the Semi-Structured Interview and Beyond: From Research Design to Analysis and Publication*. New York: NYU Press. Retrieved 16. October 2018, from amazon.com

Gardeva, A.; Rhyne, E. (2011, July). Opportunities and Obstacles to Financial Inclusion. *Center for Financial Inclusion Publication 12*. [blog post] Retrieved June 19, 2018, from [https://centerforfinancialinclusionblog.files.wordpress.com/2011/12/opportunities-and-obstacles-to-financial-inclusion\\_110708\\_final.pdf](https://centerforfinancialinclusionblog.files.wordpress.com/2011/12/opportunities-and-obstacles-to-financial-inclusion_110708_final.pdf)

Garcia, M.; Moore, C.M.T. (2011). *The Cash Dividend - The Rise of Cash Transfer Programs in Sub-Saharan Africa*. Retrieved 19. September 2018, from <http://documents.worldbank.org/curated/en/435291468006027351/pdf/672080PUB0EPI0020Box367844B09953137.pdf>

Gemalto. (2018, September 18). *Gemalto and R3 pilot blockchain technology to put users in control of their Digital ID*. Retrieved 25. October 2018, from <https://www.gemalto.com/press/pages/gemalto-and-r3-pilot-blockchain-technology-to-put-users-in-control-of-their-digital-id.aspx>

George, D.; Hatt, T.; Sharma, A.; Arese Lucini, B.; Dewar, C.; Evans D.; Rizzato, F.; James H.; Stryjak, J.; Gillet, J.; Bahia, K.; Bains K.; Okeleke; K.; Giles, M.; Little M.; Iji, M.; Corral San Martin, M.; Rogers, M., Meloán, M.; Afonso, N.; Iacopino, P.; Castells, P.; Wyrzykowski, R.; Kechiche, S.; Pedros, X. 2016. (2016, October). *Global mobile trends*. Retrieved 22. October 2018, from <https://www.gsmaintelligence.com/research/?file=357f1541c77358e61787fac35259dc92&download>

Gigler, B-S. (2015). *Development as Freedom in a Digital Age - Experiences of the Rural Poor in Bolivia*. Retrieved 17. September 2018, from <https://openknowledge.worldbank.org/handle/10986/21631>

Gillet, J. (2014, May 22). *Measuring mobile penetration*. Retrieved 22. October 2018, from <https://www.gsmaintelligence.com/research/2014/05/measuring-mobile-penetration/430/>

Given, L. (2007). Marginalized Populations. *The SAGE Encyclopedia of Qualitative Research Methods*. Retrieved 18. September 2018, from <http://methods.sagepub.com/reference/sage-encyc-qualitative-research-methods/n252.xml>

Global Innovation Exchange. (2016). *Principles for Digital Payments in Humanitarian Response*. Retrieved 05. October 2018, from [https://static.globalinnovationexchange.org/s3fs-public/asset/document/Digital-Payments-Humanitarian-Principles\\_0.pdf?BvMH5s\\_7H6psd5btsC7ZIS3v8KBx4Xdj](https://static.globalinnovationexchange.org/s3fs-public/asset/document/Digital-Payments-Humanitarian-Principles_0.pdf?BvMH5s_7H6psd5btsC7ZIS3v8KBx4Xdj)

Grossman, J.; Nelson, P.K. (2014). *Digital Finance for Development - A handbook for USAID Staff*. Retrieved 23. September 2018, from [https://www.fhi360.org/sites/default/files/media/documents/Digital\\_Finance\\_Handbook\\_-\\_Complete\\_Vesion\\_-\\_v11.pdf](https://www.fhi360.org/sites/default/files/media/documents/Digital_Finance_Handbook_-_Complete_Vesion_-_v11.pdf)

Global System for Mobile Communications Association [GSMA]. (2017, May). *Landscape Report: Mobile Money, Humanitarian Cash Transfers and Displaced Populations*. Retrieved 27. July 2018, from [https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/05/Mobile\\_Money\\_Humanitarian\\_Cash\\_Transfers.pdf](https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/05/Mobile_Money_Humanitarian_Cash_Transfers.pdf)

Global System for Mobile Communications Association [GSMA]. (2017a). *The Mobile Economy - Sub-Saharan Africa 2017*. Retrieved 22. October 2018, from <https://www.gsmaintelligence.com/research/?file=7bf3592e6d750144e58d9dcfac6adfab&download>

Global System for Mobile Communications Association [GSMA]. (2017b). *Refugees and Identity: Considerations for mobile-enabled registration and aid delivery*. Retrieved 25. October 2018, from <https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/06/Refugees-and-Identity.pdf>

Global System for Mobile Communications Association [GSMA]. (2017c). *State of the Industry Report on Mobile Money: Decade Edition 2006–2016*. Retrieved 16. November 2018, from <https://www.gsma.com/mobilefordevelopment/wp->

content/uploads/2017/03/GSMA\_State-of-the-Industry-Report-on-Mobile-Money\_2016.pdf

Global System for Mobile Communications Association [GSMA]. (2018, September). *Distributed Ledger Technology, Blockchains and Identity - A Regulatory Overview*. Retrieved 10. December 2018, from <https://www.gsma.com/identity/wp-content/uploads/2018/09/Distributed-Ledger-Technology-Blockchains-and-Identity-20180907ii.pdf>

Government of Malawi. 2016. *Communications Act, 2016*. Retrieved 09. November 2018, from <http://www.macra.org.mw/wp-content/uploads/2014/07/Communications-Act-2016.pdf>

Government of Malawi. (2017, February 16). *Financial Crimes Act, 2016*. Retrieved 10. November 2018, from <https://www.rbm.mw/Home/GetContentFile/?ContentID=26313>

Government of Malawi. (2017a, March 30). *Government of Malawi Payments Road Map: A Five-Year Plan to Digitize Government Payments in Malawi*. Retrieved 10. November 2018, from <https://www.uncdf.org/article/2413/government-of-malawi-payments-roadmap>

