Towards more foundational humanitarian Self-Sovereign Identity systems

Exploring strategies for humanitarian organizations to nurture support for SSI systems in Kenya, as a way to facilitate in-name SIM- and mobile money registration of un(der)documented, by using a design-oriented approach.

Master thesis submitted to Delft University of Technology

in partial fulfilment of the requirements for the degree of

MASTER OF SCIENCE

in **Complex Systems Engineering & Management**

Faculty of Technology, Policy and Management

by

M.F. Bouwens

Student number: 4244265

To be defended in public on: 08-07-2020

Graduation committee

Chairperson	: Prof.mr.dr., J.A., de Bruijn, Multi-Actor Systems
First Supervisor	: Dr.ir., B.M., Steenhuisen, Multi-Actor Systems
Second Supervisor	: Dr., T.C., Comes, Engineering Systems and Services
External Supervisor	: Ir., L., Stevens, 510 NLRC

Preface

Dear reader,

The document you see in front of you is the result of my concluding challenge for the MSc Complex Systems Engineering and Management program at Delft Technical University. I started working on this research subject due to my concerns regarding the imbalance of control over personal data and the increasing monetization of digital footprints. My personal conviction and passion for this subject is what kept me going through what became a long and challenging process full of personal setbacks. However, this was not the only thing that enabled me to bring this research to a conclusion.

From the TU Delft, I am most grateful to Bauke Steenhuisen. Bauke went to great lengths in his support for me. No matter what, Bauke was always there to answer questions and to provide feedback. During the weekend, while out cycling with his child in the backseat, while changing diapers; regardless of the circumstance, Bauke was available for urgent matters. He forced me to manage my expectations and while my discussions with him may sometimes have been frustrating, they have been key in reaching a comprehensible storyline. Furthermore, I would like to thank Tina Comes and Hans de Bruijn for their expertise and critique during our graduation committee meetings.

From 510 NLRC, Lars Stevens has been my pillar of strength, for which I would like to thank him. Throughout this research, Lars constantly inspired me with confidence, forced me to structure my deadlines, had multiple coaching and substantive meetings with me, and frequently checked in on my progress. I would also like to thank the entire team for giving me the feeling that no matter what, 510 would have my back during my struggle. They provided me with an environment in which I instantly felt welcome, this is something for which Jonath and Orla in particular deserve a lot of credit.

Finally, I am extremely grateful to my family and friends. I have the privilege of being surrounded by this amazing group of people who unconditionally provide me with social, emotional, practical, and financial support. During these past few months, I have relied on these people many times and I hope to return the favor in the future.

M.F. Bouwens
Amsterdam, June 2020

Extended Summary

African and Asian regions pose the biggest challenge for the UN sustainable development goal of providing a legal identity to everyone (UN, 2015). These regions host the majority of 1 billion people that lack the means of official identification (The World Bank, 2018). Under-documentation and complete lack of proof of identity create big obstacles for Humanitarian Organizations (HOs). This is especially a problem for the increasingly popular Cash Transfer Programs (CTPs), which now comprises 15% of global humanitarian aid and is expected to increase further (Stevens, 2018). CTPs, instead of delivering in-kind aid, enable beneficiaries to self-procure their necessities through direct funding.

A lack of identity proof among vulnerable people creates several problems for HOs. Firstly, it creates significant parallel targeting and registration costs for every HO (Stevens, 2018), which due to privacy concerns and competition is not shared with other HOs. Secondly, it complicates efficient payment facilitation for CTPs (UNHCR & GSMA, 2019) due to a lack of access to financial services for beneficiaries, such as the in Africa prevalent mobile money services (transactions through SMS texting). This lack of access to increasingly vital services also restricts the ability of beneficiaries to self-procure necessities efficiently and safely. Thirdly, in many countries, it prevents people of concern to get access to in-name (registered to an individual's identity) mobile network services (GSMA, 2017). Obstructing the ability of HOs to distribute life-saving information in the case of disaster or crisis. Finally, in light of the humanitarian-development nexus, a renewed approach of humanitarian aid that acknowledges the dramatic increase in prolonged humanitarian intervention, a new urgency has emerged for better connectivity between humanitarian and development efforts in order to reduce risk, vulnerability, and increase overall resiliency (OCHA, 2017). This broadens the problems of a lack of identity proof for HOs beyond the boundaries of humanitarian aid delivery, as it is limiting the quality of life, dignity, safety and the ability of un(der)documented to re-establish livelihood which eventually often leads to vulnerability, poverty and further pressure on humanitarian aid capacity.

Several humanitarian initiatives have emerged that develop digital identity management systems to solve these problems. Progress has been made up to the point that the first two problems have at least been partially addressed. In order to do this HOs deviated from traditional identity management systems, which lack in privacy, security and are prone to function creep, and have started developing Self-Sovereign Identity (SSI) systems. Through SSI, which is a blockchain-enabled user-controlled identity management scheme, HOs are able to give control over humanitarian registration data to beneficiaries. The beneficiaries can leverage this information as a digital identity to prove their identity to other HOs. However, in order to fully address the four identified problems, the system must be scaled beyond the boundaries of HOs into a more foundational purpose. For example, HOs see potential for these SSI systems to facilitate un(der)documented people to gain access to in-name private sector services such as SIM cards and mobile money accounts.

In earlier humanitarian research Stevens (2018) designed the foundations of the technical and institutional design principles for a humanitarian SSI system with built-in flexibility to further

scale to more foundational purposes. However, he emphasized the need for a process design: "A process design deals with the participation of stakeholders, creating support and changing a conceptual design into a final working system." Subsequently, Meyling (2019), who researched the potential of these humanitarian SSI systems to facilitate a more foundational purpose concluded that SSI does have potential for more foundational purposes such as financial inclusion, however, he added the following: "For a more formal, legally-compliant and sustainable acceptance, the humanitarian agency must however involve the public sector and prove SSIs advantages when compared to the incumbent systems." This research takes a first step in exploring potential support nurturing principles that create more support from public- and private sector stakeholders for this initiative. This is done specifically for the case of Kenya. This leads to the main research question:

"How can humanitarian organizations nurture support for humanitarian SSI systems as a way to facilitate in-name SIM- and Mobile money registration for un(der)documented in Kenya?"

This research has been conducted in collaboration with Delft Technical University, the Netherlands Red Cross and their data-science team "510". A Design Science Research (DSR) inspired approach has been used to answer the research question. It combines systems theory and technology acceptance factors to explicate the problem, define more favorable circumstances and conditions in Kenya that could drive support for a humanitarian SSI system, generate support nurturing principles to nurture these conditions and validate the usefulness of said support nurturing principles. The research deviates from an original DSR approach, as it is only shaping part of a more complete process design. The requirements and the support nurturing principles are limited to creating more favorable circumstances and conditions as a way to allow for more stakeholder support. Creating support among public- and private sector stakeholders is just aimed at laying the foundation for a longer-lasting process of collaboration. Subsequently, the research further deviates from a traditional DSR approach as the demonstration of the support nurturing principles has been left out of the research scope. This was excluded in the research due to the nature of the artefact, which is hard to demonstrate without applying it in a real-world scenario. As part of this approach, a System analysis has been conducted in which the current state of technical, institutional, and stakeholder context in Kenya's identity ecosystem has been explored. Requirements have been defined in the form of required changes to the local circumstances and conditions in Kenya, which according to technology acceptance factors and the insight of several involved respondents could lead to more acceptance and thus support of public- and private stakeholders. The final deliverable is a set of advised and evaluated support nurturing principles, which could be included in a more complete process design. Methods that have been used in this research are: Literature review, desk research, semi-structured interviews, and expert validation.

System Analysis: Exploring Kenya's Identity ecosystem

The system analysis provides a birds-eye-view of the Kenyan identity ecosystem. It describes the socio-technical system in which the proposed humanitarian SSI system would have to be integrated in. Including the established and anticipated systems of identity provision in the country, related institutional context, and an analysis of involved stakeholders.

The system analysis concluded in three lists of bullet points which describe the technical-, institutional- and stakeholder environments of the Kenyan identity ecosystem. Several things were found that were used as a basis to further shape the requirements and design. Firstly, the privacy regulation pressure in the country is currently non-existent. Secondly, awareness with regard to privacy in the country is still limited. Thirdly, the technological environment in Kenya is relatively well connected and advanced when considering mobile phone coverage and usage. Fourthly, there seems to be both intentional and unintentional identity exclusion in the country. Fifthly, service providers in the country have to deal with relatively strict onboarding regulations. Sixthly, Kenya as a country is actively exploring blockchain and its possibilities, however understanding and experience with SSI as a technology is still only on sporadic individual basis and not on an organizational level. Seventhly, there is humanitarian involvement in identity provision for refugees and asylum seekers to some extent. However, this remains on a parallel basis and is not a gateway to private sector services. Finally, there is a high degree of information asymmetry in the country between public, private and non-governmental organizations. This is especially the case due to the fragmentation of identity systems in the country and the continuous data collection by HOs.

Based on the developments within Kenya's identity ecosystem and discussions with HO representatives about the engagement with public- and private stakeholders two things were concluded. Firstly, national public- and private sector stakeholders inevitably have to be involved in the process due to their essential resources and responsibilities. National authorities especially have significant blocking power to obstruct the proposed development. Secondly, there is currently not enough sense of urgency for these stakeholders to support developments for a humanitarian SSI system. As a result of these insights, the scope of the research was slightly adjusted. Where initially the research had the intention to create a full process design, it now is focused on exploring how support can be nurtured using design principles.

Requirements: Favorable circumstances and conditions

Semi-structured interviews were conducted with six respondents that have an affiliation to humanitarian or private sector SSI initiatives. During these interviews, local circumstances and conditions were identified that drive or limit the support for a (humanitarian) SSI system, independently of the Kenya case. These insights were categorized, as displayed in table 1, and placed in the context of Technology Acceptance Modelling as external variables that can influence the "Attitude towards using". This research assumes that creating support among stakeholders for (humanitarian) SII systems goes hand in hand with establishing a positive attitude towards using a technology or system. By establishing scales of suitability for each category, a framework was composed with which the suitability of local circumstances and conditions can be assessed.

Table 1: Categories of local circumstances and conditions assessment framework.

#	Local circumstances and conditions assessment categories:
1	Privacy legislation pressure
2	Information privacy awareness
3	Online accessibility
4	Identity exclusion motive

5	Financial service onboarding obstacles
6	SIM card onboarding obstacles
7	Degree of information and knowledge of SSI
8	Humanitarian involvement in refugee and asylum seeker registration
9	Identity information asymmetry

The findings gained during the technical-, institutional- and stakeholder analysis sub-conclusions were used to fill out the framework for the case of Kenya. Based on this assessment, which is displayed in figure 1, several possible changes to the local circumstances and conditions in Kenya were identified using this framework to increase the support of public- and private sector stakeholders for a humanitarian SSI system as a way to facilitate SIM- and mobile money registration of un(der)documented. The local circumstances and conditions labeled #1, #2, #4 - #8 as displayed in table 1 were found to be unfavorable or moderately unfavorable for the Kenya case. Therefore, improving on these identified circumstances and conditions in Kenya provides a way to increase the support of public- and private sector stakeholders in the country for the proposed humanitarian SSI system.

Suitability: / Local Circumstance / condition:	Unfavorable:	Moderately unfavorable:	Moderately favorable:	Favorable:
Privacy Legislation pressure	No Data protection legislation.	Consent focused data protection legislation which stimulates hedging against data breaches and data misconduct.	Legislation enforcing private sector data handling accountability which stimulates data responsibility offloading.	Legislation enforcing public and private sector data handling accountability which stimulates data responsibility offloading.
Information Privacy Awareness	Unaware of the elements* related to information privacy	Knowledge of the elements* related to information privacy.	Understanding that elements* related to information privacy exist in the current environment.	Projection what impact elements* related to information privacy have in the future.
Online accessability	Low mobile network coverage, low mobile phone penetration, insufficient access points in rural areas and low digital literacy.	Average / High mobile network coverage, low mobile phone penetration, some central access service points in rural areas and low digital literacy.	High mobile network coverage, average mobile phone penetration, wide spread central access service points in rural areas and some digital literacy.	Full mobile network coverage, high mobile phone penetration also in rural areas,wide spread central access service points and high digital literacy.
Identity exclusion motive	Mainly intentional exclusion.	Mixed intentional/ unintentional exclusion.	Exclusion mainly unintentional due to a burden of proof or cost for individuals.	Exclusion mainly unintentional due to lack of government registration capacity or voluntary exclusion due to privacy / security concerns.
Financial service onboarding obstacles	strict KYC restrictions.	KYC restrictions & limited remote registration.	KYC restrictions, limited remote registration & limited access to high risk areas.	Loose KYC restrictions, limited remote registration & limited access to high risk areas.
SIM card onboarding obstacles	strict KYC restrictions.	KYC restrictions & limited remote registration.	KYC restrictions, limited remote registration & limited access to high risk areas.	Loose KYC restrictions, limited remote registration & limited access to high risk areas.
Degree of information and knowledge of SSI	No understanding of SSI technology or value proposition. Not much available information.	Some knowledge and information on SSI value proposition, low technical understanding. No exposure and experience with the technology.	Sufficient understanding of SSI technology and value proposition. Low exposure to the technology.	Broad spread understanding of SSI value proposition and technical understanding. Exposure / experience with the technology.
Humanitarian involvement in Refugee and Asylum seeker registration process	Host Government-Led registration	Joint-Led, Parallel HO registration	Joint-Led	Humanitarian Agency-Led
Identity information asymmetry	Identity information symmetry between stakeholders	Low identity information assymetry between stakeholders	High Identity Information assymetry between stakeholders	High Identity Information assymetry between stakeholders. Especially with HOs.

Figure 1: Circumstances and conditions assessment framework filled out in yellow for Kenya case.

Design: Support nurturing principles

Through the second part of the semi-structured interviews, several ideas of humanitarian involvement with the purpose of achieving the identified changes to circumstances and conditions in Kenya were generated. These ideas were aggregated and combined to design a set of 5 support nurturing principles that can contribute to nurturing more support among public- and private sector stakeholders for the proposed system. The principles were substantiated with several ideas of more concrete action. The initial version of the support nurturing principles is displayed in table 2.

Table 2: First version of support nurturing principles

#	Support nurturing principle:
1	Advocate for flexible KYC and financial/social inclusion of un(der)documented.
2	Create intrinsic motivation by stimulating privacy.
3	Protect core-values by sticking to mandates in humanitarian demonstration.
4	Broaden the agenda to leverage interest of the private sector.
5	Delay government commitment by initiating network effect through identity provision mandated stakeholders.

Validation

In order to validate the usefulness of the design, interviews were conducted with 2 experts; one respondent which is affiliated to a high-profile HO and the other affiliated to ID2020, a global public-private identity alliance. The 5 support nurturing principles and the local circumstances and conditions assessment framework were assessed with these experts. The assessment focused on usefulness, risks, and usability by the humanitarian sector. The design was received positively for the most part by both respondents. The main criticism was that flexible KYC should not be the long-term end goal of advocacy, instead, more defined KYC should be. And secondly, the establishment of network effects in Kenya through identity provision mandated stakeholders, outside of the government, was deemed to be ineffective. Based on the expert input, two refinements were implemented in the first and fifth support nurturing principle of the final design, which is displayed in figure 2.

Conclusions

Although this research originally set out to deliver a process design, during the research process it was established that the local circumstances and conditions do not provide a sufficient starting point for this, because there is not enough interest and sense of urgency among crucial stakeholders such as national authorities, FSPs and MNOs. These particular stakeholders hold significant blocking power and required resources to realize the proposed change, without their active support and dedication, chances of success remain low. This has led this research to focus on approaches to nurture support among these stakeholders.

This research has performed a design science research inspired cycle resulting in five support nurturing process principles. These principles, displayed in figure 2, were identified during the study and were found to be useful for the humanitarian sector to nurture more support for the in-name SIM and mobile money registration of un(der)documented through humanitarian SSI systems in Kenya. It does this by creating more favorable circumstances and conditions in the country.

Furthermore, the research provides a framework (figure 1) with which HOs can assess the circumstances and conditions in similar countries, by looking at several identified required circumstances and conditions. Using this, HOs can assess if certain countries are fruitful for a humanitarian SSI system or it can act as the basis for strategizing to make the environment more favorable for a humanitarian SSI system.

Finally, during the research it became evident that the support of a humanitarian SSI system for social and financial inclusion goes hand in hand with a political issue: The extent to which governments want to include un(der)documented people in the first place. This is a technological agnostic issue but does play an important part in the nurturing of support. Other findings include that refugees and asylum seeker registration, while at first glance seem to pose an excellent use-case to demonstrate the proposed system with, is unfit for this purpose due to the message of temporality that host countries want to emphasize to these people. Finally, humanitarian SSI initiatives should find ways to create intrinsic motivation for stakeholders on a national level to use SSI and for identity inclusion in general.

	Humanitarian support nurturing approach			
	#	Process principle	Implications	Risks
	1*	**Advocate for further defining of KYC, flexible KYC and financial/social inclusion of un(der)documented***	• Allow for existing **onboarding obstacles** to be met by innovative solutions. • Allow for further KYC exemptions for humanitarian purposes, enabling further demonstration oppertunities. • Discourage intentional exclusion and thus improves the **identity exclusion motive** in the country.	• Changing regulation does require long term commitment. • Flexibility in KYC could lead to encouraging a less rigorous system.
	2	**Create intrinsic motivation by stimulating privacy**	• Stimulate **information privacy awareness** and **digital literacy**. • Stimulate **privacy legislation pressure**. • Increase intrinsic economic and societal value of privacy and private systems.	• Stimulating privacy is a long term process. • Privacy is a complex and quickly evolving topic. A lack of continuous due dilligence from involved HOs can do more harm then good.
	3	**Protect core-values by sticking to mandates in humanitarian demonstration**	• Allows for a proof of value/concept with minimal political obstacles. • Creates exposure of the technology to public- and private sector stakeholders, more direct exposure is possible through lateral services. • Increases **information and understanding of SSI**. • Increase **information privacy awareness** and further increases **online accessibility** factors such as **digital literacy** among beneficiaries in practice. • Can potentially emphasize value of rectifying unintenional exclusion, disarming intentional **identity exclusion motives**.	• Overinflating the value in terms of inclusion potentioal of SSI. • Function creep and unintenional exclusion when scaling to lateral services. • Risk of losing innovation budget.
	4	**Broaden the agenda to leverage interest of the private sector**	• Alleviates **onboarding obstacles** by enriching identities with private sector data. • Can create direct commercial incentives, by including SSI use-cases such as KYC sharing. • Creates **exposure of SSI technology** to private sector stakeholders. • Increased private sector interest creates pressure on government stakeholders on a national level.	• Due to differences in core values between HOs and the private sector, friction can arise between neutrality and commercial interest. • There is a risk of correlatability of data when extending functionality.
	5*	**Delay government commitment by initiating network effects abroad***	• Expand through the way of minimal political resistance. • Allows for proof of value/concept, increasing **degree of information and knowledge of SSI**.	• Missing out on government capacity and expertise.

Figure 2: Final version of support nurturing principles (refined after validation, Implications on requirements in bold)*

Content

List of Figures

List of Tables

List of Acronyms

AML	Anti-Money Laundering
AP	Attribute Provider
BAKE	Bloggers Association of Kenya
BIMS	Biometric Identity Management System
CBA	Commercial Bank of Africa
CBK	Central Bank of Kenya
CONCISE	Coalition on Nationality, Citizenship and Statelessness Empowerment
CSO	Civil Society Organization
CTP	Cash Transfer Program
CSP	Corporate Social Responsibility
D-ID	Digital Identity
DID	Decentralized Identifier
DLT	Distributed Ledger Technology
DSR	Design Science Research
FSP	Financial Service Provider
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
GSMA	GSM Association
IdM	Identity Management System
IdP	Identity Provider
ID4D	Identification for Development
IEBC	Independent Electoral and Boundaries Commission
IFRC	International Federation of Red Cross and Red Crescent Societies
IPRS	Integrated Population Registry Service
HO	Humanitarian Organization
KCB	Kenya Commercial Bank
KICTANet	Kenya ICT Action Network

KHRC	Kenya Human Rights Commission
KNCHR	Kenya National Commission on Human Rights
KRCS	Kenya Red Cross Society
KYC	Know your Customer
MDP	Ministry of Devolution and Planning
MNO	Mobile Network Operator
MoI	Ministry of Interior and Co-ordination of National Government
MoICT	Ministry of Information Communication & Technology
MDP	Ministry of Devolution and Planning
MDTF	Multi-Donor Trust Fund
NGO	Non-Governmental Organization
NIIMS	National Integrated Identity Management System
NLRC	Netherlands Red Cross Society
OSF	Open Society Foundations
PKI	Public Key Infrastructure
PRIMES	Population Registration and Identity Management Ecosystem
ProGres	Profile Global Registration System
UNHCR	United Nations High Commissioner for Refugees
UNICEF	United Nations Children's Fund
USAID	United States Agency for International Development
SP	Service Provider
SSI	Self-Sovereign Identity
SSO	Single Sign-on
SDG	Sustainable Development Goals
WFP	World Food Programme

1. Introduction

1.1 Identity exclusion in Africa and digital identity

Providing a legal identity to everyone is one of the sustainable development goals that the UN aims to achieve by 2030 (UN, 2015). The African and Asian regions pose the biggest challenge in reaching this goal, as these regions host the majority of the 1 billion people that lack the means of official identification (The World Bank, 2018). African countries generally have limited and fragmented identity management infrastructures and more often than not lack a foundational form of identity that is available to everyone. This can be due to a burden of cost, burden of proof, limited state identification capacity or targeted exclusion. This is especially the case for un(der)-documented groups such as refugees, the stateless and marginalized groups. For these people reliance on national identification programs is often not possible. These individuals need a trusted, verifiable way to prove who they are, both in the physical world and online. Africa has the potential for leapfrogging in the development of inclusive digital identity solutions as digital technologies such as telecommunications and mobile phone payments have developed at a high rate. Digital identity systems have proven to increase accessibility and can lead to an estimated increase in the GDP by 3 to 13 percent (McKinsey, 2019). African countries have the opportunity to reduce identity exclusion by designing for inclusion through a complementary foundational digital identity system that enables these vulnerable un(der)-documented groups to participate in society.