Haahr, M. (2017). *Hack the Future of Development Aid*. Retrieved February 22, 2018, from <http://sustainiaworld.com/wp-content/uploads/2017/12/hack-the-future.pdf>

Hansen, L. (2018, August). *Finance for Refugees: the state of play*. Retrieved 22. November 2018, from [http://www.inclusivefinanceplatform.nl/documents/Documents/npm%20report\\_finance-for-refugees\\_the%20state%20of%20play.pdf](http://www.inclusivefinanceplatform.nl/documents/Documents/npm%20report_finance-for-refugees_the%20state%20of%20play.pdf)

Hemsteede, R. (2018, February 15). *From manual to digital: First hand insight into Malawi's Social Cash Transfer*. [blog post]. Retrieved 13. November 2018, from <http://socialprotection.org/learn/blog/manual-digital-first-hand-insight-malawi%E2%80%99s-social-cash-transfer>

Hodges, A.; White, P.; Greenslade, M. (2011). *Guidance for DFID country offices on measuring and maximising value for money in cash transfer programmes*. Retrieved 26. September 2018, from <http://siteresources.worldbank.org/INTPENSIONS/Resources/395443->

1142535808399/2329423-1350588199143/8898265-  
1350588563122/guid\_dfid\_cnty\_offs\_meas\_max\_vfm\_csh\_trsf\_r\_progs.pdf

Holzmann, R.; Jørgensen, S. (2001). *Social Risk Management: A New Conceptual Framework for Social Protection, and Beyond*. Retrieved 29. October 2018, from <https://doi.org/10.1023/A:1011247814590>

Huduma Kenya. (2016). *Huduma Card*. Retrieved 15. November 2018, from <https://www.hudumakenya.go.ke/card.html>

ID2020 Alliance. (2017). *Committed to improving lives through digital identity*. Retrieved 20. August 2018, from [https://static1.squarespace.com/static/578015396a4963f7d4413498/t/5b4f6273575d1feb288ae0a5/1531929204374/ID2020%2BAlliance%2BDoc\\_UPDATED.pdf](https://static1.squarespace.com/static/578015396a4963f7d4413498/t/5b4f6273575d1feb288ae0a5/1531929204374/ID2020%2BAlliance%2BDoc_UPDATED.pdf)

IGI Global. (2018). *What is Information and Communication Technology (ICT)*. Retrieved 18. September 2018, from <https://www.igi-global.com/dictionary/information-and-communication-technology-ict/14316>

Infobip. (2018). *Mobile Phone Penetration*. Retrieved 21. October 2018, from <https://www.infobip.com/en/glossary/mobile-phone-penetration>

International Rescue Committee. (2016, May). *Untapped Humanitarian Demand: A Business Case for Expanding Digital Financial Services*. Retrieved 23. October 2018, from <http://www.cashlearning.org/downloads/untappedhumanitariandemand-abusinesscaseforexpandingdfs.pdf>

International Telecommunication Union [ITU]. (2017). *ICT Development Index*. Retrieved 10. November 2018, from <https://www.itu.int/net4/itu-d/idi/2017/index.html>

International Telecommunication Union [ITU]. (2017a). *Measuring the Information Society Report. Volume 2. ICT Country profiles*. Retrieved 10. November 2018, from [https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2017/MISR2017\\_Volume2.pdf](https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2017/MISR2017_Volume2.pdf)

International Telecommunication Union [ITU]. (2018). *ITU Key 2005-2017 ICT data*. [Excel file]. Retrieved 22. October 2018, from [https://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2017/ITU\\_Key\\_2005-2017\\_ICT\\_data.xls](https://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2017/ITU_Key_2005-2017_ICT_data.xls)

International Telecommunication Union [ITU]. (2019). *The ICT Development Index (IDI): conceptual framework and methodology*. Retrieved 02. January 2019, from <https://www.itu.int/en/ITU-D/Statistics/Pages/publications/mis2017/methodology.aspx>

International Telecommunication Union [ITU] and Universal Postal Union. 2017. *Digital Financial Services Glossary*. Retrieved 30. October 2018, from [http://www.upu.int/uploads/tx\\_sbdownloader/digitalFinancialServicesGlossaryEn.pdf](http://www.upu.int/uploads/tx_sbdownloader/digitalFinancialServicesGlossaryEn.pdf)

Investopedia. (N.D). *Due Diligence*. Retrieved 05. October 2018, from <https://www.investopedia.com/terms/d/duediligence.asp>

Jacobsen, K. 2017. On humanitarian refugee biometrics and new forms of intervention. *Journal of Intervention and Statebuilding*, 11, (4), 529-551. Retrieved 15. October 2018, from <https://doi.org/10.1080/17502977.2017.1347856>

Juden, M.; Pisa, M. (2017, July). Blockchain and Economic Development: Hype vs. Reality. *CGD Policy Paper 107*. Retrieved 04. April 2018, from [https://www.cgdev.org/sites/default/files/blockchain-and-economic-development-hype-vs-reality\\_0.pdf](https://www.cgdev.org/sites/default/files/blockchain-and-economic-development-hype-vs-reality_0.pdf)

Julliard, H.; Sloane, E. (2016, February). *Revised Pre-crisis market analysis*. Retrieved 21. September 2018, from [https://www.emma-toolkit.org/sites/default/files/bundle/PMCA\\_FINAL\\_WEB.pdf](https://www.emma-toolkit.org/sites/default/files/bundle/PMCA_FINAL_WEB.pdf)

Karimi, M. (2017, November 01). *Kenya Government and WFP Disburse Relief Cash to Drought Stricken Families*. Retrieved 06. October 2018, from <https://insight.wfp.org/kenya-government-and-wfp-disburse-relief-cash-to-drought-stricken-families-7dc1d790238d>