1.2 Traditional Digital Identity management infrastructures falling short

Traditional digital identity management systems (IdM's) have been primarily interesting for governments to improve security, access of online public services and to create administrative efficiency (Strauß, 2011). However, privacy has been a rather implicit goal that is insufficiently designed for in traditional IdM's. These systems are heavily focused on unique identification but lack crucial aspects such as anonymity and pseudonymity (ibid). Additionally, the risks and liabilities that come with storing huge amounts of personal information in centrally controlled servers are becoming more evident. Instances like the Cambridge Analytica scandal and the Equifax breach where the personal information of over 143 million people was compromised (Gressin, 2017) indicate that service providers are not always able to bear the responsibility that comes with storing or distributing large amounts of personal data. Traditional IdM's, which often rely on centralized data servers, are prone to security risks and function creep due to the relative accessibility of these data repositories. According to Strauß (2011), the major challenge is to compensate for the imbalanced control over personal information in these systems.

This is especially important when the goal is to reach a more inclusive digital identity system. The people that are currently excluded from a legal identity in Africa consist of extra vulnerable or marginalized groups for which misconduct or leaking of their identity information could potentially have a life-changing impact. A study commissioned by the ID4D initiative on the identification of marginalized groups in Nigeria emphasized the importance of strong data privacy

protocols. These must be clearly conveyed to digital identity participants in order to optimize participation and to minimize risk. Since several marginalized populations in Nigeria are already subjected to government- or third-party coercion or harassment (LeVan et al., 2018). This article recommended that digital identity systems must minimize the danger of loss of control over personal information and eliminate the risk of accessing personal data for surveillance or targeted abuse, whether by third parties or by the government. Kenya Human Rights Commission (2019) also established in their latest report that most Kenyans do not trust the government with collecting and keeping citizen identity information. This indicates a necessity to move away from user consent focused systems and to embrace user-controlled systems.

1.3 Lack of identity proof inhibiting humanitarian aid

Due to the high rate of un(der)documented people among its beneficiaries, the humanitarian aid sector encounters difficulties in particular. Currently, these organizations are burdened with high targeting and registration costs. These costs are cutting in the budget available for humanitarian assistance. Increasingly so, the humanitarian sector is focused on providing people in need with the means to self-procure necessities, as opposed to providing the necessities directly. Humanitarian Organizations (HOs) especially apply this approach in situations where the existing economy, infrastructure, and/or services remain functional. For example, Cash Transfer Programs (CTPs) are increasingly becoming the intervention of choice in ongoing situations of disaster or as a preventive measure to prepare for disaster. By providing people in need with funds, these people can provide themselves with the services and goods they need. This has several advantages such as significant overhead cost reduction, restoration of dignity, timeliness of providing aid, stimulating the local market, and positively effecting health and reducing poverty (Lee, 2012). This is reflected in the strong growth of CTP share in total global humanitarian aid. This share was 6% by the end of 2015, increased to 15% by the end of 2017 and the share is expected to increase further in the future (Stevens, 2018).

The lack of identity proof among vulnerable groups and potential beneficiaries creates problems in fourfold: Firstly, identity information of potential beneficiaries is required to assess eligibility and to prevent fraud when targeting and registering for CTPs or other humanitarian interventions. Currently, every HO has independently developed its own registration procedure and manages its own beneficiary records. The resulting lack of interoperability creates sector-wide inefficiencies.

Secondly, beneficiaries need a proof of identity for access to financial services in order to facilitate cash transfers. For example, they require access to a bank account or mobile money account (the ability to transfer money through text messages) to remotely receive funds from humanitarian organizations. Similarly, access to an in-name mobile money accounts greatly improves the efficiency of self-procuring lifesaving necessities.

Thirdly, beneficiaries need a proof of identity for access to mobile network services. In almost 120 countries MNOs (mobile network operators) require a state-issued proof of identity to issue SIM cards (GSMA, 2017), resulting in the social exclusion of un(der)documented. This is problematic for HOs, as distributing information, especially in crisis or disaster situations, is one of its core tasks. Without in-name registered mobile connections, distributing lifesaving information in the case of disaster or crisis is complicated.

Fourthly, in recent years the humanitarian sector has started to rethink its approach of humanitarian assistance due to the dramatic increase of prolonged humanitarian intervention. A new urgency has emerged for better connectivity between humanitarian and development efforts in order to reduce risk, vulnerability, and increase overall resiliency. This approach, which aims to proactively alleviate some of the need for humanitarian intervention is dubbed the Humanitarian Development Nexus (OCHA, 2017). In light of this approach, the lack of identity proof among people creates risk, vulnerability, and a lack of resiliency to disaster. Quality of life, dignity, and safety of un(der)documented remain limited due to social and financial exclusion that originates from a lack of identity proof. For example, The UNHCR found that for many refugees, mobile devices are regarded as a core survival tool. Refugee families in Jordan were found to spend up to 20 percent of their cash on mobile connectivity and refugees often sell a portion of their food rations in order to purchase air time for their mobile phones (GSMA, 2017). Mobile phone connectivity and access to financial services are crucial for refugees to maintain contact with friends and family in home countries, access vital information, and for re-establishing a livelihood. Because these people cannot register services in their own name, they have to rely on the registration or service access of third parties. This puts these already vulnerable groups at risk of further extortion (GSMA, 2017).

To allow un(der)documented people to register and receive humanitarian aid more efficiently, HOs are developing digital identity solutions. Given the described shortcomings of traditional identity management infrastructures and following the humanitarian mandate to 'do no harm', HOs have started to develop user-controlled identity management schemes.

1.4 Self-Sovereign Identity as a solution

In recent years, development in blockchain technology infrastructure has given rise to a new form of identity management. This so-called 'self-sovereign identity' (SSI) management shifts away from the traditional centralized information storing and allows identity holders to control and distribute their personal information without the need to trust a third party (Baars, 2016). In order to reduce risk for marginalized and vulnerable groups, a Self-Sovereign digital identity system can reconstruct control over personal information, leading to improved and safer participation.

This is a very interesting proposition for HOs as it can allow for social and financial inclusion in a way that prevents data misconduct. In the last few years, several cases of SSI systems with a functional purpose have started to emerge. Several of these initiatives are actively exploring options to use blockchain for identity management in the humanitarian sector. Some of the ongoing initiatives include pilots such as the World Food Programme's (WFP): "Building Blocks". Another consortium effort including The International Federation of Red Cross and Red Crescent Societies (IFRC), Norway Refugee Council (NRC), Save the Children Norway and Norwegian Red Cross: "Dignified ID (DIGID)" and another consortium effort, including Netherlands Red Cross (NLRC) 510: "121 system".

These functional SSI systems can provide un(der)documented with a proof of identity that is required for targeting and registration of CTPs and other humanitarian interventions. It facilitates interoperability between the registration procedures of multiple HOs, potentially resolving the current sector-wide inefficiency. However, due to its functional purpose, these systems are not

established as proof of identity towards services outside of the humanitarian sector. As such, leveraging the local capabilities and services to assist in (disaster) relief and to alleviate vulnerability and poverty is still limited. This would require the current functional humanitarian SSI systems to scale to a more foundational nature. Enabling un(der)documented to register for financial and mobile network services using a humanitarian SSI would be a first step towards having a foundational identity for these people. As financial services can act as a gateway to other services. HOs are not the only organizations that are working on this, several private sector initiatives such as Sempo and Gravity are also committed to creating financial inclusion for un(der)documented through SSI systems.

1.5 Research Problem Definition

Scaling humanitarian SSI systems towards a more foundational purpose requires the involvement and dedication of additional public and private stakeholders, as it transcends the boundaries of its original functional purpose. Enabling the registration of un(der)documented for financial- and mobile network services through these systems would be a major milestone, but it is also a major challenge as additional social complexity is added to an already technically complex situation. In earlier humanitarian research Stevens (2018) designed the foundations of the technical and institutional design principles for a humanitarian SSI system with built-in flexibility to further scale to more foundational purposes. However, built-in flexibility is not enough to reach a foundational purpose on its own, he emphasized the need of a process design: “A process design deals with the participation of stakeholders, creating support and changing a conceptual design into a final working system.” Subsequently, Meyling (2019), who researched the potential of these humanitarian SSI systems to facilitate a more foundational purpose concluded that SSI does have potential for more foundational purposes such as financial inclusion, however, he added the following: “For a more formal, legally-compliant and sustainable acceptance, the humanitarian agency must however involve the public sector and prove SSIs advantages when compared to the incumbent systems.” This raises the question and knowledge gap: “How could this be done by HOs from a process perspective?” This research takes a first step in this by exploring potential support nurturing principles that create more support from public- and private sector stakeholders to facilitate financial and social inclusion of un(der)documented through humanitarian SSI systems.

1.6 Affiliation with the CoSEM study program

This research problem is appropriate to approach from a complex systems engineering perspective for the following reasons. Identity is deeply rooted in a complex technical- and social environment. Complex systems engineering provides a theoretical lens through which an innovation like an SSI system can be shaped for successful implementation, by considering socio-technical aspects such as technical systems, regulatory environments, and stakeholder environments. Scaling SSI systems to a more foundational purpose goes beyond just technical challenges, as it requires alignment and design for existing dynamic systems. As such, this research problem is deemed suitable for a graduation project in the CoSEM MSc. program.

2. Background

In this chapter, the existing knowledge regarding fundamental concepts related to this research problem will be presented. Primarily, this will be used to provide a basic level of understanding which is essential for conducting and understanding this research. In paragraph 2.1, the concept of digital identity is elaborated on. This is followed by paragraph 2.2, describing different digital identity management systems. Subsequently, in paragraph 2.3, blockchain technology is explained. And finally, in paragraph 2.4, the concept of Self-Sovereign Identity is briefly introduced.

2.1 Digital Identity

A study has been performed by El Maliki & Seigneur (2013) on online identity and User management systems. In their paper, the authors defined digital identity as "a representation of an entity in a specific context". Traditionally, digital identity was considered as the equivalent of our real-life identity regardless of the context including attributes such as: Who we are, what we like, and what our reputation is. Overtime issues such as phishing, spam, and identity theft have emerged with the development of the virtual world. These developments have shifted the perspective on the definition of digital identity. Recent academic work has concluded that this strong link between the real world identity and the digital identity is not always mandatory (El Maliki & Seigneur, 2013). This is especially the case for online services. For example, online marketplace platforms only need to know the reputation of the digital identities involved and if the users can prove control over that identity. For this purpose, the online marketplace is not interested in the other attributes of the user's digital identity. This means the representation of a digital identity needs to be context-specific.

2.2 Digital Identity management systems

Digital identity is just a record of attributes, on its own, it doesn't provide much functionality. For this, it relies on digital identity management. There is a multitude of systems providing digital identity management to users. These systems can be distinguished between in terms of architectural models and in terms of purpose.

2.2.1 Digital Identity management

El Maliki & Seigneur (2013) defined identity management as: "the process of representing, using, maintaining, deprovisioning, and authenticating entities as digital identities in computer networks." As such Identity management systems enable the functionality of digital identities. The Authors describe several main components in identity management:

User: Entity requesting access to a service.

Service provider (SP): Entity imposing an identity check.

Identity provider (IdP): Entity issuing user identity.

Identity: A set of user's attributes.

Identity attribute: A value that describes one of the following things: What a user has, what a user is, what a user knows, or what a user does.

Credential: A proof of identity- or attribute ownership (i.e. username/password or a fingerprint).

These components interact with each other during the lifecycle of a digital identity. Figure 2.1 presents a graphical representation of a digital identity lifecycle. Compared to El Maliki & Seigneur, 2 more components have been used in this diagram to represent the functioning of less traditional identity management systems. It introduces the following two concepts:

Attribute provider (AP): Entity that issues an attribute (claim) about the user.

Authentication provider: Entity that performs authentication checks on digital credentials.

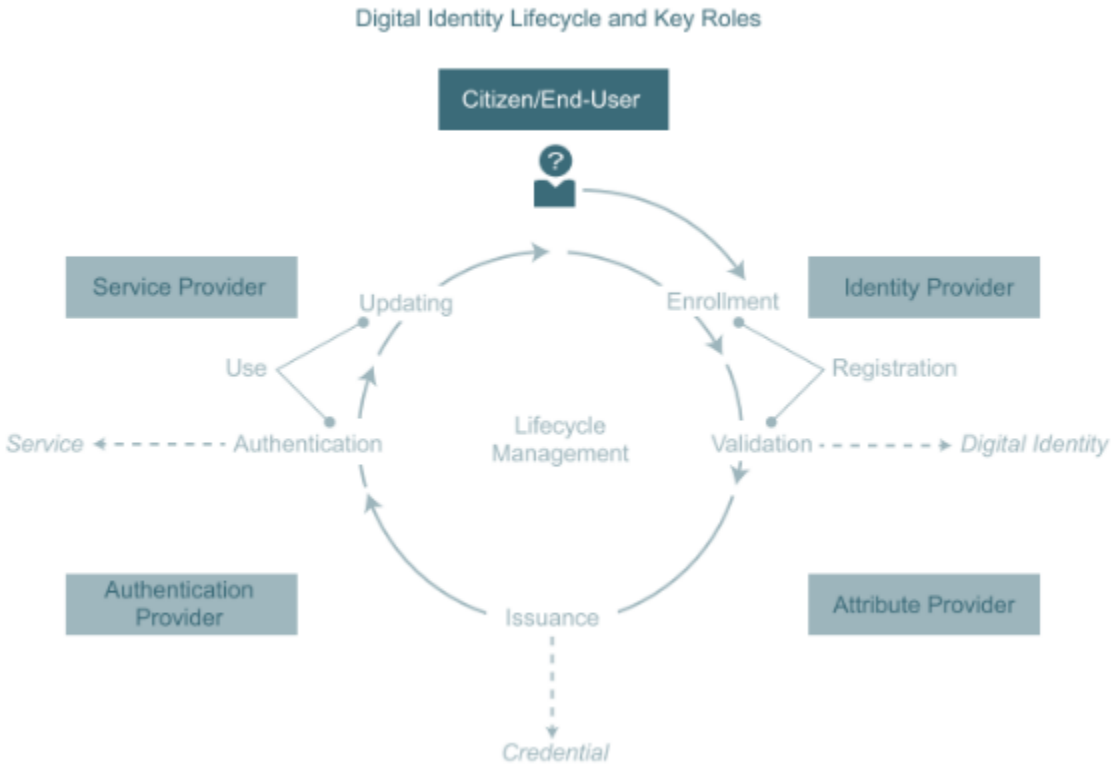

Figure 2.1: Digital Identity Lifecycle and Key Roles (World Bank Group & GSMA, 2016)

A digital identity is created when a user enrolls at an IdP. The user provides enrollment information which is validated by the IdP. If the information is found to be accurate by the IdP, a record of digital identity is created and stored. An attribute provider, which can coincide with a service provider, but can also be a trusted third party, issues a digital credential. The user can use this

credential to approach related service providers. Upon presenting the credential, authentication is performed by the authentication provider. The purpose of authentication is to determine if both interacting parties are who they claim to be. If this is the case, users gain access to a service provided by a service provider. Changes in user attributes are updated along the way.

2.2.2 Traditional Identity management models

Several different architectural models can be defined based on how these roles are distributed among a set of parties or technologies.

Isolated- / Siloed- identity management

In the Isolated/siloed identity model, service providers take on a second role as identity providers (El Maliki & Seigneur, 2013). This means that for every service that a user employs, a service provider goes through the steps of identification registration and stores a separate record of identity-related to that user. This essentially creates detached siloes of information. Authentication is done individually by every service provider by comparing the credentials a user presents with the stored information.

Centralized identity management

In the centralized identity model, the role of service provider and identity provider are separated (El Maliki & Seigneur, 2013). Users can rely on one single identity provider to gain access to multiple services. Essentially, service providers trust a third-party identity provider to perform authentication requests for them. The IdP (for example Facebook) provides identification and authentication, allowing users to log in to partnered service providers with their google account. This way the identity information of the user is not stored in individual "siloes" anymore, but only in one central server owned by Google.

Federated identity management

The federated identity model distributes identity data across multiple IdP's instead of storing it in one central server (Abraham, 2017). IdP's essentially form a federation to jointly provide the identity data required to access a service. Initially, this started in the form of Single Sign-on (SSO) systems, wherein the same enterprise credentials can be used for all individual internal components and departments within one organization. Later, systems emerged where different enterprises (service providers) started sharing the same credentials across identity management systems.

User-Centric identity management

In 2008 Cameron (2008) described a new form of identity management system in his paper: "A User-Centric Identity Metasystem". Unlike the other identity management models, the user's identity data is stored in the user's domain (Abraham, 2017). The sharing of information with service providers requires consent from the user. Cameron promoted the values of individual control, permission, and consent in his identity model. While User-Centric identity systems do provide users with more control, users still have to rely on centralized entities (Tobin & Reed, 2016).

2.2.3 Classification IdMs purpose

According to the 2017 USAID (United States Agency for International Development) report, there are two ways of distinguishing between the purpose of Digital ID (D-ID) systems. The first distinction in D-ID systems is the difference between functional and foundational systems. The USAID states that functional D-ID systems are typically developed for a specific application: for example a driver's license, an identification for elections, or health care (USAID, 2017). Therefore, any given person may own multiple functional IDs.

In contrast, foundational D-ID systems are developed to serve an entire range of needs for legal identity. These systems are typically owned and operated by governmental institutions and include, for example, passports and national identity cards. With a foundational identity, users can access multiple services across a wide range of sectors.

However, according to the USAID, exclusively distinguishing between functional and foundational systems dismisses the importance of the D-ID system design. Therefore, a distinction is made between instrumental and infrastructural approaches. Designing an ID system with an instrumental approach means that it is constructed to serve a, possibly single, purpose. Applying this type of design results in fragmented, single-application ID systems.

On the other hand, the infrastructural design of ID systems ensures a repurposable ID system that can be applied in similar projects. Additionally, it is designed to be compatible with previously developed local systems which result in a more cohesive ID ecosystem. The USAID additionally states that the infrastructural and instrumental approaches should be interpreted as a spectrum: ID systems may include elements of both design approaches. Below in figure 2.2, the cohesion between the concepts explained above is displayed.

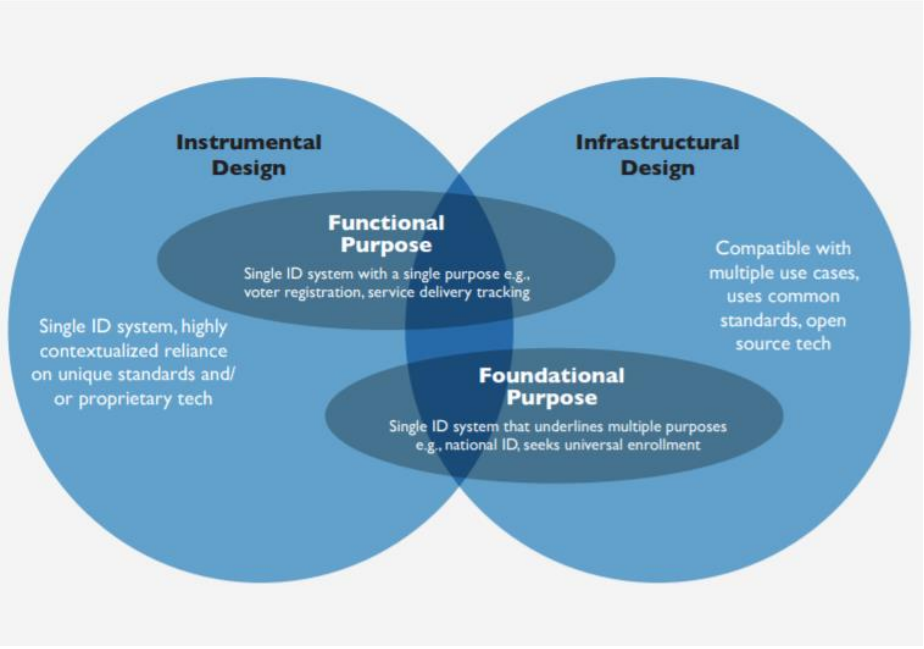

Figure 2.2: *Identity classification diagram acquired from: (USAID, 2017)*

2.3 Blockchain technology

Bacon, Michels, Millard, & Singh (2017) provide a clear description of blockchain technology in their publication: “a specific type of database that uses certain cryptographic functions to achieve the requirements of data integrity and identity authentication”. Blockchains generally track transactions, hence they are referred to as ledgers. The specifics of such transactions have to be tamper-resistant. By using hash functions, this data integrity can be offered. When a transaction occurs, the system has to verify that both parties associated with the transaction are engaging in the transaction. This identity authentication is covered in blockchain by leveraging public key infrastructure. Blockchain ledgers can be distributed across a peer-to-peer network, this way changes in the ledger are only accepted when consensus is reached across the whole network. The decentralization of the network in this way provides redundancy of network components. This greatly improves the resilience of the system as a whole. By relying on the consensus mechanism of the whole network, transacting parties do not have to rely on a trusted third party. The lack of this trusted third party means transactions are truly peer-to-peer and users experience full control over their own transactions. Additionally, blockchain also acts as a tool to digitally confirm the authenticity of the party you are transacting with.

There are several blockchain architecture types. The distinction is made between public and private blockchains. In the former, anyone can participate and read the network, in the latter only authorized participants can join and read the blockchain contents. A second distinction is made between permissionless and permissioned blockchains. In the former, all network participants have the right to write on the blockchain, in the latter only a selection of the participant has the right to write on the blockchain. For example, in a private permissioned blockchain only authorized participants can join and read the contents on the blockchain and only a select few of those participants can write to the blockchain.

The initial use-case of this DLT (distributed ledger technology) has been focused on financial transactions. The most well-known application of this technology is Bitcoin, founded in 2007 by anonymous figure Satoshi Nakamoto. In the bitcoin network, users can digitally prove their ownership over a digital currency. In recent years innovation has pushed the boundaries of the unit of accounting that can be tracked in these DLTs. This broader unit-of-accounting is conceptualized as “tokens”. Tokens can represent a wide variety of digital assets, but they can also be linked to physical assets. Essentially this development allows for digital proof-of-ownership over a wide variety of things. Among other things, it can be used to digitally prove certain attributes related to your identity.