Kita, S. (2014, May). *Is cash transfer a better devil than food aid? A study of Malawi's use of cash transfer as a response tool to food insecurity in 2012/2013 and 2013/2014*. Retrieved 10. November 2018, from <https://www.unocha.org/sites/dms/Documents/Kita%20-%20Is%20cash%20transfer%20a%20better%20devil%20than%20food%20aid%20in%20Malawi.pdf>

Koles, B.; Nagy, P. (2014, August). The digital transformation of human identity. Retrieved 01. November 2018, from

[https://www.researchgate.net/publication/268387603\\_The\\_digital\\_transformation\\_of\\_human\\_identity](https://www.researchgate.net/publication/268387603_The_digital_transformation_of_human_identity)

Kondakhchyan, A.; Sagmeister, E.; Seilern, M; Andrawes, L.; Nzimbi, A.; Harvey, P.; Pavanello, S. 2018. *Kenya case study - Improving user journeys for humanitarian cash transfers*. Retrieved 14. November 2018, from [https://reliefweb.int/sites/reliefweb.int/files/resources/User\\_Journeys\\_Kenya\\_Report\\_2018.pdf](https://reliefweb.int/sites/reliefweb.int/files/resources/User_Journeys_Kenya_Report_2018.pdf)

Kopinak, J.K. (2013, March 10). *Humanitarian Aid: Are Effectiveness and Sustainability Impossible Dreams?* Retrieved 30. October 2018, from <https://sites.tufts.edu/jha/archives/1935>

Lepoutre, J.; Oguntoye, A. (2018, June). The (non-)emergence of mobile money systems in Sub-Saharan Africa: A comparative multilevel perspective of Kenya and Nigeria. *Technological Forecasting and Social Change*, (131), pp. 262-275. Retrieved 14. November 2018, from <https://doi.org/10.1016/j.techfore.2017.11.010>

Levin, A.; Varghese, A.; Chibba, M. (2015, April). *Know Your Customer Standards and Privacy Recommendations for Cash Transfers*. Retrieved 18. October 2018, from <http://www.cashlearning.org/downloads/erc-know-your-customer-web.pdf>

Lewis, A. (2017, May 17). *A gentle introduction to self-sovereign identity*. Retrieved 12. December 2018, from <https://bitsonblocks.net/2017/05/17/gentle-introduction-self-sovereign-identity/>

Ligomeka, B. (2017, December 06). Malawi National IDs: Great milestone with transformative promise. *Malawi24*. Retrieved 20. November 2018, from <https://malawi24.com/2017/12/06/malawi-national-ids-great-milestone-transformative-promise/>

Longley, D.; Sporny, D. (2018, April 03). *Identity Credentials 1.0. Draft Community Group Report*. Retrieved 25. October 2018, from <https://opencreds.org/specs/source/identity-credentials/>

Madise, S. (2014, November 27). Payment Systems and Mobile Money in Malawi: Towards Financial Inclusion and Financial Integrity. *ANULJ 2014* (2), 2, pp. 71-96. Retrieved 08. November 2018, from <https://ssrn.com/abstract=2531319>.

Malenga, B. (2017, November 10). Only Malawians will receive IDs – NRB. *Malawi24*. Retrieved 12. November 2018, from <https://malawi24.com/2017/11/10/malawians-will-receive-ids-nrb/>

Malik, T.; Mittal, A. (2017). *Technical Standards for Digital Identity Systems for Digital Identity*. Retrieved 17. October 2018, from <http://pubdocs.worldbank.org/en/579151515518705630/ID4D-Technical-Standards-for-Digital-Identity.pdf>

Mas, I.; Radcliffe, D. 2011. Bill & Melinda Gates Foundation. Scaling mobile money. *Journal of Payments Strategy & Systems*, 5, (3.) Retrieved 16. November 2018, from [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1681245](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1681245)

Mchulu, A. (2018, October 04). *Financial inclusion powered by mobile money*. Retrieved 08. November 2018, from <https://mwnation.com/financial-inclusion-powered-by-mobile-money/>

Metcalfe-Hough, V.; Poole, L.; Bailey, S.; Belanger, J. (2018, June). *Grand Bargain annual independent report 2018*. Retrieved 12. December 2018, from <https://www.odi.org/sites/odi.org.uk/files/resource-documents/12253.pdf>

Michael-Phiri, M. (2017, June 11). National ID program in Malawi raises questions, fears. New national ID project ahead of 2109 elections dogged by questions of incompetence, racism, corruption. *Anadolu Agency*. Retrieved 14. November 2018, from <https://www.aa.com.tr/en/africa/national-id-program-in-malawi-raises-questions-fears/839438>

Minges, M. (2012). Part II: Statistical Appendix. *Key Trends in the Development of the Mobile Sector*. Retrieved 22. October 2018, from <https://siteresources.worldbank.org/EXTINFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/Resources/IC4D-2012-Appendix-1.pdf>

Mita, C. (2015, May 27). *Cash and Voucher Solutions to Hunger in Malawi*. Retrieved 08. November 2018, from <https://www.wfp.org/stories/cash-and-voucher-solutions-hunger>

Morduch, J. (1999, August). Between the State and the Market: Can Informal Insurance Patch the Safety Net? *The World Bank research observer*. – 14, (2), pp. 187-207. Retrieved 25. March 2018, from

<http://documents.worldbank.org/curated/en/487051468337871759/Between-the-state-and-the-market-can-informal-insurance-patch-the-safety-net>

Msiska, R.; Ghello, T. (2018, May 10). *Refugee camp in Malawi gets banking services*. Retrieved 10. November 2018, from <http://www.unhcr.org/afr/news/stories/2018/5/5af45b034/refugee-camp-in-malawi-gets-banking-services.html>

Muthiora, B. (2015, January). *Enabling Mobile Money Policies in Kenya - Fostering a Digital Financial Revolution*. Retrieved 20. November 2018, from [https://www.itu.int/en/ITU-T/focusgroups/dfs/Documents/2015\\_MMU\\_Enabling-Mobile-Money-Policies-in-Kenya.pdf](https://www.itu.int/en/ITU-T/focusgroups/dfs/Documents/2015_MMU_Enabling-Mobile-Money-Policies-in-Kenya.pdf)

Muthuri, R.; Monyango, F.; Karanja, W. (2018). *Biometric Technology, Elections, and Privacy Investigating Privacy Implications of Biometric Voter Registration in Kenya's 2017 Election Process*. Retrieved 19. November 2018, from <https://blog.cipit.org/wp-content/uploads/2018/05/Biometrics-Privacy-Report-by-CIPIT.pdf>

Ndung'u, N. (2017, July). M-Pesa – a success story of digital financial inclusion. *Practitioner's Insight*. Retrieved 14. November 2018, from <https://www.bsg.ox.ac.uk/sites/default/files/2018-06/2017-07-M-Pesa-Practitioners-Insight.pdf>

Neil, S. (2010). Degrees of Digital Division: Reconsidering Digital Inequalities and Contemporary Higher Education. *RUSC. Universities and Knowledge Society Journal*, (7), 1, pp. 33-42. Retrieved 15. August 2018, from <http://www.redalyc.org/articulo.oa?id=78012953011>

Norwegian Refugee Council. (2017, November). *Recognising Nairobi's Refugees - The Challenges and Significance of Documentation Proving Identity and Status*. Retrieved 22. November 2018, from [http://hrp.law.harvard.edu/wp-content/uploads/2017/11/recognising-nairobis-refugees\\_nrc\\_ihrc\\_november2017\\_embargoed.pdf](http://hrp.law.harvard.edu/wp-content/uploads/2017/11/recognising-nairobis-refugees_nrc_ihrc_november2017_embargoed.pdf)

Nyst, C.; Pannifer, S.; Whitley, E.; Makin, P. (2016, June 08). *Digital Identity: Issue Analysis*. Retrieved 18. October 2018, from [https://www.chyp.com/wp-content/uploads/2016/07/PRJ.1578-Digital-Identity-Issue-Analysis-Report-v1\\_6-1.pdf](https://www.chyp.com/wp-content/uploads/2016/07/PRJ.1578-Digital-Identity-Issue-Analysis-Report-v1_6-1.pdf)

Overseas Development Institute [ODI]. (2015, September). *Doing cash differently - How cash transfers can transform humanitarian aid - Report of the High-Level Panel on Humanitarian Cash Transfers*. Retrieved 19. September 2018, from <https://www.odi.org/sites/odi.org.uk/files/odi-assets/publications-opinion-files/9828.pdf>

Ogola, R. (2012, December 13). *Mobile Cash For Emergency Response In Kenya*. Retrieved 06. October 2018, from <https://www.wfp.org/stories/mobile-cash-emergency-response>

Organisation for Economic Co-Operation and Development [OECD]. (2001). *Understanding the Digital Divide*. Retrieved 04. October 2018, from <https://www.oecd.org/sti/1888451.pdf>

Organisation for Economic Co-Operation and Development [OECD]. (2017). *Food Security— Mobile Money Accelerator Program (MMAAP). 2017 Aid for Trade - Case Story Template*. Retrieved 06. October 2018, from [https://www.oecd.org/aidfortrade/casestories/casestories-2017/CS-147-USAID-Food-Security-Mobile-Money-Accelerator-Program-\(MMAAP\).pdf](https://www.oecd.org/aidfortrade/casestories/casestories-2017/CS-147-USAID-Food-Security-Mobile-Money-Accelerator-Program-(MMAAP).pdf)

Osafo-Kwaako, P.; Singer, M.; White, O.; Zouaoui, Y.; (2018, March). *Mobile money in emerging markets: The business case for financial inclusion*. Retrieved 30. October 2018, from <https://www.mckinsey.com/~/media/McKinsey/Industries/Financial%20Services/Our%20Insights/Mobile%20money%20in%20emerging%20markets%20The%20business%20case%20for%20financial%20inclusion/Mobile-money-in-emerging-markets.ashx>

Oxfam. (2016). *Innovative Electronic Cash Transfer Programme for Emergencies. An Oxfam-Visa Case Study in the Philippines*. Retrieved 22. September 2018, from <https://reliefweb.int/sites/reliefweb.int/files/resources/oxfam2.pdf>

Park, C-Y.; Mercado, R. V. (2015, January). *Financial Inclusion, Poverty, and Income Inequality in Developing Asia. ADB economics working paper series No. 426*. Retrieved 23. June 2018, from <https://www.adb.org/sites/default/files/publication/153143/ewp-426.pdf>

Parker, S. R. (2010, November 29). *Social Protection and Financial Inclusion*. [blog post]. Retrieved 29. October 2018, from <http://www.cgap.org/blog/social-protection-and-financial-inclusion>

Pilkington, M. (2015, September 2018). *Blockchain Technology: Principles and Applications*. Retrieved 22 January 2018, from [https://papers.ssrn.com/sol3/Papers.cfm?abstract\\_id=2662660](https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2662660)

Pirlot de Corbion, A.; Hosein, G.; Fisher, T.; Geraghty, E.; Callander, A.; Bouffet, T.; Quintanilla, J.; Marelli, M.; Pelucchi, S. (2018, October). *The Humanitarian Metadata Problem: "Doing No Harm" in the Digital Era*. Retrieved 12. December 2018, from <https://privacyinternational.org/sites/default/files/2018-12/The%20Humanitarian%20Metadata%20Problem%20-%20Doing%20No%20Harm%20in%20the%20Digital%20Era.pdf>

Price, G. (2008). The benefits and drawbacks of using electronic identities. *Information Security Technical Report*, 13, (2), pp. 95-103. Retrieved 16. October 2018, from <https://doi.org/10.1016/j.istr.2008.07.002>