2.4 Self-Sovereign Identity management

The recent developments in blockchain technology have revitalized interest in an alternative identity management model. This model, called Self-Sovereign Identity (SSI) management, evolved from the existing user-centric identity model which turned into a more interoperable, federated identity model. Enabled by the ability of blockchain to digitally prove ownership over identity attributes, SSI allows users to store and control their own identity without having to rely on any centralized entities. As users can carry and manage their own identity, it has the potential to fulfill a foundational purpose. This is the case only if enough services accept its validity.

3. Research design

To translate the described research problem to practical and actionable research, a research design is required. Firstly, paragraph 3.1 describes which organizations were involved in the research. Then in paragraph 3.2, the research problem is demarcated to a more actionable research scope. Subsequently, paragraph 3.3 presents the selection of a suitable research approach. In paragraph 3.4 the research approach is applied to the demarcated problem, leading to the formulation of the main research question and several sub-questions. Then paragraph 3.5 links these sub-questions to appropriate research methods, resulting in a research flow diagram. Finally, societal and scientific relevance is justified in paragraph 3.6.

3.1 Research collaboration

The humanitarian aid sector believes they are in a position where they can improve financial- and social inclusion through digital identity in developing countries while simultaneously improving the efficiency of humanitarian aid. This provides for unique collaboration opportunities for this research project. “121” (pronounced one-to-one) is a project run by a consortium of humanitarian aid-, public- and private organizations that developed an SSI system to streamline the identity management for Cash Transfer Projects. Currently, their system is only functional in nature, meaning it is only limited to a single purpose. 510, an initiative of the Netherlands Red Cross and a leading stakeholder in the 121 consortium, is currently exploring the viability of scaling the system to a more foundational purpose, to further improve the efficiency of humanitarian aid. Their intentions align well with the problem that was defined earlier. By collaborating with 510, a direct contribution can be made to the 121 system. In return 510 can contribute to the research by offering specialized knowledge concerning SSI systems and by providing access to their established network of stakeholders. Furthermore, the research is carried out for Delft Technical University as part of the CoSEM MSc. Program.

3.2 Research scope

This research is due to time and resource restrictions specifically focused on SSI as a solution for financial- and social exclusion of un(der)documented in Kenya. The scope is demarcated in terms of purpose, case country, and in terms of technology.

3.2.1 Problem scope

Providing access to financial- and mobile network- services is only a milestone in reaching a broader defined foundational purpose. However, financial- and mobile network services serve as a gateway to other services. In addition to that, access to financial- and mobile network- services for beneficiaries is required to provide efficient humanitarian (cash-based) assistance. For HOs it is most relevant to explore how they can facilitate un(der)documented people in gaining access to mobile money accounts and mobile network connectivity. This would greatly improve the efficiency of CTPs and information distribution in case of disaster/crisis situations.

3.2.2 Technology scope

In their report, the USAID (2017) identifies several technology trends for inclusive development of identity in a digital age. These technology trends are compared in table 3.1 on their potential for inclusion and several related criteria.

In their report, the institute describes developments in biometric-based identities. Because of the decreasing costs of biometric registration devices, this solution is getting increasingly attractive. User accessibility is increased, as almost everyone can provide biometrics. It is very effective in establishing the uniqueness of persons. But this solution does not provide any control over information to the users, as it is a consent-based type of system, and often lacks in transparency. Essentially, users run a bigger risk due to the more privacy sensitivity of biometrics. Biometrics still have to be linked to a person, which is why they are often linked to state-issued credentials. This limits the inclusion potential and creates corruption capability among central enrolling or authenticating authorities.

Secondly, the institute identified the technology trend of Mobile-ID. In this technology, users can verify identity through an account registered with a mobile network operator instead of a traditional ID card. In this solution, users do not gain any control over their information and the responsibility for the information is just shifted from public to private institutes. Users have no transparency in what their data is being used for. The capability for corruption is only increased by this. Additionally, the potential of inclusion relies on the requirements of registration at MNOs. For this, users often need a state-issued ID, thus limiting the potential of inclusion to a big group of users.

Thirdly, algorithmic identity is increasingly used. In this alternative, identity aspects are derived from a person's digital footprint. Anyone with digital activity can gain access to this identity technology. This creates a big potential for inclusion. This technique is increasingly used by services to serve populations who may lack official IDs. However, users lose complete control over their data and often do not know which data is used. This technology is often still unregulated and the capability of corruption is high due to a lack of transparency and control.

Finally, developments in SSI technology have shaped up to be a front runner when it comes to rebalancing the control over data in functional identity systems. By giving the user a central position in the identity ecosystem, the user has control over his own data and opens up a whole range of identity providers that a user can leverage. This creates additional accessibility for users because users are theoretically not limited to state-issued credentials in an SSI system. The underlying DLT (Distributed Ledger Technology) provides transparency and removes the reliance on central authorities, greatly reducing the capability of corruption.

All technologies can contribute to user accessibility of identity and have the potential for inclusion under certain circumstances. But from the perspective of humanitarian organizations, only SSI allows full user control and allows for a less corruptible and more transparent identity system. For these reasons, this research will focus on SSI as a technological solution.

Table 3.1: Inclusive digital identity technological solutions selected from (USAID, 2017).

Digital identity solutions:	Corruptibility	User Control	Transparency	User Accessibility	Inclusion Potential
Biometric centralized ID register	+	-	-	+	+/-
Mobile ID	+	-	-	+	+/-
Algorithmic Identity	+	-	-	+	+
SSI	-	+	+	+	+

3.2.3 Country scope

Limiting the study to a specific case country makes it more manageable. In order to select a relevant case country for this research, the identity registration statistics of the top 10 largest African countries by population size will be compared. The initial selection on population size is done to ensure the societal relevance of the research. This includes the countries as displayed in table 3.2.

Table 3.2: Population registration statistics (World Bank Group, 2018)

Country:	% Unregistered population:
Nigeria	72%
Ethiopia	65%
Egypt	2%
DR Congo	40%
South Africa	27%
Tanzania	47%
Kenya	18%
Uganda	49%
Algeria	11%
Sudan	38%

According to the statistics, Egypt and Algeria are excluded as they have a relatively small percentage of unregistered population. The remaining countries are compared with respect to their potential to leapfrog in digital identity management development. To do this, it is important that underlying ICT infrastructure and eGovernance aspects are relatively developed. This potential is measured with UN eGovernance indicators and ICT development index statistics as displayed in table 3.3.

Table 3.3: eGovernance & ICT Development statistics (World Bank Group, 2018)

Country:	UN eGovernance Rank:	IDI ICT Development rank:
Nigeria	143	143

Ethiopia	157	170
DR Congo	180	171
South Africa	76	92
Tanzania	134	165
Kenya	119	138
Uganda	128	152
Sudan	161	145

Based on these statistics Nigeria, South Africa, and Kenya are most suited to be selected as a case for this research. Nigeria and Kenya are especially interesting as their national identity systems remain very fragmented (World Bank Group, 2017). Both these countries are actively developing their identity systems and recent attempts have run into resistance regarding adoption and problems with inclusion. Nigeria's initiative to distribute identity numbers for their national identity system has only been registered by 20% of the population (Bloomberg, 2019). Kenya is running into similar problems (Kakah, 2019).

From these countries, Kenya is a practical choice when considering access to data. Due to existing connections of research partner 510 in this region. There are several other reasons that make Kenya an appropriate choice as a case country. For starters, the geopolitical situation in Kenya is relatively stable. While there are cases of extreme poverty and natural disaster, there is currently no large scale conflict which constricts the functioning of private sector services. Without a functioning private sector, CTPs and a more foundational identity provision is not possible. Secondly, the political structure in Kenya is not authoritarian, which potentially leaves some room for an innovation that shifts power to the user. Thirdly, there is substantial humanitarian involvement in Kenya, among which multiple humanitarian SSI initiatives. Kenya, as a progressive African country, would be among the most suitable African countries to start experimenting with this technological innovation. Therefore, the scope of this research will be focused on Kenya.

3.3 Research approach

The problem situation as described is a classic example of a technical innovation in a complex-socio technical system. Design Science Research (DSR) (Johannesson & Perjons, 2014) is chosen as a scientific approach to bridge the identified knowledge gap. DSR is suitable for this problem situation, especially because there is an identified gap between the current state of the system and a desired state of the system (Johannesson & Perjons, 2014). The current state of digital identity management creates inefficiencies due to its siloed nature and has risks embedded in its centrally controlled nature. From the perspective of HOs, the desired state is a self-sovereign form of digital identity management which allows for SIM- and mobile money registration of un(der)-documented, marginalized, and vulnerable groups. Additionally, DSR is a good research approach to deal with the wickedness of practical problems. The problem at hand is difficult or impossible to solve due to incomplete knowledge, contradictory and changing requirements, and the complex interplay between related problems (Johannesson & Perjons, 2014). DSR provides flexibility during the research process and allows for changing requirements, making it a suitable method to approach this problem.

A DSR project is distinguished from a regular design project by offering relevant results for both local practices and for the research community. Regular design projects often only contribute to local practice (Johannesson & Perjons, 2014). The contribution framework of a DSR project can be seen in figure 3.1. In the case of this project, the collaboration with 510 and the scope choice of Kenya function as a local practice. The DSR project contributes insights to 510 (local practice contribution) in doing so, important conclusions can be drawn (empirical data) to contribute to the research problem on a larger scale. The resulting design for 510 will contribute to the global self-sovereign identity space (global practice) and more general scientific insights will be deducted to contribute to the scientific body of knowledge. Generally, there are two different strategies of doing DSR. The one applied in this research project attempts to solve a specific problem in the local practice by designing an artefact in that specific context and, from that experience, distills prescriptive knowledge that can inform a general solution (Iivari, 2015). This means most of the project remains situated within the context of the local practice and generalization to a global practice occurs in later stages of the research project.

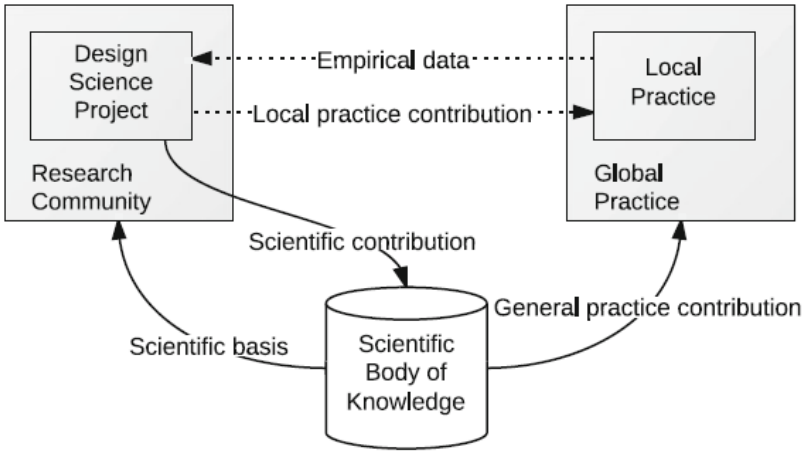

Figure 3.1: Design Science Research contribution framework

Practical problems, like the identified research problem, often require artefacts as a solution. Common to all artefacts is that they support people when they encounter problems in some practice. In the identified problem situation options for technical and institutional design artefacts have already been explored. The process of implementation and collaboration that is at the foundation of realizing a financially inclusive humanitarian self-sovereign identity system is still a large bottleneck that has been unaddressed. Therefore, this research will employ a focus on process optimization and will produce a set of principles to nurture support with for SSI as a final deliverable. These can be used in a broader process design in order to increase the likelihood of success of development collaborations. Finally, DSR is a good fit because of the collaborative nature of the research project as it allows for participatory research in the design cycle.

Some downsides can also be identified in using DSR as a research approach. A balance has to be found between scientific contribution and practical contribution. These are not always in line, this can complicate the research project. Additionally, sometimes transferability is an issue. This means

an artifact is so context-dependent that generalization to a more general scientific contribution can be complicated.

DSR projects generally consist of 5 phases (Johannesson & Perjons, 2014): Explicate Problem, Define Requirements, Design and Develop Artefact, Demonstrate Artefact, and Evaluate Artefact. These phases will be used to construct the outline of this research project. Figure 3.2 illustrates the connections and output of all these phases.

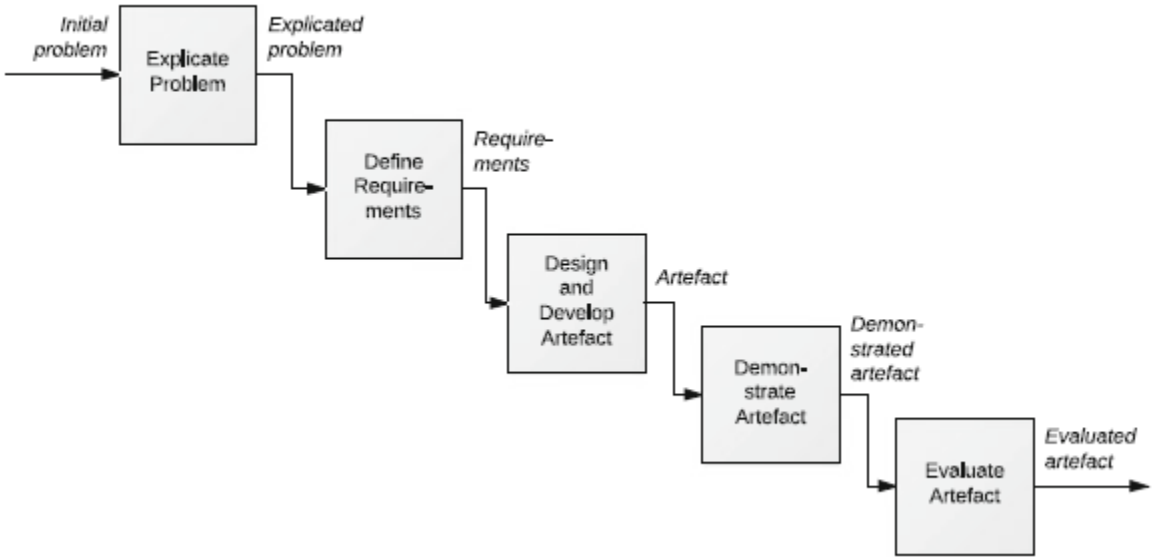

Figure 3.2: Design Science Research phases

3.4 Main research question & Sub-questions

With the problem definition, the perspective of DSR and the research scope in mind, the main research question will be formulated as:

"How can humanitarian organizations nurture support for humanitarian SSI systems as a way to facilitate in-name SIM- and Mobile money registration for un(der)documented in Kenya?"

Sub questions have been formulated that correspond to the DSR phases. However, due to the nature of the artefact and time and resources limitations of the research, the demonstration phase has been left out of the research. Together the sub-questions will form an answer to the main research question.

The following sub-questions will be used:

SQ1: "What is the socio-technical context of the Kenyan identity (registration) ecosystem?"

The first sub-question is split up in the following questions:

- "*What is SSI and what is currently known about it?"*
- *"What is the state of current and anticipated technical (digital) identity provision systems in Kenya?"*

- *"What is the institutional environment in which identity provision systems operate in Kenya?"*
- "*What is the landscape of stakeholders involved in the Kenyan identity ecosystem*

SQ2: "What are local circumstances and conditions in Kenya that drive or constrain the support of important public- and private sector stakeholders to facilitate SIM- and mobile money registration of un(der)documented through a humanitarian SSI system?"

SQ3: "What support nurturing principles can help HOs to more nurture support for in-name SIM- and mobile money registration of un(der)documented through humanitarian SSI systems in Kenya?"

SQ4: "Are the support nurturing principles of value in a humanitarian context?"

3.5 Research methodology

In this chapter, we will first determine which data is required to answer all the sub-questions. Then we will match these data requirements with corresponding research methods that have been used. Subsequently, an overview will be provided of the flow of tasks across the whole research process. This will be illustrated in a Research Flow diagram.

Data requirements

For the first sub-question, qualitative data is required which describes the situation of the identity ecosystem in Kenya. Data is required on the state of technical identity management systems, supporting institutional arrangements including broader norms and values and the current situation of stakeholders. For the second sub-question, qualitative data is required which defines what favorable and unfavorable circumstances and conditions would be for the proposed humanitarian SSI system. This data is encompassed in the experience and tacit knowledge of (humanitarian) SSI initiatives. The third sub-question requires the creative generation of different approaches, which can be aggregated into more general support nurturing principles. However, it also requires knowledge of what approach remains within the power of the humanitarian sector. Finally, in the case of the fourth sub-question, insights from an identity expert are required to evaluate the support nurturing principles.

Research methods

The first sub-question is aimed at explicating the problem situation. In this phase, the system in which the problem is present, the Kenyan identity ecosystem, needs to be described. In order to gather information on the state of technical systems and institutional context in Kenya, a desk research will be used. This desk research will dive into a mix of government reports and publications, reports from development organizations, and private sector publications. In order to understand the concept of SSI, a literature review has been performed. Furthermore, to acquire data on the stakeholder situation in Kenya, desk research has been complemented with insights from semi-structured interviews.

Subsequently, for the second sub-question, semi-structured interviews have been conducted with individuals with an affiliation to (humanitarian) SSI initiatives. For this, the network of 510 was

made available. Desk research was used to relate the findings of the interview with technology acceptance factors.

The third phase of the project builds forth on insights acquired in the semi-structured interviews and desk study to compose several approaches for humanitarian organizations that can be used to nurture support among stakeholders in Kenya. This phase concludes with a set of support nurturing principles as a design artefact.

Subsequently, a fourth phase is usually meant to demonstrate the artefact in the problem situation. Due to the nature of the design and the limited resources and time of this research project, a demonstration of the process artefact is not possible. Demonstrating the value of support nurturing principles is hard without implementing them in the real world situation.

Finally, the last phase of the research project is to evaluate the effectiveness of the artefact. This is done by assessing the usefulness, the usability, and the risks of the support nurturing principles. To do this, discussions with experts in the field were initiated through expert validation interviews.

Research flow diagram

In figure 3.3 the research flow is presented in a flow diagram. The different methods that are to be performed are linked to the different phases of DSR.

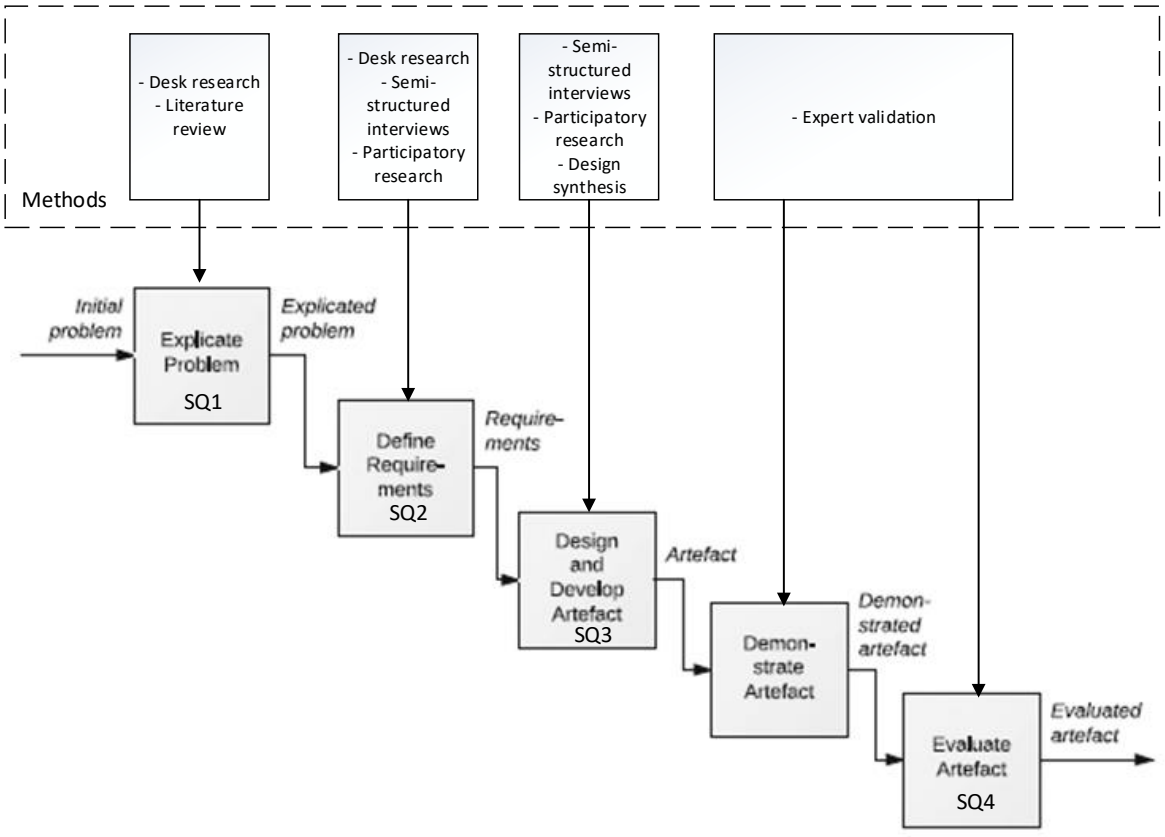

Figure 3.3: Research flow diagram

3.6 Societal and Scientific relevance

From a societal perspective, this research contributes by identifying approaches for HOs to create sufficient support among public and private stakeholders for a humanitarian SSI system that could potentially allow for more financial and social inclusion of un(der)documented. By exploring which local circumstances and conditions are beneficial and unbeneficial for the value proposition of SSI, decision-makers can potentially gain powerful tools and insights to realize collaboration between multiple actors for a more inclusive and privacy-preserving way of managing identities. In the case of Kenya, this could potentially decrease the percentage of underdocumented population, resulting in inclusion and prosperity gains. Furthermore, it could maybe give un(der)documented the opportunity for more dignity, self-procurement of necessities, and better humanitarian aid. Research results could potentially also steer decision-makers clear from humanitarian SSI as a solution in specific countries, in the case local conditions and circumstances are found to be unfavorable for the integration of financial- and mobile network-service registration in humanitarian SSI systems. Development resources can then be focused on more suitable countries.

From a scientific perspective, the following scientific contributions can be made: Firstly, research regarding SSI technology can be supplemented with more implementation focused insights. The study provides empirical results regarding the perspective of SSI in the context of a developing country from several kinds of stakeholders. Secondly, it provides some insight in to which local conditions and circumstances drive and constrain the support for inclusion focused (humanitarian) SSI systems.