Privacy International. (2018, December 11). *Companies must "do no harm" in the humanitarian sector*. [blog post]. Retrieved 14. December 2018, from <https://privacyinternational.org/blog/2536/companies-must-do-no-harm-humanitarian-sector>

Republic of Kenya. (2006). *Refugees Act, 2006*. Retrieved 22. November 2018, from [http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/RefugeeAct\\_No13of2006.pdf](http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/RefugeeAct_No13of2006.pdf)

Republic of Kenya. (2009). *Proceeds of Crime and Anti-Money Laundering Act, 2009*. Retrieved 17. November 2018, from <http://www.kenyalaw.org/lex//actview.xql?actid=No.%209%20of%202009>

Republic of Kenya. (2013). *Proceeds of Crime and Anti-Money Laundering Regulations, 2013*. Retrieved 17. November 2018, from [http://kenyalaw.org/lex/rest//db/kenyalex/Kenya/Legislation/English/Acts%20and%20Regulations/P/Proceeds%20of%20Crime%20and%20Anti-Money%20Laundering%20Act%20Cap.%2059B%20-%20No.%209%20of%202009/subsidiary%20legislation/docs/Proceeds\\_Of\\_Crime\\_And\\_Anti\\_Money\\_Laundering\\_Act\\_Subsidiary.pdf](http://kenyalaw.org/lex/rest//db/kenyalex/Kenya/Legislation/English/Acts%20and%20Regulations/P/Proceeds%20of%20Crime%20and%20Anti-Money%20Laundering%20Act%20Cap.%2059B%20-%20No.%209%20of%202009/subsidiary%20legislation/docs/Proceeds_Of_Crime_And_Anti_Money_Laundering_Act_Subsidiary.pdf)

Republic of Kenya. (2013a). *Second Medium Term Plan, 2013 – 2017*. Retrieved 15. November 2018, from [http://www.issueab.org/requester/sdgs/id/21901?\\_ga=2.44671844.1585118509.1509650669-1038809230.1509650669](http://www.issueab.org/requester/sdgs/id/21901?_ga=2.44671844.1585118509.1509650669-1038809230.1509650669)

Republic of Kenya. 2018. *Statute Law (Miscellaneous Amendments) Bill, 2018*. Retrieved 17. November 2018, from <http://kenyalaw.org/kl/fileadmin/pdfdownloads/bills/2018/StatuteLawMiscellaneousAmendmentsBill2018.pdf>

Republic of Kenya. (2018a). *Data Protection Act, 2018*. Retrieved 22. November 2018, from <http://www.ict.go.ke/wp-content/uploads/2016/04/Kenya-Data-Protection-Bill-2018-14-08-2018.pdf>

Reserve Bank of India. (2017, March 20). *Master Directions on Issuance and Operation of Prepaid Payment Instruments in India*. Retrieved 01. November 2018, from [https://www.rbi.org.in/Scripts/bs\\_viewcontent.aspx?Id=3325](https://www.rbi.org.in/Scripts/bs_viewcontent.aspx?Id=3325)

Reserve Bank of Malawi. (2006). *Money Laundering Proceeds of Serious Crime and Terrorist Financial Act, 2006*. Retrieved 10. November 2018, from <https://www.rbm.mw/Home/GetContentFile/?ContentID=3753>

Reserve Bank of Malawi. (2011). *Guidelines for Mobile Payment Systems*. Retrieved 08. November 2018, from <https://www.rbm.mw/PaymentSystems/GetContentFile/?ContentID=3556>

Reserve Bank of Malawi. (2018, June). *Monthly National Payments System Report*. Retrieved 09. November 2018, from <https://www.rbm.mw/PaymentSystems/GetContentFile/?ContentID=26225>

Rosenstein, M. (2012, February 16). *What is "Sovereign Source Authority"?* Retrieved 02. November 2018, from <https://www.moxytongue.com/2012/02/what-is-sovereign-source-authority.html>

Rouse, M. (2016). Personally Identifiable Information (PII). GDPR compliance requirements for CRM managers. Retrieved 03. December 2018, from <https://searchfinancialsecurity.techtarget.com/definition/personally-identifiable-information>

Sabates-Wheeler, R.; Devereux, S. 2010. *Cash Transfers and High Food Prices: Explaining Outcomes on Ethiopia's Productive Safety Net Programme*. Retrieved 26. September 2018, from <https://europa.eu/capacity4dev/file/17609/download?token=x8x-lv0C>

Safaricom. 2012. *Customer Identification Procedure*. Retrieved 15. November 2018, from <https://safaricom.amlawareness.com/documents/Customer%20Identification%20Procedure.pdf>

Saxby, S. 2013. The 2013 CLSR-LSPI seminar on electronic identity: The global challenge – Presented at the 8th International Conference on Legal, Security and Privacy issues in IT Law (LSPI) November 11–15, 2013, Tilleke & Gibbins International Ltd., Bangkok, Thailand. *Computer Law & Security Review*, 30, (2), April 2014, pp. 112-125. Retrieved 23. October 2018, from <https://doi.org/10.1016/j.clsr.2014.01.007>

Schlatt, V.; Schweitzer, A.; Urbach, N.; Fridgen, G. (2016, December). Blockchain: Grundlagen, Anwendungen und Potenziale. [Blockchain: Basics, Applications and Potentials]. *Fraunhofer FIT, December 2016*, pp. 1-54. Retrieved 22 January 2018, from <http://www.fim-rc.de/Paperbibliothek/Veroeffentlicht/642/wi-642.pdf>

Schmitz Guinote, F. 2018, June 21). *A humanitarian-development nexus that works*. [blog post]. Retrieved 10. November 2018, from <http://blogs.icrc.org/law-and-policy/2018/06/21/humanitarian-development-nexus-that-works/>

Scott, R. (2014, October). Imagining More Effective Humanitarian Aid - A Donor Perspective. *OECD Development Co-Operation Working Paper 18*. Retrieved 30. October 2018, from [https://www.oecd.org/dac/Imagining%20More%20Effective%20Humanitarian%20Aid\\_October%202014.pdf](https://www.oecd.org/dac/Imagining%20More%20Effective%20Humanitarian%20Aid_October%202014.pdf)

Scott, B. (2016, February 10). *How Can Cryptocurrency and Blockchain Technology Play a Role in Building Social and Solidarity Finance?* Retrieved 25. February 2018, from <http://www.unrisd.org/80256B3C005BCCF9/search/196AEF663B617144C1257F550057887C?OpenDocument>

Simister, N. (2015). *Outputs, Outcomes and Impact*. Retrieved 26. October 2018, from <https://www.intrac.org/wpcms/wp-content/uploads/2016/06/Monitoring-and-Evaluation-Series-Outcomes-Outputs-and-Impact-7.pdf>

Smith, G.; McCormack, R.; Jacobs, A.; Chopra, A.; Vir Gupta, A.; Abell, A. (2018, February). *The State of The World's Cash Report: Cash Transfer Programming in Humanitarian Aid*. Retrieved October 03. 2018, from <http://www.cashlearning.org/downloads/calp-sowc-report-web.pdf>

Sossouvi, K. (2013). *E-Transfers In Emergencies: Implementation Support*. Retrieved 22. September 2018, from <http://www.cashlearning.org/downloads/e-transfer-guidelines-English-20-12-2013.pdf>

Sovrin, (2018, January). Sovrin™: A Protocol and Token for Self-Sovereign Identity and Decentralized Trust. *Whitepaper (1)*. Retrieved 25. October 2018, from <https://sovrin.org/wp-content/uploads/2018/03/Sovrin-Protocol-and-Token-White-Paper.pdf>

State Department for Immigration, Border Control and Registration of Persons. (2018). *Introduction*. Retrieved 22. November 2018, from <http://www.immigration.go.ke/introduction/>

Stevens, L. 2018. *Self-Sovereign Identities for Scaling up Cash Transfer Projects - Designing a blockchain based digital identity system*. Retrieved 20. August 2018, from internal Netherlands Red Cross Server. For reference: uuid:6cdb5450-9a81-47a9-8ffa-f9bd77c72448

Stewart, F. (2002, February) *Horizontal Inequalities: A Neglected Dimension of Development*. 20. February 2018, from [https://www.qeh.ox.ac.uk/sites/www.odid.ox.ac.uk/files/www3\\_docs/qehwps81.pdf](https://www.qeh.ox.ac.uk/sites/www.odid.ox.ac.uk/files/www3_docs/qehwps81.pdf)

Stewart, F. (2009). Horizontal Inequality: Two Types of Trap. *Journal of Human Development and Capabilities* 10, (3), *Selected papers from the 2008 International Conference of the Human Development and Capability Association*, pp. 315-340. Retrieved 20. February 2018, from <https://doi.org/10.1080/19452820903041824>

Techopedia. (N.D.). *Identity Token*. Retrieved 24. October 2018, from <https://www.techopedia.com/definition/24834/identity-token>

Telekom Network Malawi. (2017). *What is Mpamba*. Retrieved 09. November 2018, from <https://www.tnm.co.mw/mpamba>

The Standard. (2018, March 19). *Huduma Card out in October*. Retrieved 16. November 2018, from <https://www.standardmedia.co.ke/business/article/2001273730/huduma-card-out-in-october>

Tobin and Reed, (2017, March 27). *The Inevitable Rise of Self-Sovereign Identity*. Retrieved 26. October 2018, from <https://sovrin.org/wp-content/uploads/2017/06/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf>

Tobor, N. (2018, October 22). Malawi is about to force businesses to accept digital payments. *IAfrikan*. Retrieved 10. November 2018, from <https://www.iafrikan.com/2018/10/22/malawi-mobile-money-fintech-policy-governance/>

United Nations (2016, September). High-Level Panel on Humanitarian Financing Report to the Secretary-General. *Too important to fail—addressing the humanitarian financing gap*. Retrieved 27. September 2018, from <https://reliefweb.int/sites/reliefweb.int/files/resources/%5BHLP%20Report%5D%20oo%20important%20to%20fail%E2%80%94addressing%20the%20humanitarian%20financing%20gap.pdf>

United Nations Capital Development Fund [UNCDF]. (2017, December). *Digital Financial Services Price Transparency and Awareness in Malawi*. Retrieved 08. November 2018, from <https://www.uncdf.org/download/file/127/5163/malawi-white-paper---price-transparencypdf>

United Nations Capital Development Fund [UNCDF]. (2018, March 16). *The M4p Story of Digital Financial Services in Malawi*. Retrieved 11. November 2018, from <http://www.uncdf.org/article/3374/the-mm4p-story-of-digital-financial-services-in-malawi>

United Nations Department of Economic and Social Affairs [UN-DESA]. (2015). *Sustainable Development Goal 16*. Retrieved 10. October 2018, from <https://sustainabledevelopment.un.org/sdg16>

United Nations Department of Economic and Social Affairs [UN-DESA]. 2015a. *Sustainable Development Goals*. Retrieved 29. October 2018, from <https://sustainabledevelopment.un.org/sdgs/>

United Nations Development Programme [UNDP] Europe. (2018). Retrieved 21. November 2018, from <http://www.europe.undp.org/content/geneva/en/home/partnerships/humanitarian-and-development-nexus-in-protracted-emergencies.html>

United Nations High Commissioner for Refugees [UNHCR]. (2018). *UNHCR Strategy on Digital Identity and Inclusion*. Retrieved 10. December 2018, from [https://www.unhcr.org/blogs/wp-content/uploads/sites/48/2018/03/2018-02-Digital-Identity\\_02.pdf](https://www.unhcr.org/blogs/wp-content/uploads/sites/48/2018/03/2018-02-Digital-Identity_02.pdf)