4. System analysis

The first step of this research is to explicate the problem. To do that, the system of interest, being Identity provision in Kenya, needs to be explored. For this, a system analysis is conducted that answer the first sub-question: *"What is the socio-technical context of the Kenyan identity (registration) ecosystem?"*

For this section, a combination of desk research, a literature review and semi-structured interviews were used as displayed in figure 4.1. The selection procedure of the literature review can be found in Appendix B. Subsequently, the interview protocol, questions and interview summaries of the conducted semi-structured interviews can be found in Appendix C. To conclude this phase of the research, a system analysis, integrating a technical, institutional and stakeholder analysis will form the answer to the first sub-question.

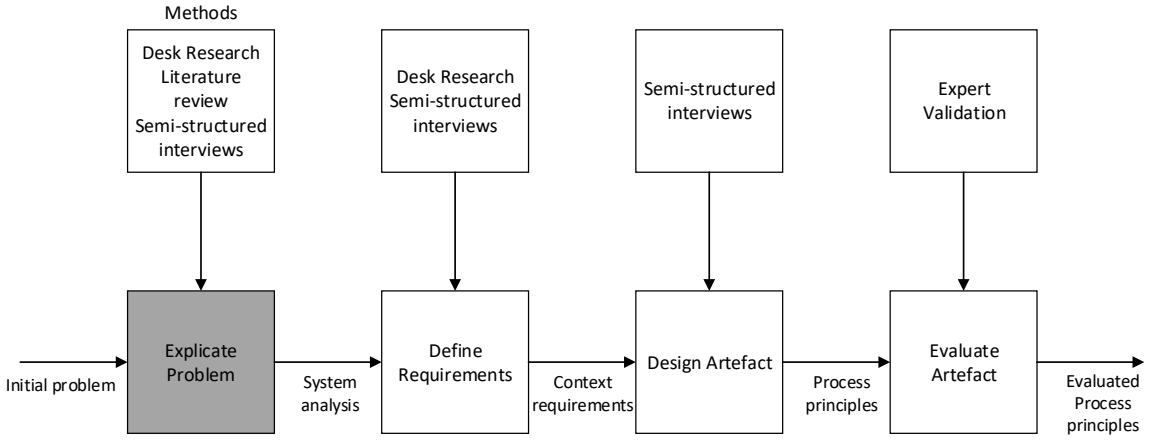

Figure 4.1: System analysis methods

System analysis is a tool widely used in the systems engineering field. The goal of a system analysis is to provide a complete view of the system-of-interest. By doing this it can provide a rigorous basis for decision making. As information systems such as identity systems are technical systems that are constantly interacting with people and organizations, not only the existing and anticipated technical systems of identity provision will be explored, but also the institutional environment and stakeholder landscape in which such systems are embedded. The approach of splitting analysis into these three parts is called the TIP approach. This will be used in this study's system analysis.

The ambition to scale humanitarian SSI systems to a more foundational purpose means it will be embedded outside of the boundaries of humanitarian aid. It will have an effect on a more broader identity ecosystem. This leads to a problematic scope for the system analysis. Encompassing the full digital identity ecosystem in Kenya in a system analysis is very challenging, due to the

infrastructural nature of identity and how deeply it is intertwined within multiple levels of a wide field of sectors. In order to do a useful analysis, to provide a base for further decision making, and to provide an explicated problem, the scoping of the system analysis is presented in figure 4.2. In this figure several leading questions indicate aspects which were focused on in the analysis in order to keep it manageable.

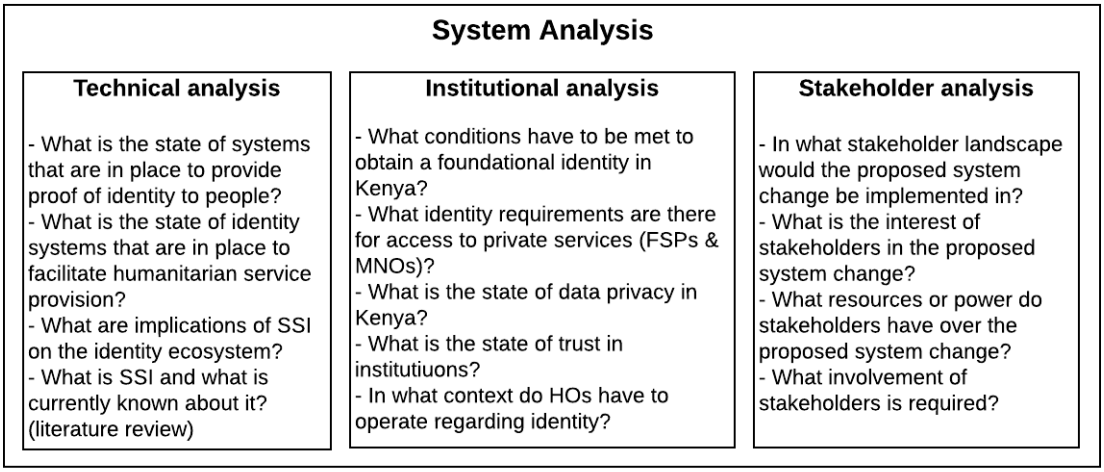

Figure 4.2: System analysis scoping

This chapter first elaborates on the results of a literature review on the concept of Self-Sovereign Identity in paragraph 4.1. Then in 4.2 the technical analysis, describing the identity systems in Kenya's identity ecosystem, are presented. Subsequently, in paragraph 4.3 the institutional analysis describes the institutional environment related to identity provision in Kenya. Paragraph 4.4 presents the current situation of stakeholders related to identity provision in Kenya. And finally, in paragraph 4.5 the findings of the system analysis are concluded.

4.1 Literature review

Before exploring the broader identity ecosystem in Kenya, it is important to understand the proposed solution. Self-Sovereign Identity is a fairly new concept, however, several publications dating back to 2016 have dived into the subject. In order to better understand the concept of SSI and to grasp the extent of current academic knowledge regarding SSI, a literature review has been conducted. For this literature review, 15 academic publications have been selected. The selection procedure is elaborated on in Appendix B. The results of the literature review provide an answer to the question: "*What is SSI and what is currently known about it?"*

4.1.1 Concept of Self-Sovereign identity

The concept of self-sovereign identity rose from the existing user-centric identity model turned into an interoperable, federated identity model. Allen (2016) laid the foundation of SSI as a concept. In his work, he defined ten principles of Self-Sovereign Identity. These principles had a focus on security, controllability, and portability as later summarized by Tobin & Reed (2016). The ten principles of SSI are displayed in table 4.1. The ten principles can be categorized into three

aspects: Firstly, the aspect of security, which implies that identity information must be kept secure. Secondly, the aspect of Controllability, which implies that the user must be in control of who can see and access their data. And finally, the aspect of portability, which implies that a user must be able to use their identity data regardless wherever they desire and without reliance on a single provider. The main difference between SSI and user-centric identity lies in this aspect of portability. User-centric identity, in contrast to SSI, can have a reliance on centralized authorities.

Table 4.1: Christopher Allen's Ten principles of Self-Sovereign Identity as summarized by Tobin & Reed (2016).

Security	Controllabillity	Portability
Protection	Existence	Interoperability
Persistence	Persistence	Transparency
Minimisation	Control	Access
	Consent	

More recently Mühle, Grüner, Gayvoronskaya, & Meinel (2018) have researched the essential components of SSI. The authors established that in the SSI model the user takes a central position. Essentially, the user is in control of his identity which consists of a collection of issued claims regarding attributes of the user. Relying parties, instead of having to trust the user on presenting accurate information can instead trust the claim-issuer. Figure 4.3 represents a highly aggregate view of SSI.

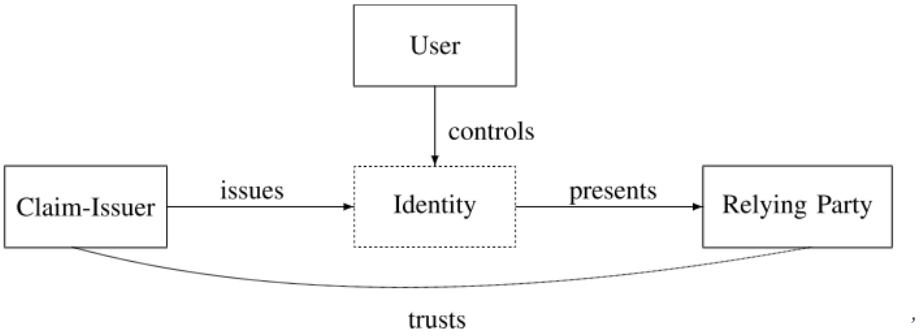

Figure 4.3: High aggregate overview of SSI according to (Mühle et al., 2018)

In order to realize such a model Mühle et al. (2018) have identified 4 essential components:

- Identification
- Authentication
- Verifiable claims
- Storage

Firstly, for the identification component, in traditional identity management systems, this is performed by a registration authority that links users to specific unique numbers (identifiers). SSI requires a way to ensure the uniqueness of identifiers without relying on such an authority.

Secondly, for the authentication component, users need a way to prove their control over the established identifier. In SSI this also should not rely on a registration authority.

The third essential component according to Mühle et al (2018) is that of verifiable claims. Claims are statements about a specific subject. Claims become verifiable claims when they are accompanied by an attestation signature by either the issuing party or a party that can attest to the correctness of the claim. SSI requires some way to link these claims and attestations to a user's identity, without using a centralized registry.

The final component, the storage of personal information, could create some type of reliance on centralized authorities. SSI systems should minimize this where possible.

4.1.2 Blockchain technology as SSI enabler

With the emerging interest and development in blockchain technology, the academic field has focused its research efforts on the potential implications blockchain technology can have for SSI.

Publications such as Van Wingerde (2017), van Bokkem, Hageman, Koning, Nguyen, & Zarin (2019) have evaluated to what extent blockchain infrastructure can allow for SSI. This research has focused on evaluating the potential of blockchain for Christopher Allen's ten principles of SSI. Mühle et al. (2018) describe the potential of blockchain in replacing the registration authority in classic identity management. Blockchain replaces this registration authority with DLT. This blockchain function is called the identifier registry. Here the pairing of identification and authentication is maintained (Mühle et al., 2018). The Blockchain identity registry can link identification with authentication without relying on a trusted registration party. By utilizing Public-Key-Infrastructure (PKI) users have a way to prove the ownership over an identifier and to verify the validity of other parties when interacting with them.

Research also evaluates the characteristics of blockchain infrastructure with existing data regulations such as the GDPR. In particular, research suggests that the GDPR's "right to be forgotten" would be problematic to adhere to with blockchain technology. The GDPR requires users to have the ability to remove information. If this information is stored on an immutable ledger, which is designed to prevent information tampering, the removal of information is problematic as described by Baars (2016), van Wingerde (2017), and Dunphy & Petitcolas (2018).

Additionally, several technical issues arise with the use of blockchain. A commonly identified issue with blockchain infrastructure is the issue of key recovery (Dunphy & Petitcolas, 2018). Increasing the sovereignty and control for end-users over their identity is combined with the increase of responsibility. But users are prone to human error, which could lead to the loss of control over their identity if for example their private keys are misplaced. Researchers identified the need for a failsafe, such as a key recovery method. But such a method could introduce new vulnerabilities and function creep risks.

A second technical issue has to do with limitations in scaling. Abraham (2017) identified the limited capability of storage on blockchains as a challenge. As all the data saved on a blockchain has to be distributed over a whole network, this severely limits the capacity.

The viability of blockchain technology as an enabling infrastructure for SSI systems has been extensively explored in academic literature. While several technical and legal challenges have been identified, most authors among which Van Bokkem, Hageman, Koning, Nguyen, & Zarin (2019),

conclude that blockchain technology is not explicitly required for SSI, but it is a good foundation to build on.

4.1.3 Exploring design options

Further research has focused on exploring several innovative design alternatives within the blockchain infrastructure of SSI systems. Some papers focus on the proposal of a new SSI initiative. For example, Tobin & Reed (2016) describe the architecture of their SSI initiative 'Sovrin' and explain their design choices. One other leading SSI initiative is the uPort initiative. Other authors such as Abraham (2017), Dunphy & Petitcolas (2018), and van Bokkem et al. (2019) compare different existing solutions. Several trends can be identified when looking at the designs of these SSI systems and by taking in to account the evaluation of these systems by other authors.

Most SSI designs converged to the use of public permissioned blockchain. This design has several advantages. A public blockchain infrastructure allows for transparency and interoperability. It is easy for participants to join the network. Permissioned blockchains have been found to be easier to comply with regulations then permissionless blockchains. By having a select few parties that write to the blockchain, which do not operate anonymously, it is easier to define liability. According to Stevens (2018), this makes public permissioned blockchains most suited for SSI purposes.

Additionally, the field seems to be converging to the use of decentralized identifiers (DIDs), as developed by the W3C open source initiative (W3C, 2019). Abraham (2017), Othman & Callahan (2018), Stevens (2018), Tobin & Reed (2016), and van Wingerde (2017) all solidify the use of DIDs to provide a sovereign way of establishing identifiers and fulfills the first component of identification.

DIDs are a new data structure developed in the W3C open source software community (W3C, 2019). A DID acts as a unique identifier that does not rely on record-keeping in a centralized server and which is in full control of the user. Additionally, DIDs are connected to corresponding DID-documents. DIDs can both be held private and public (Tobin, 2018). Private DIDs are most suited for citizens and other users and are kept in their method of custody. Public DIDs are published on the blockchain. This is most suited for institutions and service providers, by making their DIDs public they allow users to check if they are indeed connecting with the proper institution/service provider.

The comparison articles seem to indicate that the Sovrin platform, which utilizes DIDs, seems to currently have an advantage over its main competitor u-Port according to van Wingerde (2017) and Abraham (2017). The use of DIDs allows for complete off-chain storage of personal identity information. By only storing DIDs on-chain, compliance with the GDPRs right to be forgotten is less of an issue. This also alleviates the storage capacities of the blockchain, making scalability issues less of a challenge.

By utilizing the in blockchain and DID embedded PKI, users have a way to prove their ownership of DIDs. This is widely used in SSI designs to fulfill the authentication component.

For the verifiable claim component, the field mostly converged to the W3C standard in which a claim about a subject is accompanied by a public DID, a digital signature, and metadata describing what the claim can be used for. For every claim, a new DID can be used. This way information about users cannot be linked.

DIDs are anchored in the blockchains identity registry, this has the advantage that claims can easily be revocated (Mühle et al., 2018). By simply delinking the DID in the ledger, the claim becomes unverifiable and therefore invalid. The ledger enables network participants to have the same source of truth about which credentials are currently valid and who attested to the validity of the data inside the credential, without revealing the actual information.

For the last essential component of storage, several options can be considered. With the field's converging on the use of DIDs, personal data is preferably not stored on the ledger, but off-ledger. The most self-sovereign solution currently would be to allow users to store their information on their own devices. Other solutions would resort to cloud-storage or decentralized storage. With the option not to store personal information on the ledger, compliance with the GDPR is easier and the limited storage capacity of blockchains is also less of an issue.

Finally, for the problem of private-key loss, several design solutions have been developed. One popular solution is that of social recovery methods. This can be thought of as the distributing of "spare keys" among trusted parties such as family and friends, which when combined can regain access to a user's identity.

Design options both in technical and institutional design have been explored and compared to meet technical and institutional viability. Design solutions have been found for the earlier identified challenges. The field has mostly transitioned away from storing personal information on the blockchain.

4.1.4 SSI for inclusion

Several articles have focused on the potential of SSI to create more identity inclusion. Stevens (2018) explored SSI design for the purpose of Cash Transfer Programs. Subsequently, Meyling (2019) researched the potential of SSI CTP systems to satisfy KYC regulations. Meyling describes the potential for SSI systems adopted by various humanitarian actors to develop further into a system serving as a vehicle for foundational purposes. Finally, Wang & De Filippi (2020) also focused their research on the potential of SSI to create financial and social inclusion. In their paper, they emphasize that identity is inherently use-case dependent. A focus on interoperability and standardization is required, but a focus on tailoring deployment on use-cases and local conditions are also of importance. This is further emphasized by van Wingerde (2017) which describes several implementation challenges that arise from the fact that identity management crosses multiple domains and stakeholders. Reaching consensus among stakeholders on standards and technologies can be challenging and requires collaboration between the state, private sector, and civil society (Wolfond, 2017).

4.1.5 Sub-conclusion Literature review

In order to better understand the underlying concept of the proposed solution, a literature review has been conducted. The findings of the literature review provide an answer to the question: "*What*

is SSI and what is currently known about it?" The concept of Self-Sovereign Identity is a user-centric identity management model, in which the user remains in full control of its own data, without having to rely on a trusted authority. The concept of SSI has been clearly defined with corresponding evaluation criteria. The research field has identified blockchain technology as a potentially promising infrastructure to enable SSI. Research has focused on evaluating the capability and suitability of blockchain technology to enable SSI and concluded that blockchain technology, while not explicitly required, does currently provide the only good foundation to build on. Researchers have identified several challenges for blockchain-based SSI systems such as several technical and institutional issues. Meanwhile, several innovative SSI designs emerged. Comparing these several systems and their capabilities has been an ongoing focus for researchers. The field is converging to a set of best practices and design options that are most promising. But implementation is dependent on local conditions, the involvement of local stakeholders, and the collaborative forming of employed standards. Technically and institutionally the concept of SSI is well thought out, but currently as mentioned by (Stevens, 2018) there is a need for knowledge on processes to practically introduce this concept to an existing and unruly identity ecosystem.

4.2 Technical analysis

To understand why un(der)documented currently lack a sufficient proof of identity, it is important to understand the current state of technical systems designed for identity provision in the country. The technical analysis is focused on the following question: *"What is the state of current and anticipated technical (digital) identity provision systems in Kenya?"*.

The technical analysis is structured in the following way: Paragraph 4.2.1 describes government systems for acquiring and managing identity. Subsequently, paragraph 4.2.2 explores UN registration and identity systems. Then paragraph 4.2.3 explores how identity can be provided through humanitarian SSI systems and how it would look like when financial- and mobile network services would support registration through these SSI systems. Paragraph 4.2.4 explores implications of using SSI for the identity provision systems in the country. Finally, in paragraph 4.2.5, the technical analysis is concluded.

The technical analysis has been conducted using desk research. This was mostly done using grey literature, such as government publications, CSO publications, reports by development organizations, and local reporting by newspapers. Furthermore, the description of the situation in Kenya was further refined by discussing it during the conducted semi-structured interviews with respondents that are based in Kenya. Some of the implications of SSI on the identity ecosystem have also been refined using insights from the literature review and semi-structured interviews.

4.2.1 Identity provision systems in Kenya

The current identity ecosystem in Kenya is rather fragmented. Foundational systems such as the National ID card and functional systems have very little interoperability (Gatuyu, 2018). National ID cards contain personal data and biometrics but are often not utilized in functional areas. As a result, resources are wasted on duplicate registration across services, and Kenya has been looking at ways to create 'one true source of identity' for its citizens.

Integrated Population Registry Service (IPRS)

In figure 4.4 the current national system for registration and identification is displayed. At the top are the main data feeding components of the system (World Bank Group, 2016). The departments of civil registration, Immigration, and Refugee registration all hold records of respectively births/deaths, immigration, and refugees. The IPRS (Integrated Population Registry Service) is a centralized identity management system that tries to consolidate the data from these institutions in a single database to enable public and private entities to conduct a validation check on identity documents issued by the aforementioned institutions.

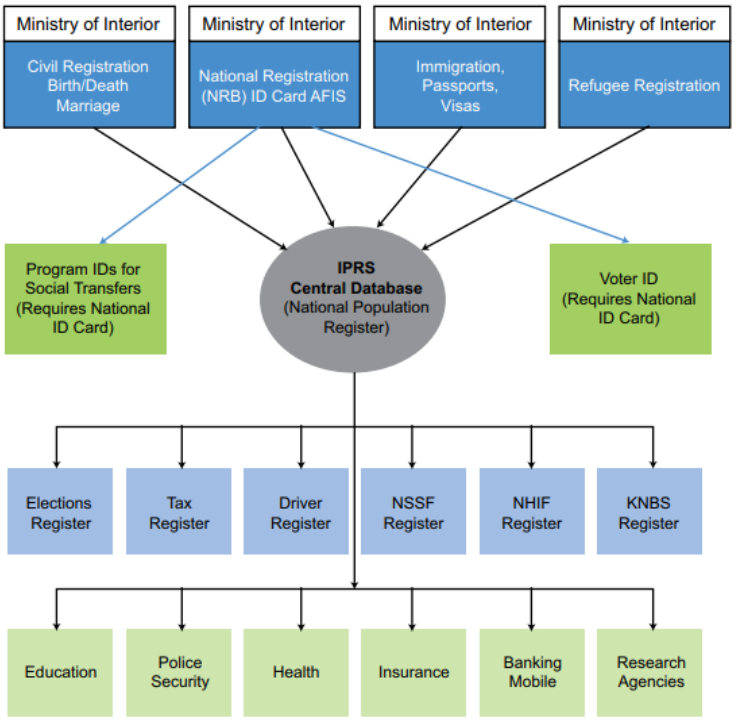

Figure 4.4: Kenya's System for Registration and Identification acquired from: (World Bank Group, 2016)

Analysis performed in 2016 shows that these systems lack interoperability (World Bank Group, 2016). The civil registration is only available in scanned PDF form. The alien and refugee registration are still paper-based and no automatic updates are being fed to the IPRS. Additionally, the biometrics collected for the national ID card is ink-based and not digitalized. Making them unusable for validation of other services. This shows an inefficient flow from information between civil registration and national ID cards.

As a result, the current system is not reliable in authenticating individuals, and public and private service providers often create their own authentication systems. The IPRS data is only available to select services and not is open for use to citizens. Social transfers and voting both require a national ID card for registration, but use their own biometric database for authentication. These systems can essentially be classified as functional identity systems. The current IPRS system can at best verify documents, but not people and not remotely (World Bank Group, 2016).

The Kenyan Single Registry System (Social protection coordination system)

To optimize social protection services that fall under the National Safety Net Program in the country, the single registry system has been developed. Several social protection services, among which some national Cash Transfer programs, consolidate their information of beneficiaries in this system. This aggregated information can be analyzed to support planning, coordination, accountability, for both program and policy-level decision-making. Bolton (Appendix C) described the single registry: "The idea behind the single registry is that all beneficiaries of humanitarian aid would be listed in one database which is controlled by the government. Through this mechanism, you would be able to control who is getting aid, who is receiving aid, when

someone receives aid and you could make sure some people don't receive aid at all". From an ethical point of view, having such a system be government-controlled creates a big potential for function creep. Furthermore, the system does not work for un(der)documented people. As the inclusion of beneficiaries is run against the IPRS to verify a national identity. Registered Kenyan nationals can receive National Safety Nets Programme Cards, supported by the information in the single registry, but this is not the case for people without a national ID card.

Ongoing digital identity developments (NIIMS)

In recent years the Kenyan government has started to roll out the National Integrated Identity Management System (NIIMS). A system intended to create and operate a national population register as a single source of information about Kenyan citizens and foreign residents in the country (Kenya National Government Communication Centre, 2019). NIIMS will collect a snapshot of the population, including biometrics, and links that information to existing functional identity databases. This will require the mass registration of all citizens, refugees, and immigrants. Registration in NIIMS will be required in order to access all public services. In January 2019 a nationwide biometric registration started to collect the information for NIIMS. During the registration, a unique number ('Huduma Namba") is assigned which was supposedly mandatory to access any services in the future.

Problems with NIIMS

The controversial government initiative has recently been challenged in court (Kakah, 2019). A cybersecurity expert testified that the system is prone to hacking. The system, which is aimed at digitizing and centralizing details of vital life events of citizens and foreigners, uses outdated technology that cannot safeguard the security of information. He pointed out that the country has taken the opposite direction from other countries which are moving towards the decentralization of information (Kakah, 2019). Data privacy and protection are the main issues with NIIMS. But some also fear for the risk the system poses for further discrimination of marginalized groups in Kenya (Open Society Justice Initiative, 2019).

Additional concerns have been brought up regarding the process in which NIIMS was initiated. The process had a lack of public participation and the use of miscellaneous amendments bill to pass substantive amendments is frowned upon (Open Society Justice Initiative, 2019). The tender process was also issued to a company in a non-transparent and non-competitive manner. Additionally, the government issued registration deadline dates in a short period. Leaving many in fear of not being able to register in the system due to a lack of mandatory documents. Bolton (Appendix C) confirms the seeming failure of Huduma Namba:" The way the data was collected was odd, 6 months before the census. There was a lot of wasted money, no one knows what is happening and everything is many years delayed."

The court has permitted the government to proceed but has enforced several limitations. Mainly the inclusion of DNA and GPS information in the system was prevented. Furthermore, the court prevented the authorities to do several things: make the registration mandatory, tying access to services to enrolment, setting a deadline for enrolment and the court prevented data sharing between agencies or to third parties.

4.2.2 UNHCR Identity provision systems

The UNHCR (United Nations High Commissioner for Refugees) is a global organization dedicated to saving lives, protecting rights, and building a better future for refugees, IDPs and stateless people. These people can register through UNHCR systems to be formally and internationally regarded as a refugee (UNHCR, 2018a). Currently, almost 500.000 persons of concern are registered through the UNHCR in Kenya.

proGres

In 2002 the UNHCR developed an IT management tool called proGres (Profile Global Registration System). ProGres is the main repository of the UNHCR for storing individuals' data. It is a centralized registration system that allows for the recording and updating of identity data in UNHCR systems (UNHCR, 2018a). However, data is stored locally, there are about 500 proGres databases world-wide. UNHCR uses the system to facilitate its international refugee registration efforts. Part of the proGres system is BIMS (Biometric Identity Management System). Refugees, IDP's and stateless people can register for a UNHCR certificate by giving up biometric information.

PRIMES

The UNHCR released the PRIMES (Population Registration and Identity Management Ecosystem) system in 2018. Where proGres was just a registration system, PRIMES is a more complete identity management ecosystem. It encompasses the proGres system and other technical modules. This includes validation or authentication of identity (based on available evidence and interaction with UNHCR over time) to governments or service providers. As such it is a complete centralized identity management system. PRIMES also consolidates all UNHCR data in a single database and is interoperable with IT systems used by governments and partner organizations such as WFP and UNICEF (UNHCR, 2018a) to enhance their ability to deliver services.

4.2.3 Humanitarian Self-Sovereign Identity provision

Multiple (international) HOs have extensive targeting and registration efforts in the country. These procedures also include the registration of un(der)documented. This is enabled through the high capacity of on-the-ground staffing available to HOs. During registration personal information is collected, this is often accompanied with geographical information, need assessments, and sometimes biometrics. At present, most HOs keep their own records of their collected information to themselves. Limiting the options for un(der)documented people severely, as they can only request aid programs from institutions which they were physically verified and registered with. This indicates both a sector-wide inefficiency due to which targeting and registration costs in the humanitarian sector are unnecessarily high, but also a major inconvenience for applicants of humanitarian aid.

Simply sharing the registration information of beneficiaries between HOs would alleviate this inefficiency, however, this is held back due to two main reasons: Firstly, contrary to expectations, HOs are extremely competitive. As HOs compete for the same pool of sponsoring, every competitive advantage is seized. Secondly, due to privacy considerations, HOs are reservedly in sharing beneficiary information. Especially due to risks of function creep. Moving beneficiary data inherently creates a risk of the information getting into the hands of a malicious entity. Due to

these two reasons, beneficiary data was not shared between HOs, until recently. Several humanitarian initiatives have emerged which use SSI as a solution to share beneficiary data in an accountable, efficient, and responsible way.

Functional Humanitarian SSI systems (current system)

"121" (pronounced one-to-one) is an example of one of those systems. 121 is a humanitarian aid delivery mechanism that has been developed in an open collaboration effort between NGOs, the private sector, the open-source community, research institutes, and government actors. 121 is an open-source digital identity system with the purpose of facilitating the targeting and registration of beneficiaries for cash transfer programs. Because of the current restriction in supported use-cases of the system, in its current state, it can be classified as a functional self-sovereign identity system.

Multiple initiatives like 121 have emerged in the humanitarian sector which aim to solve the sector-wide inefficiency created by parallel targeting and registration efforts. By leveraging blockchain technology and by using W3C's standard for "DIDs" (Decentralized Identifiers), the system allows potential beneficiaries to register their identity once at a local humanitarian aid worker and selectively allow a range of HOs to remotely validate their identity through the 121 system. Figure 4.5 shows a simplified representation of the 121 system and similar humanitarian SSI systems in their current form as functional identity systems.

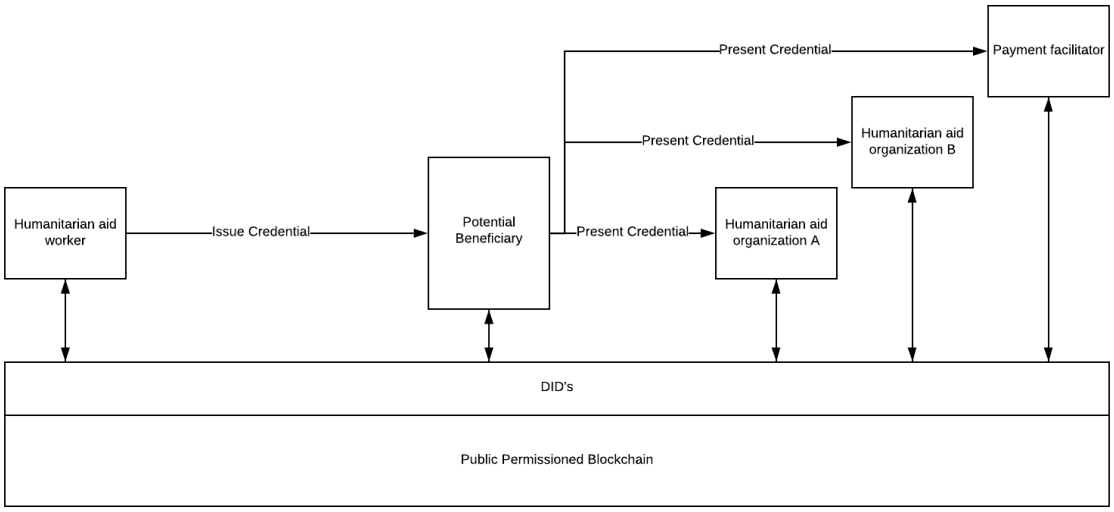

Figure 4.5: Overview of functional humanitarian SSI system

These SSI systems allow users to register once at a locally situated humanitarian aid worker and have personal information converted to digital credentials. These credentials are verifiable claims that the registrating institute makes about the identity of the potential beneficiary. The user can present these claims to other HOs that are participating in the system to apply for a variety of aid programs. Using the blockchain layer, HOs can verify if the presented claims were signed by one of their trusted partners. If the potential beneficiary complies with the inclusion requirements for a cash transfer program, a payment facilitator can request certain credentials to set up a cash

transfer method between a humanitarian organization and a beneficiary. Historically, cash in envelopes has been the transaction method of choice. However, due to accountability and accessibility issues, HOs are experimenting with alternative payment methods. This would most likely mean that local private services would handle the payment facilitation. Currently, in 121 pilots, experiments have started where payment is facilitated through special withdrawal-only mobile money accounts which are linked to specially issued non-functional SIM cards. While this does enable payment facilitation for humanitarian aid, it does not improve the efficiency of information distribution and the self-procurement of necessities.

Foundational Humanitarian SSI systems (desired system)

HOs would like to collaboratively scale and develop these functional SSI systems towards a more foundational purpose. From the perspective of HOs, these functional Self-Sovereign Identities, which are already designed to serve un(der)documented and vulnerable people, could be expanded beyond their current use-case in order to create social and financial inclusion. In particular, HOs are most interested in enabling un(der)documented to gain access to unrestricted SIM cards and mobile money accounts. These services would allow HOs to directly distribute information to un(der)documented people in case of disaster or crisis and would allow for remote payment facilitation of Cash Transfer Programs. Besides, it would allow CTP beneficiaries to self-procure their own necessities more easily.

A simplified overview of such a system where humanitarian credentials are supported for this purpose is displayed in figure 4.6.

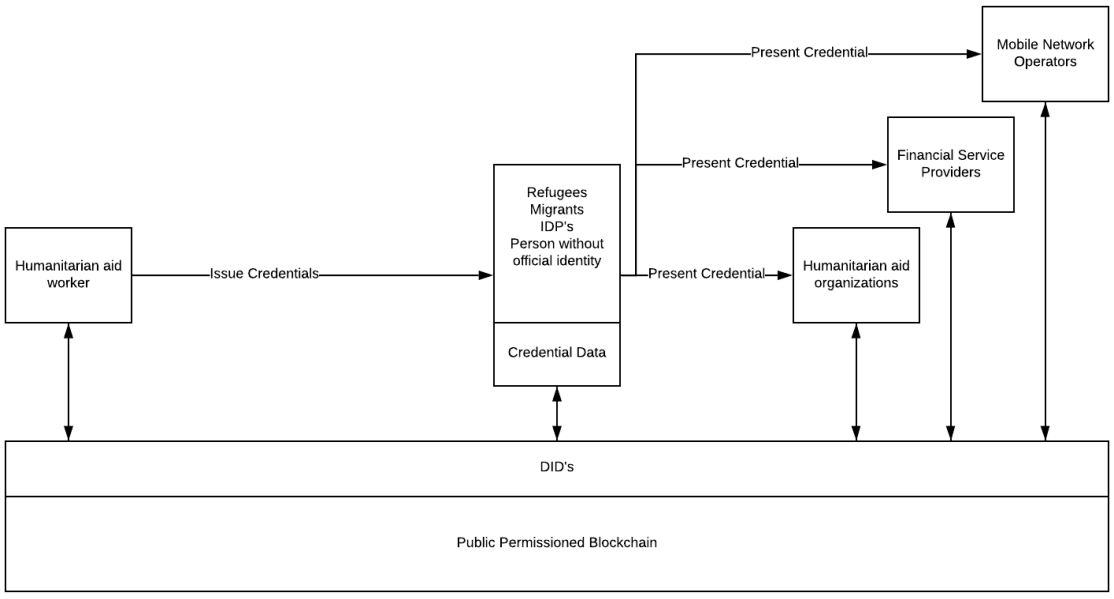

Figure 4.6: Overview of foundational humanitarian SSI system

In such a system, applicants can approach a locally situated humanitarian aid worker that registers the user. Subsequently, the humanitarian aid worker converts the personal information to digital credentials. These credentials are verifiable claims that the registrating institute makes about the identity of the user. The user can present these claims to other participating HOs to apply for a variety of aid programs. Upon acceptance of one of these aid programs, a beneficiary can use the verifiable claims issued by trusted HOs as a proof of identity to remotely meet onboarding requirements of MNOs and FSPs. Through the blockchain layer, MNOs and FSPs are able to verify that the provided application information is indeed issued by a trusted HO. This would however still require a special KYC exemption or specific humanitarian KYC standards in which HOs take up part of the KYC responsibility. Through these services, the beneficiary would gain access to a SIM card. Using a cellphone or special handsets distributed across merchants, users would be able to access their mobile money account to receive and spend aid money and stay accessible and reachable for HOs.

4.2.4 SSI technology implications on identity ecosystem

Scaling the humanitarian SSI systems beyond their current function means that additional stakeholders will be exposed to the technical components of SSI. During the literature review in chapter 4.1, the most important components of current SSI systems were identified. Important implications of these technical components are explored in the next paragraphs.

DID implications

The use of DIDs in the identity ecosystem has several implications. DIDs will require service providers to shift away from traditional identifiers. There are two important differences between DIDs and traditional identifiers. Where for traditional identifiers unique numbers are distributed to users through an external authority to enable identification, DIDs can realize this without a trusted authority. Secondly, in DID based SSI systems anonymity and more importantly pairwise pseudonymity are built-in. If a service provider just has a DID, the identity of the holder cannot be one-sidedly retrieved. In addition to this, users can use multiple DIDs, one for every interaction or relation. This aspect of pairwise pseudonymity together with the lack of a central authority makes it hard to link data together across services. Mapping user behavior and composing commercial profiles such as credit risk profiles is much more difficult. According to Stevens (Appendix C): “SSI is especially difficult to accept if your business model entirely depends on the analysis of personal data and third-party tracking of information.” This thought is adduced by van der Veen (Appendix C) which describes that a proper SSI implementation and regulation would make it more difficult for one party to hold the majority of data.

Verifiable claim implications

Credentials issued in these systems take the form of verifiable claims. In traditional systems, every service provider would need to collect and verify personal information in their own registration process. Introducing verifiable claims has 3 important implications. Firstly, it allows users to use the registration information submitted at one service provider to comply with access requirements for a second service. For relying parties this portability introduces efficiency benefits according to Stevens, Bolton, and van der Veen (Appendix C

). Duplicate registration efforts can be prevented. Secondly, according to Lamers (Appendix C), relying parties have a way to verify the authenticity of the information in the claim remotely. Currently, relying parties need to confirm the information themselves or cross-reference the information with the IPRS. With verifiable claims, relying parties can verify the authenticity of the credential and who issued it. Additionally, users can restrict the validity duration and designate the use-cases of verifiable claims. Thirdly, verifiable claims are user-owned. Theoretically, users can prove their credentials for every interaction. This would, according to Stevens (Appendix C) allow relying parties to reduce the liability of data governance responsibilities. For humanitarian organizations, this is especially interesting, as vulnerable personal data does not have to be stored and secured. Relying parties can alleviate themselves from responsibilities and reduce the risk that comes with governing large datasets and focus on their core business. Verifiable claims would cause an increase in efficiency and a shift of control from national authorities and relying parties to the users.

Blockchain layer implications

Introducing distributed ledger technology to replace a registration authority has several implications for the identity ecosystem. When implementing a public permissioned blockchain, which currently looks to be the best choice of blockchain infrastructure for identity purposes, there are three main changes compared to centralized identity systems. Firstly, DLT essentially replaces a central registration authority, this introduces an aspect of decentralization. Because changes in the ledger rely on a process of network consensus, changes can never be one-sidedly imposed by a single network node. Due to the validation of information of multiple network participants, the legitimacy of information can be secured. Secondly, making illegitimate changes to information in the blockchain is difficult. Due to the chaining of transaction blocks, a piece of information cannot be changed without having to reconstruct every transaction block that comes after it, information in a blockchain can be deemed immutable. Finally, blockchain provides transparency. Every participant can see all transactions of information (DIDs). The introduction of these three aspects is essential to rebalance the control of power within the system. It is essentially a very democratic system, where new changes in information have to be validated by network participants, one-sidedly changing information is not possible and full transparency is available to all network participant actions. Depending on the network participant composition, this greatly reduces the potential for function creep.

4.2.5 Sub-conclusion Technical Analysis

As part of the system analysis, the technical analysis provides an answer to the following question: *"What is the state of current and anticipated technical (digital) identity provision systems in Kenya?".*

In summary, based on the technical analysis, the following conclusions are drawn regarding the state of current and anticipated technical (digital) identity provision systems in the country:

- Kenya's identity system is heavily fragmented and information is essentially stored in siloes due to a lack of a truly foundational identity. There is still a high percentage (18%) of undocumented people in the country.

- The current digital identity system (IPRS) fails to consolidate the information of persons into a single digital file, due to a lack of interoperability between systems. It is not fit to provide (remote) verification and authentication of persons. At present, it can only be used to verify state-issued documents, such as the national ID card.
- The new efforts of the Kenyan government to deploy a system aimed at centralizing and consolidating all identity data (NIIMS) has raised a lot of controversies, is deemed unconstitutional, and lacks in both transparency and security. The development has come to a standstill, with no announcements or clarity of future plans.
- There is some government initiative to coordinate Humanitarian Aid through the Kenyan Single Registry system. National social protection programs that run through the Kenyan single registry, however, currently exclude un(der)documented people, as it requires verification of a state-issued credential against the IPRS. As a result, un(der)documented people are excluded from government facilitated cash transfer programs in the country.
- There are UN-facilitated identity systems available in the country. ProGres is the UNHCR's global population registry in which un(der)documented can be registered through biometrics. These systems support the local government efforts of refugee- and asylum seeker registration. Furthermore, PRIMES expanded beyond a registration-only system to a centralized identity management system. The UNHCR aims to provide verification and authentication of refugee identity, on the basis of available evidence and interaction with UNHCR over time, for government institutions and service providers. However, the UNHCR refugee mandate certificate is not recognized as sufficient for access to services.
- Humanitarian Organizations all individually collect and keep identity profiles on their beneficiaries. These include personal information, geographical information, need assessment information, and sometimes biometrics. This also includes information on un(der)documented people.
- In order to reduce targeting and registration costs, reduce the risk of data sharing, and to improve convenience for applicants of CTPs, humanitarian SSI systems have emerged. These systems allow users to carry their identity records across different HOs in a verifiable and safe way. HOs can essentially trust on the accredited credentials of partner HOs in their targeting and registration process.
- HOs are looking to use private-sector solutions for payment facilitation as a replacement for cash envelopes. Currently, in the pilots of the 121 system, solutions such as limited functionality mobile money accounts are explored. However, this is currently only for payment facilitation purposes, not registered in the name of the beneficiary, and for a limited time.
- While there are humanitarian systems in place to provide un(der)documented with a form of interoperable identity records, currently these systems are limited to a functional purpose as these identities are not recognized by public or private service providers. HOs, see opportunities to leverage these identity profiles in humanitarian SSI systems to allow un(der)documented to gain access to financial- and mobile network services. In particular unrestricted SIM cards and mobile money accounts.

- Relying on an SSI for service registration purposes would have several important implications. Firstly, due to built-in aspects of pseudonymity and anonymity, linking user behavior across different services is more difficult. It has privacy-enhancing effects built-in, making it more difficult for parties to hold a majority of data. Secondly, it would allow users to carry over information from one institution to the other. Thus, improving registration efficiency and allowing for remote registration and authentication. Additionally, it shifts the liability of data governance responsibility from service provider to the user. Thirdly, the blockchain layer rebalances the control of power over the identity management system. Due to the distributed nature, transparency, and consensus mechanism, changes in the system are established in a democratic way. One-sidedly changing information by a single entity is more difficult. This prevents the risk of function creep.

4.3 Institutional analysis

The institutional analysis is focused on identifying formal and informal institutions that shape and condition what actors can do, should and should not do within the identity ecosystem of Kenya. Formal institutions such as laws and regulations play a role in this, but informal institutions such as public norms and values do too. The institutional analysis is aimed at the following question: *"What is the institutional environment in which identity provision systems operate in Kenya?"*.

The institutional analysis is structured as follows: In paragraph 4.3.1 regulations regarding currently recognized forms of identity in Kenya are described. Subsequently, paragraph 4.3.2 explores which regulations limit private service provision. Thirdly, paragraph 4.3.3 explores how identity data should be protected in Kenya. Then paragraph 4.3.4 describes the trust in institutions. Paragraph 4.3.5 describes the institutional context within which HOs have to operate. Finally, in paragraph 4.3.6 the institutional analysis is concluded.

The institutional analysis is conducted through desk research. Consulted literature includes legislation publications, civil society reports, reports by international privacy and development organizations. This view of the institutional environment has been supplemented with insights from a locally based respondent during semi-structured interviews.

4.3.1 Identity provision in Kenya

Kenyan citizenship

State identity provision in Kenya is based on ancestry. Kenyan citizenship is rooted in Article 14.1 of the Kenyan constitution. This article states that ″a person is a citizen by birth if on the day of the person's birth, whether or not the person is born in Kenya, either the mother or father of the person is a citizen″.

The procedure and framework for registration are defined in the Registration of Persons Act. According to this act, people with Kenyan citizenship that reach the age of 18 should present themselves with the described information to a registration officer. This has proven to not always be a reliable way of establishing citizenship. According to Bolton (Appendix C):" People that currently do not have access to an identity is actually for a reason. Either they are officially denied one because they are not seen as desirable or because there is some sort of cost boundary or burden of evidence that can't be met by that individual. "

Not being able to meet a burden of evidence has been a problem in the country. As in past generations, national ID cards were not yet being issued, resulting in some older Kenyans now lacking identity documentation. This complicates the application procedure for citizenship considerably for their descendants. This is especially the case in border countries, where many births are to parents without ID cards and therefore undetermined citizenship can be the result (World Bank Group, 2016). Specific tribes such as the Shona, which came into Kenya before independence in 1963 have been deprived of nationality as they are unable to prove their origin formally or obtain birth and identification documents (KHRC, 2019). These groups are unrightfully being forced to be stateless persons.