United Nations High Commissioner for Refugees [UNHCR]. (2018a). *Global Trends Forced Displacement in 2017*. Retrieved 19. November 2018, from <http://www.unhcr.org/5b27be547.pdf>

United Nations Malawi. (2018, April 27). *Malawi's National ID Project Praised at Africa's Largest Forum on Digital Identity*. Retrieved 09. November 2018, from <https://mw.one.un.org/malawis-national-id-project-praised-at-africas-largest-forum-on-digital-identity/>

United Nations Malawi. (2018a, November 09). *With 35,000 refugees in Malawi facing ration cuts, UN agencies seek urgent funding*. Retrieved 10. November 2018, from <https://mw.one.un.org/with-35000-refugees-in-malawi-facing-ration-cuts-un-agencies-seek-urgent-funding/>

United Nations Office for the Coordination of Humanitarian Affairs [UN-OCHA]. (2002). *Best Practices in Humanitarian Information Management and Exchange*. Retrieved 21. October 2018, from <http://www2.wpro.who.int/internet/files/eha/toolkit/web/Technical%20References/Health%20Information%20Management/UN%20OCHA%20Best%20Practices%20in%20Humanitarian%20IM.pdf>

United Nations Office for the Coordination of Humanitarian Affairs [UN-OCHA]. (2008, August). *Glossary of Humanitarian Terms*. Retrieved 04. October 2018, from [https://www.humanitarianlibrary.org/sites/default/files/2014/02/ReliefWeb\\_GlossaryOfHumanitarianTerms.pdf](https://www.humanitarianlibrary.org/sites/default/files/2014/02/ReliefWeb_GlossaryOfHumanitarianTerms.pdf)

United Nations Office for the Coordination of Humanitarian Affairs [UN-OCHA]. (2017) *New Way of Working*. Retrieved 22. December 2018, from [https://www.unocha.org/sites/unocha/files/NWOW%20Booklet%20low%20res.002\\_0.pdf](https://www.unocha.org/sites/unocha/files/NWOW%20Booklet%20low%20res.002_0.pdf)

United Nations Statistics Division [UNSD]. (ND). *Mobile Cellular Subscriptions*. Retrieved 11. November 2018, from <https://millenniumindicators.un.org/unsd/mdg/Metadata.aspx?IndicatorId=0&SeriesId=780>

United States Agency for International Development [USAID]. (2017). *Identity in a Digital Age: Infrastructure for Inclusive Development*. Retrieved 02. October 2018, from [https://www.usaid.gov/sites/default/files/documents/15396/IDENTITY\\_IN\\_A\\_DIGITAL\\_AGE.pdf](https://www.usaid.gov/sites/default/files/documents/15396/IDENTITY_IN_A_DIGITAL_AGE.pdf)

United States Agency for International Development [USAID]. 2018. *Digital Tools in USAID Programming Toolkit*. Retrieved 13. November 2018, from <https://www.ictworks.org/wp-content/uploads/2018/04/Programming-Toolkit-Digital-Tools-for-Agriculture.pdf>

van der Veen, M.; Giodini, S.; Stevens, L. 2018. 510. *Future of Cash Based Assistance*. Retrieved 06. August 2018 from Netherlands Red Cross Server. Internal document.

Vorha, A. 2015, (January 11). E-wallets: Money on the move. *Financial Express*. Retrieved 01. November 2018, from <https://www.financialexpress.com/industry/banking-finance/e-wallets-money-on-the-move/28571/>

Wakaya, J. (2018, February 20). IDs fitted with electronic chips in the pipeline: Interior Ministry. *Capital FM*. Retrieved 17. November 2018, from <https://www.capitalfm.co.ke/news/2018/02/ids-fitted-with-electronic-chips-in-the-pipeline-interior-ministry/>

Wardak, K. (2018., July 26). *Malawi stands out in the 2017 Global Findex*. Retrieved 09. November 2018, from <http://mw.one.un.org/malawi-stands-out-in-the-2017-global-findex/>

Washon, F. (2016, January 21). *Malawi Red Cross bails out starving households*. Retrieved 08. November 2018, from <https://reliefweb.int/report/malawi/malawi-red-cross-bails-out-starving-households>

Windley, P. (2016, April 24). *Self-Sovereign Identity and Legal Identity*. Retrieved 25. October 2018, from [http://www.windley.com/archives/2016/04/self-sovereign\\_identity\\_and\\_legal\\_identity.shtml](http://www.windley.com/archives/2016/04/self-sovereign_identity_and_legal_identity.shtml)

World Bank. (2007, January 16). *IEG Guidelines for Global and Regional Program Reviews (GRPRs)*. Retrieved 23. September 2018, from <http://siteresources.worldbank.org/EXTGLOREGPARPROG/Resources/GRPPguidelines.pdf>

World Bank. (2012, August). *Financial Inclusion Strategies Reference Framework*. Retrieved 17. August 2018, from <https://siteresources.worldbank.org/EXTFINANCIALSECTOR/Resources/282884-1339624653091/8703882-1339624678024/8703850-1339624695396/FI-Strategies-ReferenceFramework-FINAL-Aug2012.pdf>

World Bank. (2014, June). *Digital Identity Toolkit - A Guide for Stakeholders in Africa*. Retrieved 01. November 2018, from <http://documents.worldbank.org/curated/en/147961468203357928/pdf/912490WP0Digit00Box385330B00PUBLIC0.pdf>

World Bank. (2016). *Cash Transfers in Humanitarian Contexts – Strategic Note*. Retrieved September 19. 2018, from <http://documents.worldbank.org/curated/en/697681467995447727/pdf/106449-WP-IASC-Humanitarian-Cash-PUBLIC.pdf>

World Bank. (2016a). *World Development Report 2016: Digital Dividends*. Retrieved 22. October 2018, from <http://documents.worldbank.org/curated/en/896971468194972881/pdf/102725-PUB-Replacement-PUBLIC.pdf>