Unfortunately, it also seems to be the case that some people are being denied an identity because they are seen as undesirable. According to a study of the KNCHR, the general policy and legal framework for registration of persons are not always applied equally. In particular, there have been cases where groups of Nubians, Kenyan Somalis, and Kenyan Arabs were exposed to stricter rules of registration (KNCHR, 2007). These vetting procedures are a result of the increased threat of terrorism, but the effectiveness to prevent terrorism is controversial. CSOs argue that the administrative and legislative efforts that are meant to stop illegitimate persons from getting citizenship are being used to prevent legitimate citizens from getting registered and allow illegal persons a way through (KHRC, 2019). Women can also experience difficulty with obtaining official identity documents (KHRC, 2019). There are plenty of cases were women had to deal with exploitative/predatory behavior or struggle with long application processes.

Finally, as there are still plenty of cases of extreme poverty in Kenya (36.1% of the population earns under the international poverty line of $1.90 per day), there are people for which the $1 fee for a renewal is a cost boundary preventing them from gaining an identity.

Alien and Refugee registration

Refugee and asylum seeker registration in Kenya is categorized as being joint-led in the report of the GSMA (2017). This means that it is a joint effort between the host government and humanitarian agencies. UNHCR provides support to the government's registration procedures. Refugee registration is being done by the DIS (Department of immigration services) and the RAS (Refugee Affairs Secretariat), under the supervision of the MoI. Refugees can acquire Alien cards which are needed as proof for the leave to remain, legal identity, dealing with police, accessing essential services and charities, obtaining resettlement permits, and registering births. Since 2017 however, the issuance and renewal of alien cards have halted. Ongoing immigration and terrorism issues are most likely the reason that the DIS has stopped the issuance of alien-cards to refugees (IHRC & NRC, 2017). This is a big problem for refugees with expiring alien-cards, new refugees, and refugees that lost their documentation.

UNHCR registration

If states refuse to issue people of concern with identity documentation, the only other option for un(der)documented people currently is registration by the UNHCR. The UNHCR issues international refugee identity certificates through a process of biometric registration. However, this certificate does not provide any access to services in the private or public sector of Kenya. As confirmed by Bolton (Appendix C) "I think in Kenya, they only recognize state-issued credentials or RAS issued alien cards". Humanitarian agencies' ID's are thus currently not recognized in the country. The UNHCR has the international mandate on identity provision for refugees, IDPs, and stateless people. The recognition of its ID is different from country to country.

4.3.2 KYC/AML requirements and SIM card registration

Ongoing political unrest in surrounding regions, especially in Somalia, has led to a continuous inflow of immigrants in recent years. This has led to controversy in the country and the emergence of political debate regarding immigration issues. The increasing threat of terrorism seemingly originating from these countries has only increased the tension. Al-Shabaab, an affiliate of Al-Qaeda has especially wreaked terror in the northern part of Kenya. Among others, schools, police

stations, and communication infrastructure have been the target of deadly attacks (Achuka, 2020). Fear of allowing terrorists to enter the country under false pretenses and terrorism financing has influenced the country's perspective of supporting refugees and is a motivation for the government to further maintain or increase their control in identity systems (International Telecommunication Union, 2016). This has also led to several private and public service restrictions over the years.

The implementation of the Anti-Money Laundering (AML) Act in Kenya in 2008 was meant to further strengthen the Kenyan financial system against criminal activities (Arasa, 2015). To achieve this, appropriate systems were established by institutions to ensure the prevention of money laundering and terrorism financing (ibid). Therefore, according to Njoroge-Kibe & Kageni (2019) and Arasa (2015), financial institutions are required to maintain compliance programs.

They list the following required elements of such a program for the Board of Directors of a banking institution operating in Kenya:

- The bank must obtain, maintain, and ensure proper identification of prospective customers wanting to open an account or make a transition directly or through a proxy.
- They must maintain records regarding the sources of funds and details of transactions for a minimum of seven years.
- They must regularly train staff in the prevention and detection of money laundering and the identification of transactions that are out of ordinary.
- Suspicious transactions or activities (such as attempts to cover the true identity of customers or the ownership of assets) must be reported to the Central Bank of Kenya.
- They must establish internal control measures to assist the prevention of money laundering.
- Opening or maintaining anonymous accounts or accounts registered under fictitious names is prohibited.
- They must monitor their provision of designated services and they, therefore, must implement KYC systems, transaction monitoring, and customer due diligence.

The Central Bank of Kenya (CBK) and the Financial Intelligence Unit (FRC) are the country's institutions in charge of overseeing KYC (Know Your Customer) and AML regulation (Meyling, 2019). Through these public organizations, the state can define which services need to comply with customer due diligence regulations. More specifically, the state can define which services require verification against state-issued credentials such as the national ID.

Due to the increasing threat of terrorism, the state has been seeking to obstruct the ability of extremists and criminals to use cell phones. As a result, in 2015 a SIM card registration act has been included in the information and communications regulations (Communications Authority of Kenya, 2015). SIM card registration now requires a national ID upon registration. Similar requirements have been set for mobile banking and mobile money (International Telecommunication Union, 2016). For these services, validation with the IPRS is required. The government controls the blacklists of individuals that are to be excluded from these services. The state has both the control over deciding which services require state-issued credentials and the control over verifying these credentials (Caribou Digital, 2019).

4.3.3 Data protection regulations

Currently, Kenya does not have any active data protection laws or a supervising authority for data protection (Open Society Justice Initiative, 2019). A new data protection bill has recently been signed by the president, but it is still unclear when this goes in to effect. The new NIIMS system allows the government to collect more personal information, including DNA samples, biometric data like fingerprints and retinal scans, and GPS information. This has recently been effectuated with amendments to the Registration of Persons Act. The government claims this is for enhanced security, but many believe constitutional privacy rights to be violated. This cannot be determined due to a lack of a legal framework. The recently signed data protection bill follows the same key principles as Europe's GDPR, but the proposed amendments to the Registration of Persons Act will overrule such a bill. As stated by respectively van der Veen and Bolton (Appendix C), both involved in a functional SSI pilot in Kenya, "the new data protection bill in Kenya took out some critical parts of the GDPR. Especially those parts which require the government to change their way of handling data" and "the agenda still seems to be: gather information, hoard and don't share.". Difficulty in the realization of the data protection bill can be found in the government's premise that they have the authority to collect all information and the resulting quest to collect population data (KHRC, 2019).

Non-transparent Security Services

Intelligence agencies have become increasingly active in their attempts to guarantee safety and security. These activities take place behind closed doors, but several reports indicate that security services exploit their control over personal information in their quest to counteract terrorism. The National Intelligence Service (NIS) operates without any form of oversight (Privacy International, 2017b). While allegations have never been legally pursued, reports indicate that security services partake in identity vetting procedures for groups related to terrorism risk (ibid.). Additionally, security services are alleged of unrightfully accessing identification and communication information owned by telecommunication companies (ibid.).

Public- and Private sector Data misconduct

More controversy regarding the abuse of personal data in Kenya has come to light recently due to developments in the legal case against UK based Cambridge Analytica. Company executives and other employees have revealed that the data analytics firm has been involved in the 2013 and 2017 Kenyan elections (Moore, 2018). During these campaigns, Cambridge Analytica seemingly supported president Kenyatta's party in the targeted advertisement, the composing of speeches, and the establishing of a political platform. They abused personal data, unrightfully obtained through Facebook and surveys, to create accurate voter profiles. This information was used to spread divisive propaganda, raising ethnic enmity. Several people have received targeted text messages with political propaganda. This suggests that the personal information of individuals across voter registration, social media, and telephone numbers were independently linked (Moore, 2018).

The private sector also has instances were personal data is being abused. This has especially been the case in the digital- credit and lending sector, which has gone through a rapid expansion in the past decade. The sector has outpaced regulatory development (Gwer, Odero, & Totolo, 2019).

More on this in the stakeholder analysis chapter. In 2018 the ministry of Finance submitted a draft bill for the regulation of smaller credit providers that currently are unregulated. This was mainly due to concerns over consumer privacy.

4.3.4 Trust in institutions

The government has the official mandate in Kenya to provide identity to its citizens, but it seems that increasingly more citizens are starting to doubt the government's ability to do so. The reliability of the Kenyan government is also somewhat put in to question on an international level. This indicates that even when a well-functioning foundational government identity system would be realized, there will be a group of individuals that will exclude themselves willingly.

Decreasing trust in government

As a result of cases of data abuse, identity exclusion, and malpractices in the Huduma Namba process, the trust of Kenyans in government institutions has decreased. Especially when the personal information of individuals is involved. Kenyan citizens are yet to get to the level of trust to allow the government to collect and keep such personal data (Kenya Human Rights Commission, 2019). This is also confirmed by Bolton (Appendix C), 510's Kenya country lead, which states:" People in Kenya don't trust the new government Huduma Namba Initiative or at least there is a large portion of the population who do not. There are a lot of rumors of corruption or issues with the facilitation." During the semi-structured interviews, it became clear that for some people the lack of trust in government is enough reason to exclude themselves from government identity systems all together. Internationally the reputation of the Kenyan government also leaves room for improvement. On the Corruption Perception Index 2019, Kenya ranked 137 among the 180 countries. The score of 28 (0 being highly corrupt and 100 being very clean), which is established based on nine independent information sources, indicates that unfortunately Kenya is perceived internationally to suffer from a significant amount of corruption (Transparency International, 2020).

Conflicts of interest between public- and private sector

In late 2019 discussions have emerged around potential conflicts of interest among government officials also holding positions in the private sector. President Kenyatta, in his war against corruption, has put several public officers on notice over conflict of interest (Gaitho, 2019). A stronger Conflict of Interest Bill has also been drafted to replace the existing Public Officers Ethics Act of 2003. This has sparked political conversations in which the interests of the president himself are also debated. The Kenyatta family has several business interests which will be further explained in the stakeholder analysis. Bolton (Appendix C) can confirm at least some entanglement of interest from a formal side, with the government stake in leading MNO Safaricom.

4.3.5 Humanitarian mandate & data protection responsibility

Humanitarian aid organizations have to abide by their specific mandate. A set of overarching humanitarian principles can be found. The most important principles are that of Humanity, Neutrality, Impartiality, and Independence (Greenwood, Howarth, Escudero Poole, Raymond, & Scarnecchia, 2017). These principles provide the foundation for humanitarian action. This means the purpose of humanitarian action is always to protect life and health and ensure respect for human beings. Humanitarian actors must not take sides in hostilities or engage in controversies of a

political, racial, religious, or ideological nature. Subsequently, humanitarian action must be carried out on the basis of need alone, giving priority to the most urgent cases of distress and making no distinctions on the basis of nationality, race, gender, religious belief, class or political opinions. And finally, humanitarian action must be autonomous from the political, economic, military, or other objectives that any actor may hold with regard to areas where humanitarian action is being implemented.

With the increased role of information and ICT systems in humanitarian action new best practices regarding data protection and responsibility, guidelines have been established. For beneficiaries, several rights can be defined that humanitarian organizations should adhere to (Greenwood et al., 2017):

- The right to Information
- The right to Protection
- The right to Privacy and Security
- The right to Data agency
- The right to Rectification and Redress

To secure these rights several principles for data responsibility have been composed. Among which: Fair and legitimate processing of data, purpose specification, necessity relevancy, and adequacy of data processing, limited retention, accuracy, confidentiality, security, transparency, data transfers, and accountability (OCHA, 2019).

Two main issues that are related to data responsibility come up with the scaling of humanitarian SSI systems to a more foundational purpose. The first issue has to do with interoperability with financial service providers. KYC obligations could require cross-checking of information against lists of designated persons established by the Kenyan national government. This process is thus partially controlled by public authorities. This gives rise to questions as to inclusion (i.e. can beneficiaries be excluded from an assistance program on the basis of a match being found) and compromises the neutrality and independence of Humanitarian Action (ICRC & Brussels Privacy Hub, 2017).

Secondly, opening a system with information on beneficiaries to third-party service providers brings challenges and risk of function creep (use of the system for other purposes than the ones originally designated) (ICRC & Brussels Privacy Hub, 2017). Identity systems are prone to pressure by various national or regional authorities to acquire the data. Purpose specification of data can therefore not always be safeguarded. The risk of the data being used for purposes such as law enforcement or border control can cause friction with the humanitarian principle of ‘do no harm’ and could potentially break the right to privacy and security of beneficiaries.

4.3.6 Sub-conclusion Institutional Analysis

As part of the system analysis, the technical analysis provides an answer to the following question: *“What is the institutional environment in which identity provision systems operate in Kenya?”*

In summary, based on the institutional analysis, the following conclusions are drawn regarding the institutional environment in the country:

- Registration of persons in Kenya suffers from unintentional exclusion. People can become un(der)documented due to a burden of evidence that can't be met by certain individuals. Secondly, to a lesser extent, some individuals are expected to be excluded due to a burden of cost. Thirdly, some individuals are willingly excluded due to a lack of trust in government identity systems.
- Over the years, the ongoing threat of terrorism and the government's premise of having the authority to collect all information has led the government to increase its control over the country's identity system. It is expected that the government will try to maintain or increase this level of control in the future.
- The increased government control is reflected in KYC/AML regulations which limit access to private sector services such as financial- and mobile network services. The national authorities control both which services require state-issued credentials and control the verification of these credentials through the IPRS and government blacklists.
- Government control is also reflected in registration procedures. This creates cases of intentional exclusion of people. Examples of this are cases of identity vetting procedures, supported by non-transparent security services without any form of oversight. Administrative and legislative efforts that are meant to stop illegitimate persons from getting citizenship are being used to prevent legitimate citizens from getting registered.
- There are national institutions in place to provide alien and refugee registration. The resulting identity documents from these procedures do provide access to private and public services. However, the issuance and renewal of documents is extremely inconsistent and often not active.
- The UNHCR provides people of concern such as refugees, IDPs, and stateless people with identity documentation. However, these documents are not recognized by public and private service providers in Kenya.
- There is a lack of active data protection regulations. While new GDPR inspired regulations have been announced, critical parts have been removed so the government does not have to change its own ways of handling data.
- To some extent, the public- and private sector abuse the lack of data protection and privacy. There have been cases of data misconduct and corruption among public institutions and major private sector organizations.
- Trust in government institutions, especially concerning the handling of personal data is low among citizens and from an international perspective there is some degree of corruption in the country.
- There are informal conflicts of interests among government officials, entangling private business interests with public legislation. Also, formally the government has stakes in major private sector organizations such as Safaricom.
- HOs have to operate within their humanitarian mandate. As HOs diverge into slightly different roles than just aid relief, for example, Humanitarian innovation, data responsibility guidelines need to be taken in to account with extra care. Adhering to national KYC/AML regulations could cause friction with neutrality and humanity principles. Additionally, HOs are wary for risks of function creep.

4.4 Stakeholder analysis

The stakeholder analysis is focused on identifying which actors are involved in or have an interest in identity provision in Kenya, including stakeholders related to SIM and mobile money services which are relying on these identities. It explores how these actors are configured, what their potential interest/ disinterest in the proposed system change is, and what resources they have. The stakeholder analysis is focused on the following question: "*What is the landscape of stakeholders involved in the Kenyan identity ecosystem?*".

The stakeholder analysis is structured as follows: Paragraph 4.4.1 identifies which stakeholders are involved in the Kenyan identity ecosystem. Then paragraph 4.4.2 describes how these stakeholders are configured. Paragraph 4.4.3 explores the power and resources available to stakeholders. Subsequently, paragraph 4.4.4 explores the interest and perspectives of stakeholders for a potential humanitarian SSI system. Then paragraph 4.4.5 explores which stakeholders should be involved in realizing the proposed humanitarian SSI system. Finally, in paragraph 4.4.6 the stakeholder analysis is concluded.

The stakeholder analysis is conducted through desk research and semi-structured interviews. Grey literature has been consulted, ranging from public- and private sector reports and development organization reports.

4.4.1 Stakeholder identification

Table 4.2 presents the groups of stakeholders that are involved in Kenya's national identity ecosystem, including service providers of SIM cards and mobile money accounts. And stakeholders that are involved with the identification procedures for national residents and un(der)documented people.

Table 4.2: Identified stakeholder groups in the Identity ecosystem

Identity ecosystem stakeholders
National Government Authorities
Local Government Authorities
Mobile Network Operators
Financial Service Providers
National Civil Society Organizations
International Identity Development Organizations & Initiatives
UN agencies
Humanitarian Organizations

4.4.2 Stakeholders configuration

In this paragraph, the composition and configuration of the previously identified stakeholder groups will be made clear for the case of Kenya. This overview will include dependencies between stakeholders and responsibilities related to the identity ecosystem. Firstly, the configuration of national stakeholders and, thereafter, international stakeholders will be elaborated on.

National stakeholders

A. Un(der)documented people

For the population of Kenya, there is a significant amount of people that lack any form of state-issued documentation, such as a national ID card or Alien card. According to World Bank Group (2018), this group consists of around 9 million people. These people are often part of vulnerable groups, such as; People in extreme poverty situations, tribes located in border regions or refugees and asylum seekers. This is reflected by data from the Hunger Safety Net Program conducted in 4 poor counties, which concluded that around 20 percent of the target households did not have one or more adults with a national ID card (World Bank Group, 2016). In Kenya, there are about 500.000 refugees and asylum seekers registered by the UNHCR. Most of these refugees and asylum seekers live in rural refugee camps, 44% in Dabaab, 40% in Kakuma, and 16% live in urban areas such as Nairobi. Furthermore, the UNHCR identified close to 18500 stateless persons.

Many of these vulnerable individuals lack any form of identity documentation. This could be because they were never incentivized to own one, the application process was too expensive or inconvenient, or their government lacked the capacity to issue identity documents to its citizens (GSMA, 2017). These people are regarded as 'undocumented'.

Furthermore, some individuals have some identity documents, but they are not enough to satisfy registration requirements in Kenya. For example, some people have birth certificates but are not eligible for national identity because they can't prove their parents' nationality and therefore do not have proof of ancestry for a national ID card. These individuals are regarded as 'under-documented'.

Some un(der)documented people, despite their lack of identity proof, find ways to bypass access requirements for SIM registration. For instance, by registering the SIM under another person's ID (GSMA, 2017). According to Ebert (Appendix C), the MNOs in the country know full well that this happens.

B. National Government authorities

The Ministry of Interior and Co-ordination of National Government (MoI) is the main institute that governs the Kenyan Identity Ecosystem. The Ministry of Information Communication and Technology (MoICT) provides support to the MoI. The MoI is the most powerful ministry in Kenya, in charge of realizing major development plans according to Kenyatta's vision (Caribou Digital, 2019). The MoICT is in charge of making plans to support Kenya's rapidly developing digital economy. The MoI has a wide range of responsibilities among which the responsibility of population registration. This means that the MoI maintains the existing IPRS system and together with the MoICT these parties form the driving force behind the newly introduced NIIMS. Furthermore, the MoI governs the entire legal identity structure through its four departments as displayed in figure 3.3. Effectively having power over Civil Birth/Death registration, National ID card registration, Immigration, and Refugee registration.

The state has been acting according to the Kenya Vision 2030 as established in 2007 (Government of the Republic of Kenya, 2007). In doing so they have attracted investment and stimulated innovation by actively developing digital communications infrastructure, by providing tax breaks for key industries and by maintaining a low regulatory environment (Caribou Digital, 2019). The

state plans to continue on this trajectory and further strengthen its digital economy. Besides, it aims to further develop e-government applications.

Other relevant national government authorities are the KYC and AML overseeing institutes. For the financial service sector, the CBK and the Financial Intelligence Unit oversee KYC compliance. For SIM registration regulations, this is the Communications Authority of Kenya. Furthermore, the NIS is involved in security surveillance services and identity vetting procedures.

C. Local Government authorities

A report from the Commonwealth Local Government Forum provides a clear overview of the local government layer in Kenya. Local authorities are divided into 47 county governments (CLGF, 2017). County governments consist of a county assembly and a county executive. County government functions are decentralized among urban and non-urban sub-counties. Counties have 14 functions which mostly provide operational support of public goods such as transport, healthcare, and others. Additionally, county governments are responsible for ensuring and coordinating the participation of communities and locations in governance at the local level and assisting communities and locations to develop the administrative capacity for the effective exercise of the functions and powers and participation in governance at the local level. Since 2017 a policy on the devolved system of Government was adopted by the national government, launching a new phase of consolidating devolution, clarifying and strengthening the roles and responsibilities of both the national and county governments. This was to further implement devolution as envisaged in the constitution. This is overseen by the Ministry of Devolution and Planning (MDP). Counties have some degree of autonomy, but the MDP assists with the coordination of intergovernmental relations and the implementation. Within the MDP a special SDG unit has been established to coordinate the implementation of sustainable development goals. Local SDG units are being formed in every county to coordinate the implementation of relevant technical matters and targets (CLGF, 2017).

D. Mobile Network operators

The mobile network business in Kenya is very successful. As of 2018, the total number of mobile service subscriptions in the country stood at 45.5 million. The biggest mobile network service provider in the country is Safaricom. The company has a market share of 65.4% (Njanja, 2018). The Kenyan government has a 35% share in the company, 35% is owned by Vodacom and 5 % is owned by Vodafone.

Airtel Kenya is the second biggest provider with a market share of 21.4%. Airtel Kenya operates as a subsidiary of Airtel Africa which is owned by Bharti Airtel. 64% of this is owned by India based Bharti Enterprises and 36% is owned by Singapore based SingTel. Telkom Kenya is the third-largest telecom provider with a market share of 8.9%. Telkom Kenya is 60% owned by private equity firm Helios and 40% owned by the Kenyan government. Rumors have re-emerged as of late 2019 regarding a planned merger between Airtel Kenya and Telkom Kenya to enable competition with the dominant Safaricom (Mukami, 2019). The company will be called Airtel-Telkom. The merger has already been approved by competition regulators. This means the competition in the mobile network sector will become even smaller.

As previously mentioned, MNOs rely on the state for the verification of state credentials. SIM card registrations have to be completed with national IDs that are authenticated against the IPRS. As such, SIM cards have come to serve as an important form of digital identity for other services (Caribou Digital, 2019). Verification of phone numbers is increasingly required to gain access to services. Additionally, more services use phone numbers for customer due diligence purposes. The government added strength to this form of identification by directing all MNOs in 2018 to suspend all unregistered SIM cards.

E. Financial service providers

The ecosystem of financial products consists of several financial products and service providers. A survey conducted by the (Central Bank of Kenya, 2019) provides an overview of the recent state of the financial systems in the country. In the report, several financial institutions are distinguished as displayed in figure 4.5.

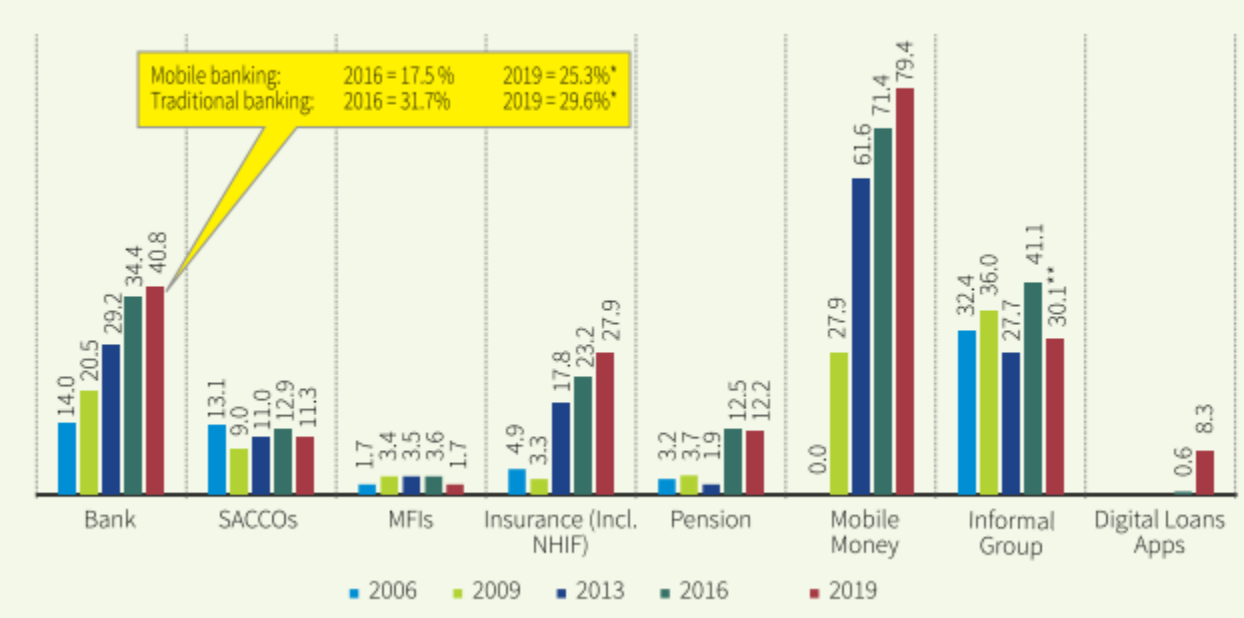

Figure 4.5: Percentage of adults relying on financial service providers (Central Bank of Kenya, 2019)

Mobile money expansion enabling financial inclusion

The figure shows a trend of increasing financial inclusion in general, but specifically in the mobile money business. Kenya has leapfrogged developments in the financial sector and is currently perceived to be the leading country concerning mobile money. This development was enabled due to the country's widespread coverage and adoption of mobile phones.

Furthermore, the report indicates a difference between rural and urban areas. Both areas have a high usage rate of mobile money providers, but banks and insurance service providers are used significantly less in rural areas compared to urban areas. This is in line with the difference in trust that the Central Bank of Kenya (2016) determined in its 2016 survey. Participants in rural areas have less trust in banks compared to urban areas.

Mobile money providers such as M-Pesa, Airtel Money, MobiKash, Orange Money, and Tangaza Pesa have been introduced in 2007 and have seen rapid growth. These services allow people to make transactions by SMS. Safaricom's M-Pesa has by far the biggest market share with estimations ranging from 65% - 85%. Airtel Telkom's Airtel Money is the second biggest provider. Mobile money services are currently the driving force of financial inclusion in the country.

Adaptation to digital credit services entangle interests

Traditional banks are also still relevant to Kenya's financial landscape. In contrast to the mobile network operator, there is more competition among banks. There is a wide variety of different banks, among others: **Commercial Bank of Africa (CBA), Kenya Commercial Bank (KCB), Equity Bank Kenya**, Barclays Bank Kenya, Standard Chartered Bank Kenya, Cooperative Bank of Kenya, Diamond Trust Bank of Kenya, National Bank of Kenya and NIC Bank.

Some banks, next to their traditional services, also partnered with mobile network operators to provide mobile banking accounts. CBA works with 'M-Shwari', KCB with 'KCB M-Pesa', Equity Bank Kenya with 'Equitel Money'. Customers can have mobile savings accounts with the banks and can receive other financial services such as digital lending. Financial service providers adapted to the changing landscape of financial services in this way. The collaborations between financial service providers and mobile network operators create entanglement of interests. Even the interests of the public sector seem to be involved in these collaborations. Apart from the earlier mentioned 35% direct government share in Safaricom, president Kenyatta's family owns a 25% share in the CBA. This means the president and state have a direct interest in the dominancy of the M-Shwari service.

MNO dominancy and algorithmic credit scoring

Safaricom's unique position of dominant network provider with the biggest user base makes it especially powerful. The leapfrog of the mobile money business is outpacing the developments in regulation (Gwer et al., 2019). Mobile network operators leverage their position of power for profit (Caribou Digital, 2019). MNOs use the data obtained from their services as a network provider in their mobile money businesses. Services such as M-Shwari categorize individuals according to credit ratings, this process is enabled by algorithmic credit scoring. These ratings are established using a combination of state-verified credentials, M-Pesa transactions, mobile phone behavior, and social media usage (Caribou Digital, 2019). The direct access to this information combined with network effects put Safaricom and M-Pesa in an even more dominant position.

Mobile money providers are not the only parties taking advantage of this lack of data regulations and algorithmic credit scoring. Digital lending apps such as Tala and Branch have emerged recently (Privacy International, 2017a). These apps use the fact that SMS is not encrypted on phones. Users can opt-in to allow the app to use the data on their phone to be eligible for a digital loan. By giving this access to the apps, algorithms are fed all M-Pesa transaction data through the SMS log, social media data, GPS data, and phone log data. Such algorithms take into account what you spend your money on, who your friends are (what their history of defaulting loans is), where you live and who you contact (Privacy International, 2017a). Analysis by Tala for example found out that people who regularly contact their parents are 4% more likely to repay their loans (Privacy International, 2017a). Based on this information, a credit rating is established which decides the

terms of the loan. This takes place in a matter of minutes, giving users instant access to loaned funds. But users are often unaware of what they are giving up.

F. National Civil Society Organizations

Civil Society Organizations (CSOs) is a broader term for non-state, not-for-profit, voluntary entities formed by people in the social sphere that manifest the will and interest of citizens, individuals, and organizations in a society. This can include community-based organizations as well as NGOs.

In Kenya, several CSOs have been involved with development of the country's identity ecosystem. Kenya National Commission on Human Rights (KNHCR) and the Kenya Human Rights Commission (KHRC) have both actively researched corruption and exclusion cases against marginalized groups and women in the process of identity registration. CSOs are generally in a position of trust among citizens, especially excluded groups. CSOs such as the Nubian Rights Forum and Namati has been filing legal proceedings against the government for human right abuses in identity registration processes. CSOs have been actively pushing back against the government when faced with human rights abuses. With the recent Huduma Namba/ NIIMS developments, CSOs have started to get more involved. Successfully preventing the government from doing several things in the rollout of NIIMS. CSOs have formed networks together such as the Coalition on Nationality, Citizenship and Statelessness Empowerment (CONCISE) and Kenya ICT Action Network (KICTANet) to discuss developments in the country's identity ecosystem and ICT systems. These networks aim to introduce more multi-stakeholder participation in the forming of identity regulations and systems. Bloggers Association of Kenya (BAKE) is another example of such a networked community in which online bloggers promote human rights and media rights. CSOs advocate the interests of citizens, marginalized groups, and stateless people.

The CSOs in Kenya have several competencies and resources, such as the ability to: conduct research, raise awareness, perform lobbying, file legal proceedings, and form public participation networks. But CSOs lack technical capabilities and knowledge and therefore often take a reactive stance (address when things go wrong) instead of more active participation in development (provide solutions) (Caribou Digital, 2019). Additionally, CSOs indicate that they have a less direct impact on government regulation compared to the private sector.

G. International Identity Development Organizations & initiatives

In recent years an international movement for better digital identity systems has emerged. A wide variety of organizations have joined this cause. These organizations believe that digital identity is a key enabler for sustainable development goals. Several international organizations have been very influential in the international push for a better digital identity. The World Bank Group has actively been contributing to this cause and it has started the ID4D (Identification for Development) initiative. ID4D is a cross-sectoral platform partnering with a wide variety of organizations providing expertise and funds. It advocates to raise awareness, directly informs countries with good practices and design options. Additionally, under the ID4D a Multi-Donor Trust Fund (MDTF) has been set up to further advance the developments of digital identity through funding. This MDTF is supported by big donor organizations such as the Bill & Melinda Gates Foundation, the UK, the Australian government, and Omidyar Network. Secondly, the GSMA (an

association of international MNOs) started an identity initiative to develop digital identity services with an optimum balance between privacy, security, and convenience. Thirdly, ID4Africa is an NGO movement that supports African nations in their development of digital identity systems for development goals and humanitarian action. Fourthly, ID2020 is a public-private partnership, with partners like Microsoft, Gavi, and Accenture, that is maximizing the potential of digital ID to improve lives.

H. United Nations agencies

Several UN agencies are also committed to improving identity in developing countries. UNICEF has been working on improving birth registration and civil registries and the UNHCR is determined to end statelessness. The high commissioner of the UNHCR has expressed his vision that every refugee should have his unique digital identity. In an early proposal by the UNHCR, an identity model is described where individual refugees have agency and control over their identity, while the UNHCR leverages its institutional weight to provide credibility of the information (UNHCR, 2018b). Currently, the UNHCR already provides documentation to refugees in countries where refugee documentation is not available from the government, in some countries it is even accepted for SIM- and mobile money registration.

I. Humanitarian organizations

HOs have the main focus of providing aid and disaster relief. However, many HOs have branched out to more development-oriented activities. This is partially done to make communities and vulnerable individuals more prepared for disaster situations and to prevent and relieve poverty. Humanitarian innovation is therefore sometimes not only aimed at improving aid delivery but also at improving local conditions to prevent the need for humanitarian intervention.

Several humanitarian organizations have developed and deployed functional SSI systems to support the registration of possible beneficiaries who want to apply for cash transfer programs in developing countries. By giving back the control and ownership of personal data to individuals, this allows users to reuse their registered credentials at other humanitarian organizations. Thus, increasing collaboration and efficiency in the sector. While data can be of value, it can also be a liability. This is especially the case for humanitarian organizations, which aim to “do no harm”. For these organizations, the registration and storing of personal information becomes a huge liability.

The World Food Program (WFP) is one of these organizations that experimented with using blockchain innovations for humanitarian aid in their program “Building blocks”. After their successful pilot, the organization discussed the vulnerability of storing beneficiary information in a central location and expressed the ambition to move to SSI to solve this issue (Genc, 2017). The IFRC expressed the same need in their collaborative blockchain pilot with the KRCS. More recently the IFRC has partnered with four Norwegian humanitarian organizations to launch the start of their project “Dignified Identities”, which aims to develop such an SSI system.

The “121” consortium, consisting of humanitarian organizations like the NLRC, development partners, academic partners, and others, has actively been developing the “121” system. This is an SSI system build for the registration of potential beneficiaries applying to cash transfer programs.

Similarly, the IFRC and KRCS are actively working on their project called "Dignified Identities in Cash programming" to leverage humanitarian data for identity provision.

Humanitarian innovation initiatives have become more prevalent over the years. Due to this, these organizations have gained expertise regarding the design of inclusive solutions. This includes development for systems in remote and poorly connected locations. As well as tuning design to ensure inclusion for difficult groups or people with a special need.

Concluding, humanitarian organizations have an interest in developing SSI systems in emerging countries to improve the efficiency and effectiveness of humanitarian aid. Currently, it is one of the few "service providers" in Kenya for which hoarding and securing personal information is a liability, due to their unique mandate. They have been actively using their resources and expertise to realize such a system.

4.4.3 Stakeholder resources and power

In this section stakeholder resources and power are identified. This elaborates on how stakeholders could contribute to realizing SIM- and mobile money registration through a humanitarian SSI system, or how they could block this initiative.

A. Un(der)documented

Un(der)documented people do not have a lot of resources or power as individuals. As end-users, they form a group that is important to start network effects, but individually they do not have a lot of power. They are generally uninformed about SSI technology. There is still low information privacy awareness when looking at the majority of people, however, in discussions with the respondents it was indicated that this is starting to shift. Many un(der)documented people use workarounds for their lack of identity, such as registering SIM cards in a friend's name. Digital literacy can be assumed to be somewhat better than average in Kenya due to the high adoption rate of mobile phones and mobile money.

B. National Government authorities

The national government authorities have a high degree of blocking power due to their mandate of (legal) identity provision. The strict KYC/AML regulations that they are currently enforcing are currently the biggest barrier for expanding a humanitarian SSI system to a more foundational nature as described by Ebert and Oliveros (Appendix C). The government is in a position where they can both decide which services require KYC compliancy and govern the KYC compliancy systems (IPRS). There has been engagement of SSI initiatives with the government and the country has a team specifically dedicated to exploring opportunities of blockchain. There is some understanding of SSI among some government individuals, but probably not on an organizational level. According to van der Veen (Appendix C) understanding of the technology is most likely still limited: "I know in Kenya there is quite a lot of blockchain piloting and testing being done. So, I would assume that also identity has been presented at several levels. And how blockchain could be used to do SSI systems. But I guess it is not a very well lived through idea. It is likely they do not have a full understanding, also not a full understanding of the current limitations". Furthermore, the powerful position of the national authorities is emphasized by Bolton (Appendix C): "The only organization that is really critically involved between the operational and

foundational identity is the government". All respondents of the semi-structured interviews (Appendix C) describe the need to get national authorities on board due to the powerful position they are in, be it due to the control over KYC or other required supporting legislation.

C. Local Government authorities

Local government authorities, due to decision making on county level, have some blocking power, but not to the degree of national authorities. However, local government authorities have local networks of organizations and citizens. They are in charge of the operation of central public locations in their counties and as such could contribute to facilitating supporting infrastructure.

D. Mobile Network Operators

MNOs are in charge of the telecommunication infrastructure in the country. This is quite an enabling/blocking power that these MNOs have, due to the technical limitations of SSI. As currently SSI systems, according to van der Veen (Appendix C), only work in online environments. Furthermore, MNOs need to be cooperating as they are ultimately in charge of SIM issuance and activation, which is also a necessity for mobile money accounts. MNOs are in direct contact with government officials. This together with the entanglement of interests of government and the MNOs in the country, likely give MNOs the ability to somewhat influence the national authorities. Finally, MNOs as a trusted organization can allow un(der)documented to build up a transaction history with the MNO. This data can be issued as a verifiable credential, which can be further leveraged to further strengthen someone's identity. As such MNOs could play a role in trust provision. Some individuals within the Kenyan MNOs are familiar with SSI as a technology, but on an organizational level, there is still a lack of understanding.

E. Financial Service Providers

Financial service providers are in a similar power position as MNOs. FSPs are ultimately in charge of issuing financial services such as mobile money accounts. Similar to MNOs, FSPs are likely an influential stakeholder in pressuring or motivating the government. FSPs are also a trusted organization that could issue verifiable credentials to further build up identity profiles over time. Some individuals within the Kenyan FSPs are familiar with SSI as a technology, but on an organizational level, there is still a lack of understanding.

F. National Civil Society Organizations

National CSOs have networks and expertise with vulnerable groups in the country. These networks could be used to distribute information with vulnerable groups. They are involved in representing the un(der)documented people who are unlawfully denied an identity. CSOs have the capacity to hold the government accountable, especially in a reactive way using legal procedures. CSOs in the country lack technical capabilities and have little understanding and insufficient information on SSI technology. CSOs have a less direct influence on government stakeholders, but they can successfully bring issues to the attention of the general public.

G. International Identity Development Organizations and initiatives

International identity development organizations and initiatives have high technical capabilities and MDTF funding to develop and advise on identity systems. Especially development organizations such as the World Bank have significant power because their resources go beyond

advisory tasks, with the ability to issue low-interest loans to governments as stated by van der Veen (Appendix C). Some of the world's leading private sector organizations contribute to these initiatives, which are focused on social innovations and in particular on digital identities.

H. United Nations agencies

The UNHCR already has a mandate aimed at identity provision and registration, specifically for refugees and asylum seekers. It is supporting and working with the government on this. UN agencies have a relatively high degree of information of un(der)documented people. The UNHCR PRISM system is already facilitating some of the identity needs for un(der)documented, for which they also record biometrics. The UN agency could therefore provide interesting credentials for end-users.

I. Humanitarian Organizations

HOs have high on the ground access in high-risk areas. They are delivering aid to un(der)documented and vulnerable people in disaster/crisis situations. HOs have extensive targeting and registration procedures, collecting identity information on these groups that other stakeholders don't have. HOs are generally trusted organizations, especially in Kenya according to some of the respondents, and thus HOs can provide social legitimacy of technical systems. They are experienced with social innovation and public participation.

4.4.4 Stakeholder perspectives and interest

In this section, the perspectives and theoretical incentives, based on the technical analysis and semi-structured interviews, of a humanitarian SSI system will be discussed for each stakeholder.

A. Un(der)documented

The proposed system would provide un(der)documented people with a way to build up their own identity record, by leveraging the trust of HOs, in a secure and privacy-friendly way. While most un(der)documented are certainly interested in any opportunity to gain access to services such as SIM cards and mobile money, they are not necessarily aware of privacy issues. Most un(der)documented people are not necessarily interested in the privacy advantages of SSI, because there is a lack of understanding of the technology and privacy awareness. According to Oliveros (Appendix C), there is also a group who are willingly excluding themselves due to privacy and security concerns. This segment of un(der)documented might be more interested in a humanitarian SSI system. However, it is likely that even these groups do not have a sufficient understanding of the technology to trust the security and privacy of SSI. Apart from that, it is still unclear if un(der)documented people are willing to control their own identity information.

B. National Government authorities

From the government's perspective, several things are interesting about a humanitarian SSI system: Stevens and Bolton (Appendix C) describe the potential of a humanitarian SSI system to provide a form of identity to un(der)documented people. This way of creating inclusion could potentially be an incentive for government stakeholders, especially due to the possible increase in GPD and collectible taxes. Furthermore, capacity support in identification and registration is stated by van der Veen and Stevens (Appendix C) as an important incentive for national authorities to support a humanitarian SSI system. Especially in refugee camps, which have a high concentration of people,

HOs have the professional capacity that could take off some of the identification and registration workload of government. Finally, the government might not be able to reach certain groups for identification and registration, while HOs can. According to van der Veen (Appendix C), there is also an educational incentive for the government. They could learn about SSI, blockchain, and how they could use these technologies to their own advantage.

For government authorities some disincentives can be distinguished: SSI would decrease access to data compared to centralized systems as stated by van der Veen (Appendix C). This would mean government institutions would lose some control over identity. Both Bolton and Stevens (Appendix C) supplement this disincentive by describing that losing control over identity would go against the government's core mandate. Finally, pre-existing government identification efforts could prevent the government from supporting a new identity scheme. According to Bolton (Appendix C), developments in systems like the IPRS, Huduma Namba, and the Single registry would limit the sense of urgency for a foundational SSI system.

The trend in Kenya seems to be that the government is trying to increase its control over citizens. There seems to be no sense of urgency for government stakeholders to support a humanitarian SSI system, as there is not sufficient political will to include these un(der)documented people. Government actions, such as the halting of alien registration and the attempt to consolidate all citizen information in a centralized government system stand directly opposite the value proposition of a humanitarian SSI system.

C. Local Government authorities

Authorities on county-level especially in rural counties have a bit more interest than the national authorities. A more complete view of identity within their county makes coordination and operation of local government tasks easier. However, they do not specifically have an interest in providing SIM and mobile money access. As such, they remain limited in interest.

D. Mobile Network Operators

For MNOs there is a commercial incentive for this system, as more people could be onboarded that would normally be excluded from their services. Especially for the private sector, this makes an attractive value proposition as stated by Stevens, van der Veen, Bolton, and Ebert (Appendix C). Oliveros (Appendix C), emphasizes the interest of MNOs due to the large volume of cash that is moved with CTPs. Additionally, an SSI system would allow users to present verifiable credentials from trusted partner organizations when onboarding for a new service. This way, personal information can be carried over between services in a verifiable way. This would greatly optimize the efficiency of registration procedures as stated by Stevens, van der Veen, Bolton, and Lamers (Appendix C). Van der Veen (Appendix C) further elaborates on the efficiency advantages: "They (private sector stakeholders) would have the benefit to establish trust with customers, reidentify them more easily when they appear somewhere else, onboard people more quickly and they need fewer operators to do so. All of that would increase their interest from an efficiency point of view". But also, it would reduce compliance risk according to Lamers (Appendix C). As the validity of documents can be easily verified in a remote way. Bolton and van der Veen (Appendix C) both emphasize the significance of CSR (Corporate Social Responsibility) incentives for the private sector. Working together and showing exposure to HOs

has branding advantages according to them. Lamers (Appendix C) further extends this thought of CSR advantages by emphasizing that private sector service providers can contribute to a more private society. Furthermore, van der Veen (Appendix C) describes that private sector organizations could be interested to work with HOs as they have improved ground access in low access areas. This can be the case in high-risk areas or areas in conflict. Through SSI, private organizations could leverage HO capacity to gain access to the people in these areas.

SSI would not be in the best interest of businesses that are currently thriving on a lack of privacy. According to Stevens (Appendix C): "SSI is especially difficult to accept if your business model entirely depends on the analysis of personal data and third-party tracking of information." This thought is adduced by van der Veen (Appendix C) which describes that a proper SSI implementation and regulation would make it more difficult for one party to hold the majority of data.