World Bank. (2016b). *ID4D Country Diagnostic: Kenya*. Retrieved 18. November 2018, from <http://documents.worldbank.org/curated/en/575001469771718036/pdf/Kenya-ID4D-Diagnostic-WebV42018.pdf>

World Bank. (2017). *Technical Standards for Digital Identity Systems for Digital Identity - Draft for Discussion*. Retrieved 28. September 2018, from <http://pubdocs.worldbank.org/en/579151515518705630/ID4D-Technical-Standards-for-Digital-Identity.pdf>

World Bank. (2017a). *Principles On Identification For Sustainable Development: Toward The Digital Age*. Retrieved 05. October 2018, from <http://documents.worldbank.org/curated/en/213581486378184357/pdf/112614-REVISED-English-ID4D-IdentificationPrinciples-Folder-web-English-ID4D-IdentificationPrinciples.pdf>

World Bank. (2017b). *State of Electricity Access Report*. Retrieved 28. October 2018, from <http://documents.worldbank.org/curated/en/364571494517675149/pdf/114841-REVISED-JUNE12-FINAL-SEAR-web-REV-optimized.pdf>

World Bank. (2018). *Financial Inclusion - Overview*. Retrieved June 23, 2018, from <http://www.worldbank.org/en/topic/financialinclusion/overview>

World Bank. 2018a. *The Little Data Book on Financial Inclusion 2018*. Retrieved 08. November 2018, from <https://openknowledge.worldbank.org/handle/10986/29654>

World Bank. (2018b). *World Bank Data. Mobile Cellular Subscriptions (per 100 people)*. Retrieved 09. November 2018, from <https://data.worldbank.org/indicator/IT.CEL.SETS.P2?locations=MW>

World Bank. (2018c). *Identification for Development. Global Identification Challenge by the Numbers*. Retrieved 21. November 2018, from <http://id4d.worldbank.org/global-dataset/visualization>

World Bank. (2018d). *Access to electricity (%) of population*. Retrieved 10. November 2018, from <https://data.worldbank.org/indicator/eg.elc.accs.zs>

World Bank and GSMA. (2016, July). *Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation*. Retrieved 24. September 2018, from <https://openknowledge.worldbank.org/bitstream/handle/10986/24920/Digital0identi0e0sector0cooperation.pdf?sequence=1&isAllowed=y>

World Economic Forum. (2018, September). *Identity in a Digital World - A new chapter in the social contract*. Retrieved 18. December 2018, from [www3.weforum.org/docs/WEF\\_INSIGHT\\_REPORT\\_Digital%20Identity.pdf](http://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf)

World Food Programme [WFP]. (2015). *Bamba Chakula -Vouchers for food assistance in Kenya's refugee camps*. Retrieved 06. October 2018, from [https://www.wfp.org/sites/default/files/Update%20on%20vouchers%20in%20the%20camps%20Apr-15\\_0.pdf](https://www.wfp.org/sites/default/files/Update%20on%20vouchers%20in%20the%20camps%20Apr-15_0.pdf)

World Food Programme [WFP]. (2016). *WFP and Digital Innovation*. Retrieved 16. October 2018, from <https://documents.wfp.org/stellent/groups/public/documents/communications/wfp287655.pdf>

World Food Programme [WFP]. (2018, June 01). *Kenya country strategic plan (2018–2023)*. Retrieved 16. November 2018, from [https://docs.wfp.org/api/documents/8681e711600d423caf6c595139c10da4/download/?\\_ga=2.40350689.2116147740.1542364873-1513470843.1541678592](https://docs.wfp.org/api/documents/8681e711600d423caf6c595139c10da4/download/?_ga=2.40350689.2116147740.1542364873-1513470843.1541678592)

Zambrano, R. (2017). *Unpacking the disruptive potential of blockchain technology for human development*. Retrieved 22. January 2018, from <https://idl-bnc-idrc.dspacedirect.org/bitstream/handle/10625/56662/IDL-56662.pdf>

Zambrano, R. (2018, January 29). *An Overview of Blockchain Technology and Digital Identity*. [blog post]. Retrieved 15. December 2018, from <https://blog.raulza.me/an-overview-of-blockchain-technology-and-digital-identity/>

Zambrano, R. (2018a, July 15.) *Have You Ever Seen a Blockchain?* [blog post]. Retrieved 15. December 2018, from <https://blog.raulza.me/have-you-ever-seen-a-blockchain/>

Zambrano, R. (2018b, February 22) *Blockchain Technology and Human Development revisited*. [blog post]. Retrieved 15. December 2018, from <https://blog.raulza.me/blockchain-technology-paper-revisited/>

Zimmerman, J.; Porter, B.; Dermish, A. (2016, May). *Digital Financial Services in Post-Crisis Contexts: Improving Response, Building Resilience*. Retrieved 31. October 2018, from <https://docplayer.net/31427431-Digital-financial-services-in-post-crisis-contexts.html>

Zimmerman, J.; Bohling, K.; Kavalo, T.; Nvirongo, N.; Le Sar, B. 2015. *Development Results Focused Research Program. Country Diagnostic: Malawi*. Retrieved 13. November 2018, from [CCL](https://btca-</a></p></div><div data-bbox=)

prod.s3.amazonaws.com/documents/35/english\_attachments/BTCA-Long-Version-Malawi-Diagnostic.pdf?1438939702

Zimmerman, J.; Martin, C. (2016, September 16). *Eight Principles for Digital Payments in Humanitarian Response*. Retrieved 30. October 2018, from <https://nextbillion.net/eight-principles-for-digital-payments-in-humanitarian-response/>

Zimmerman, J. (2017). *Mission Critical: Enabling Digital Payments for Development*. Retrieved 30. October 2018, from <https://www.usaid.gov/sites/default/files/documents/15396/USAID-DFS-OpportunityBrief.pdf>

Zoona. 2018. *Sunga Pockets*. Retrieved 08. November 2018, from <https://ilovezoona.com/our-products/sunga-pockets/>