For private sector service providers such as MNOs, there are a lot of theoretical advantages to supporting such a system. MNOs are definitely engaged with the current pilots that are running. However, a big part of their service relies on a lack of privacy. Therefore, there is currently not a drive to specifically support a humanitarian SSI system, over supporting the KYC acceptability of a centralized refugee/asylum-seeker identity system, such as the UNHCR PRIMES system. Additionally, understanding of the technology has not reached the organizational scale yet. Therefore, MNOs are not as interested as they could be.

E. Financial Service Providers

FSPs are in a similar position as MNOs. Onboarding of new customer segments increased registration efficiency, remote registration/verification and lower compliancy risks are all important incentives for them. Lamers (Appendix C) adds to this the potential of new business models. FSPs in the Netherlands are seeing the potential to take up roles as trust providers in SSI systems. This makes learning about SSI also a big incentive for FSPs, as they could branch out their experience with SSI to other popular use-cases such as shared KYC systems. Lamers (Appendix C) describes the need for Dutch FSPs to make their systems more private, as this is popular among customers. This thought is also mentioned by van der Veen (appendix C): The commercial interest could be that many more people are interested in protecting their data, so the first one to launch such a system would get the majority of the users.

FSPs in the country are thriving on a lack of privacy in the country. The potential of onboarding new customer segments is limited due to the prevalence of less privacy-friendly solutions such as algorithmic identity as a way to serve un(der)documented people. Credit profiles are enriched with third party information and there is no real incentive to make internal systems more private. As such, while there is a lot of potential benefit for FSPs, this is not yet fully perceived.

F. National Civil Society Organizations

National CSOs in Kenya would certainly have an interest in the proposed system, as it could contribute to more financial and social inclusion in the country. CSOs in the country have indicated that they do not agree with the governments' centralized identity developments. A big part of the

national CSOs represent the un(der)documented and vulnerable groups in the country. Providing them with more dignity, more efficient aid and more privacy is very interesting for CSOs.

G. International Identity Development Organizations and initiatives

International Identity development Organizations like the World Bank group and initiatives such as ID2020 and the GSMA are all working towards better digital identity systems on a global scale. Many are committed to closing the identity gap in Africa. As such these stakeholders are very interested in the proposed system from an SDG standpoint. Additionally, by developing such a system, they could further learn about SSI and how it can be used.

H. United Nations agencies

UN agencies have a high interest in the proposed humanitarian SSI system. The UNHCR especially has the mandate to provide all people with a form of identity documentation. The UNHCR is actively developing digital identity solutions and is exploring the possibilities of SSI. The agency also publicly accepts proposals for SSI solutions (UNHCR, 2018b). The UNHCR is open to the idea of providing "trust services" through a well-designed SSI system. The UN agencies are highly involved in blockchain innovations in the humanitarian space.

I. Humanitarian Organizations

Humanitarian Organizations also have a high interest in a humanitarian SSI system. Not only would it allow them to give beneficiaries more control over their aid and more dignity, but it would also improve the efficiency of their humanitarian aid services, in specific cash transfer programming. All of this without putting the beneficiaries at risk due to privacy concerns and with a lower risk of function creep compared to centralized systems.

4.4.5 Stakeholder involvement

Based on the earlier identified resources/power and perspectives/interest a Power-Interest grid is constructed. This is a tool used for stakeholder prioritization. It is presented in figure 4.7. The power axis represents the stakeholders' power or influence on the outcome of a humanitarian SSI system. The Interest axis represents the stakeholders' interest in reaching the proposed system.

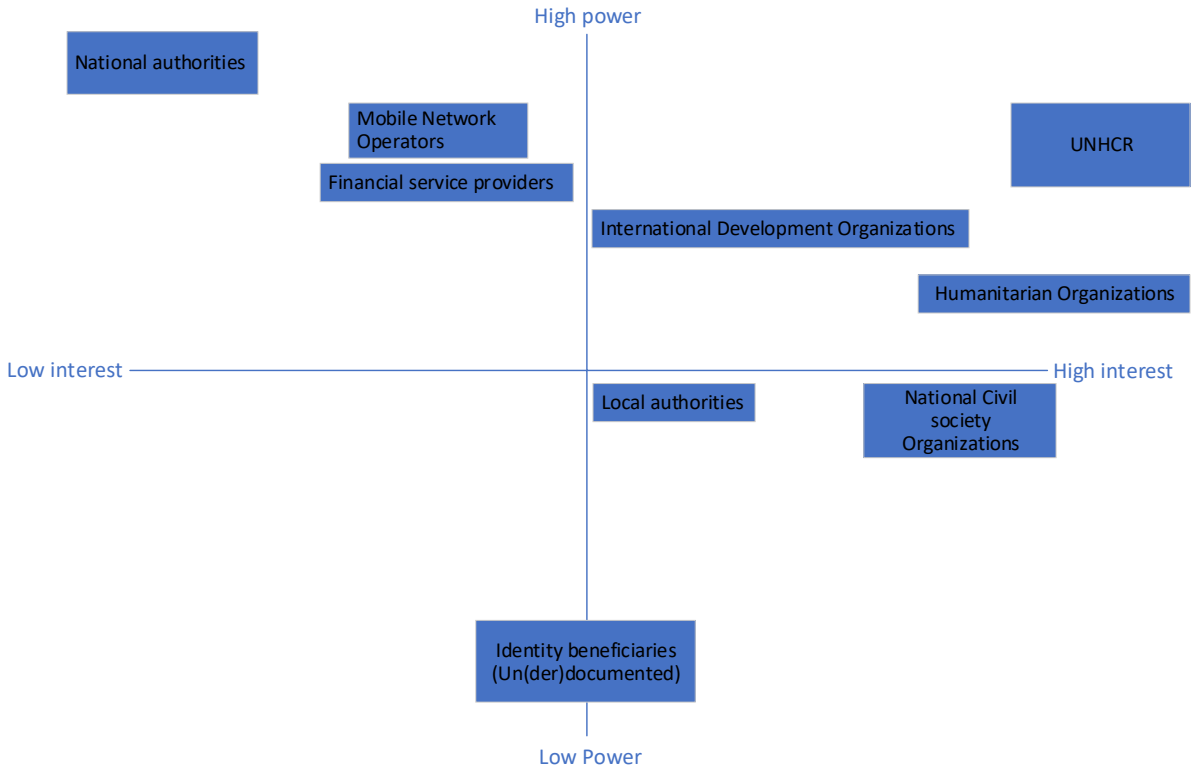

Figure 4.7: Power-Interest grid of current stakeholder field

The PI-grid can be divided into four quadrants. These quadrants are typically assigned with stakeholder types, used to determine project involvement. The upper right quadrant is classified as "Players", these are stakeholders which should be managed closely and collaborated with. The upper left quadrant is classified as "Context Setters", these stakeholders are to be consulted and kept informed. The bottom right quadrant is classified as "Subjects", these should be involved and kept satisfied. The final quadrant in the bottom left is classified as "Crowd", these should be monitored and informed.

International Identity Development Organizations, United Nations agencies, and Humanitarian Organizations are currently identified as Players. National authorities, MNOs, and FSPs are classified as context setters. National CSOs and Local authorities and un(der)documented people are identified as subjects.

For the development of a humanitarian SSI system for SIM- and mobile money registration the current state of the stakeholder landscape is quite problematic. As the context setters, especially national authorities, are required in a much more involved role. During the stakeholder analysis, it became clear that national authorities are the most important stakeholder when it comes to scaling to a more foundational purpose. These stakeholders are essential to reach the proposed system change. This is especially the case for national authorities, who have the official mandate on identity provision in the country and the control over KYC regulation and authentication. Simply consulting them and keeping them informed is not enough as they have both significant blocking power and unique development resources. Respondents universally agreed that the government

should actively be involved. The same can be said for MNOs and FSPs, who also have blocking power in terms of underlying infrastructure and the final say over service access.

National authorities, MNOs, and FSPs are required as players in the development of a humanitarian SSI system. To reach such involvement of these stakeholders, these stakeholders need to be shifted along the interest axis, this is displayed in figure 4.8.

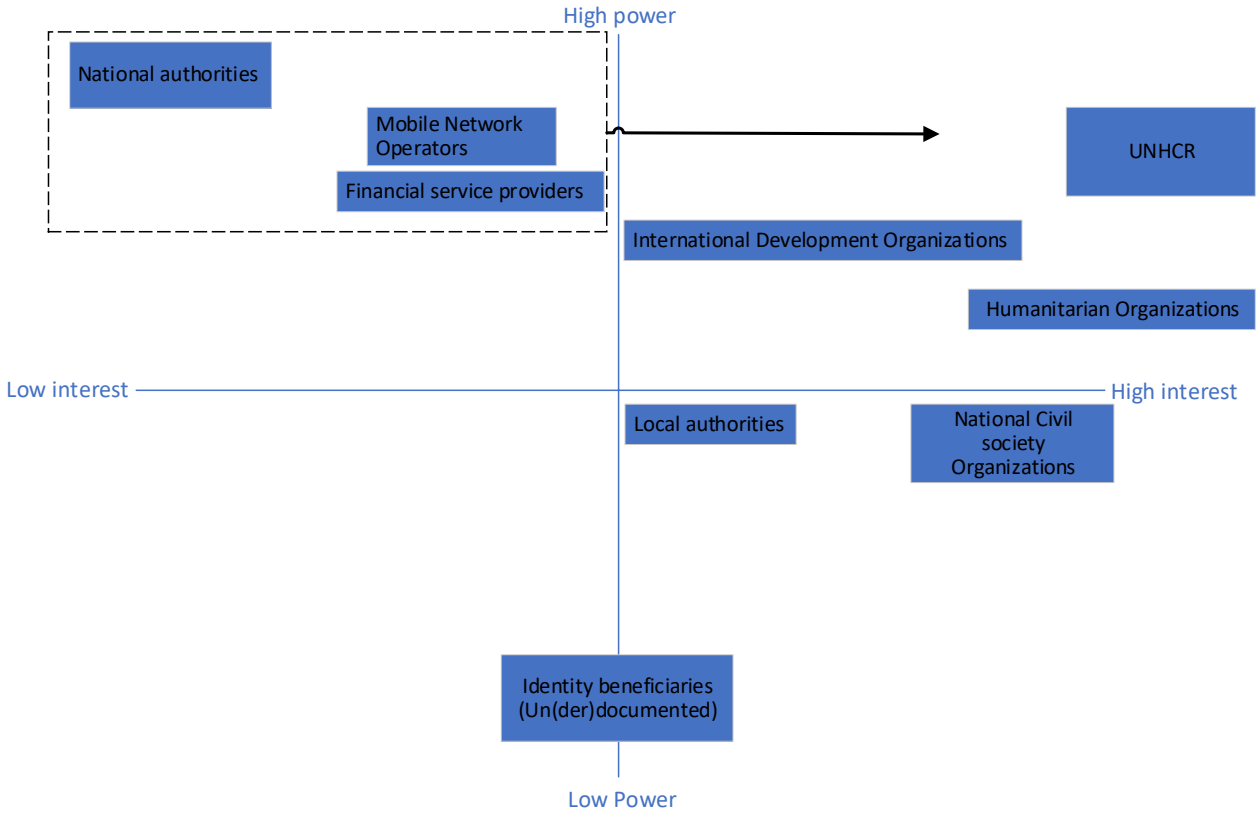

Figure 4.8: The required shift in Power-Interest grid

4.4.6 Sub-conclusion Stakeholder Analysis

As part of the system analysis, the technical analysis provides an answer to the following question: "*What is the landscape of stakeholders involved in the Kenyan identity ecosystem*.

In summary, based on the stakeholder analysis, the following conclusions are drawn regarding the stakeholder environment in the country:

- There is little competition between MNOs in the country and due to the aggressive expansion of mobile money, MNOs are in an extremely powerful position in the country. Both MNOs and FSPs in the country seem to be taking advantage of the lack of privacy regulation in the country.
- The interest of public stakeholders is somewhat entangled with the interest of MNOs and FSPs in the country. This is the case from the formal side, with a direct government stake in the dominant MNO and allegedly also from the informal side, indirect government official stakes in the private sector.

- Understanding of SSI technology is not fully present at organizational level for many of the national stakeholders. While, public- and private sector stakeholders in Kenya are open to and are involved with innovations in the blockchain space, a full understanding of SSI is most likely limited to several individuals operating in these organizations.
- The commitment of national stakeholders such as national authorities, MNOs, and FSPs is essential to realize a humanitarian SSI system that can facilitate SIM- and mobile money registration as they have significant blocking power and required resources such as supporting infrastructure.
- International stakeholders such as HOs, UN agencies, and global development organizations and initiatives are committed to closing the identity gap with a high level of development capacity, advisory capabilities, and potentially complementary funding.
- In the current circumstances and conditions there is not a sense of urgency for especially national authorities and to a lesser degree FSPs and MNOs in the country to actively pursue a humanitarian SSI system for in-name SIM- and mobile money registration.
- The lack of a sense of urgency for the national authorities seems to at least partially originate from a lack of political will to include un(der)documented people in these services.
- For FSPs and MNOs there are multiple commercial incentives to support a humanitarian SSI system, but currently, they are mostly held back in engagement due to uncertainties regarding KYC compliancy of such a digital identity.
- The lack of a sense of urgency for the private sector stakeholders is further maintained due to the acceptability of less privacy-friendly alternatives such as centralized systems or algorithmic identity.

4.5 System analysis sub-conclusion

Based on the sub-conclusions of the technical-, institutional-, and stakeholder analysis, the state of the socio-technical system for identity provision in Kenya has been described. Together these sub-conclusions provide an answer to the first research sub-question:

"What is the socio-technical context of the Kenyan identity registration ecosystem?"

The summaries of relevant points in 4.2.5, 4.3.6, and 4.4.6 provide a birds-eye-view of the socio-technical system of the Kenyan identity ecosystem and are used to further shape requirements and design. Several things were found that were used as a basis to further shape the requirements and design. Firstly, the privacy regulation pressure in the country is currently non-existent and upcoming legislation does not stimulate private- and public sector stakeholders to offload responsibility for data. Secondly, awareness concerning privacy in the country is still limited. Thirdly, the technological environment in Kenya is relatively well connected and advanced when considering mobile phone coverage and usage. Fourthly, there seems to be both intentional and unintentional identity exclusion in the country. Fifthly, service providers in the country have to deal with relatively strict onboarding regulations. Sixthly, Kenya as a country is actively exploring blockchain and its possibilities, however, understanding and experience with SSI as a technology is still only on a sporadic individual basis and not on an organizational level. Seventhly, there is humanitarian involvement in identity provision for refugees and asylum seekers to some extent.

However, this remains on a parallel basis and is not a gateway to private sector services. Finally, there is a high degree of information asymmetry in the country between public, private, and non-governmental organizations. This is especially the case due to the fragmentation of identity systems in the country and the continuous data collection by HOs. These are the main takeaways from the socio-technical situation in Kenya that are further used in requirements formulation.

From an international standpoint, there are multiple dedicated organizations and stakeholders that see an opportunity for humanitarian SSI systems in Kenya to: Improve the quality of life and dignity of un(der)documented, improve effectiveness of humanitarian aid, create financial and social inclusion with minimal risk of function creep and in the long term close the identity gap. In order to reach this, these currently functional systems have to transcend the boundaries of humanitarian aid into a more foundational purpose.

From a technical point of view, the current technical identity provision systems in Kenya are highly fragmented and are unable to provide proofs of identity to everyone. Developments to create a more complete and inclusive digital identity system in the country, through the NIIMS, have stagnated. When looking at other identity systems in the country, such as the UNHCR, there is room for complementary systems to aid in identity provision.

When looking at the institutional environment in the country this is where things get complicated for a humanitarian SSI system. The barrier to getting an identity in Kenya is quite high, leaving many people excluded from identity. However, the barriers to getting access to private sector services are similarly high and data protection regulations are non-existent. A lack of trust in government to provide identity systems may allow for HOs to fill this gap.

When approaching this development from a stakeholder perspective the cooperation from national stakeholders such as national authorities, MNOs and FSPs is unlikely. The stance that national authorities have been taking is directly in opposite of some of the values that SSI tries to implement. Especially problematic is the premise of the Kenyan government to stay in control over citizen data and the fact that FSPs and MNOs can leverage alternative, less private, technologies.

However, the collaboration of national public- and private stakeholders such as national authorities, FSPs, and MNOs in Kenya are essential for the development of a humanitarian SSI system that facilitates SIM- and mobile money registration. The main challenge identified in the system analysis is to get these national stakeholders interested and actively involved in this, up until now, internationally driven development.

The current state of the socio-technical system and the lack of sense of urgency/interest makes it difficult to design a process design that structures collaboration between stakeholders, for which the need was expressed by Stevens (2018). A much more pressing challenge in this stage of the development of SSI as an innovation, is to increase the interest for national stakeholders such as national authorities and FSPs/MNOs. Because without an intention of serious collaboration, there is not much to structure.

5. Requirements

The socio-technical environment in Kenya does not allow for sufficient interest and support among national public- and private stakeholders. This chapter identifies which circumstances and conditions drive and constrain the support for a (humanitarian) SSI. The following sub-question is focused on in this chapter: *"What are local circumstances and conditions in Kenya that drive or constrain the support of important public- and private sector stakeholders to facilitate SIM- and mobile money registration of un(der)documented through a humanitarian SSI system?"*

In order to answer this question, a combination of desk research and semi-structured interviews were used as methods. This is displayed in figure 5.1. The interview protocol, questions, and interview summaries of the conducted semi-structured interviews can be found in Appendix C. The semi-structured interviews were conducted with six individuals, all affiliated to (humanitarian) SSI initiatives. three of the respondents are internally involved within the NLRC, one of which is based in Kenya. Two respondents were affiliated with private sector initiatives, one of which is based in Kenya. Finally, one respondent of the IFRC was interviewed as well. This chapter will conclude in a set of local circumstances and conditions in Kenya that constrain support to emerge among the public- and private sector stakeholders in the country. These can be seen as context requirements for a process to nurture a more supportive environment in Kenya.

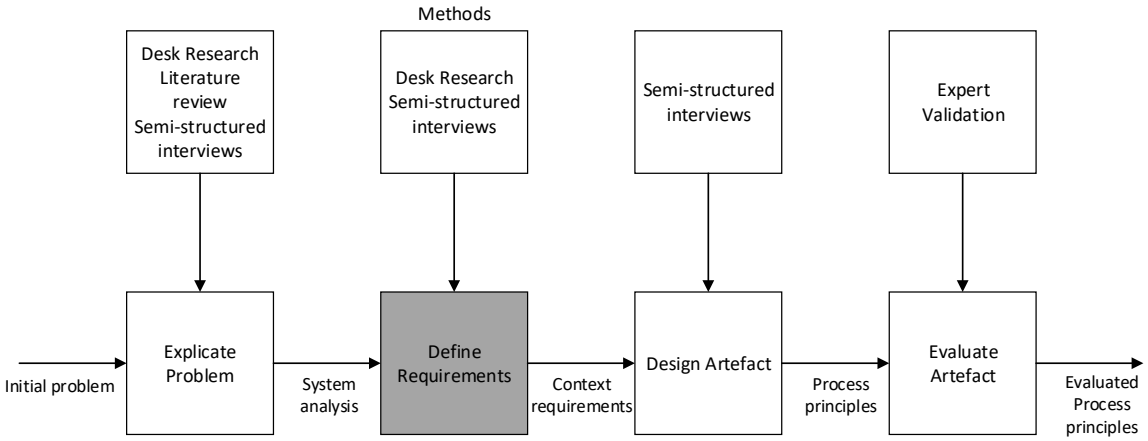

Figure 5.1: Requirements Methods

To arrive at a set of support-driving and -constraining local circumstances and conditions this chapter is structured in the following way: First, the existing knowledge from the Technology Acceptance Modelling (TAM) field regarding similar innovations was used to provide a basis of influential factors in paragraph 5.1. Subsequently, in paragraph 5.2, the tacit knowledge of several respondents was combined to identify local circumstances and conditions (external variables) which influence the attitude towards using the proposed system. In paragraph 5.3 for each of these local circumstances and conditions, a scale from inopportune to opportune was established. This

was used to establish an assessment framework. Subsequently, in paragraph 5.4 this framework is applied to the socio-technical system of identity provision in Kenya, using the findings of the system analysis. Finally, in paragraph 5.5 the findings of this chapter are concluded.

5.1 Technology acceptance factors

Davis, Bagozzi, & Warshaw (1989) formed the foundation of the technology acceptance modeling (TAM) research field. They identified a clear relationship between both the perception of usefulness and the perception of ease-of-use with the intention of people to adopt computer systems. In figure 5.2 the TAM model of Davis, Bagozzi & Warshaw is displayed. This study assumes that in order to nurture more support among stakeholders, the attitude towards using a humanitarian SSI system needs to be sufficient. This is influenced by external variables: Local circumstances and conditions of the socio-technical system an SSI has to be deployed in.

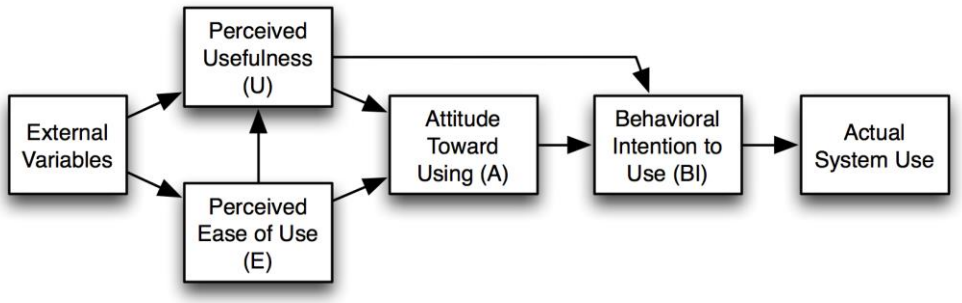

Figure 5.2: Technology Acceptance Model by Davis, Bagozzi, & Warshaw (1989)

Perceived usefulness and Perceived Ease of Use are not the only two factors through which an attitude towards using can be influenced. Several academic papers were found that explore additional factors that influence the attitude toward using technologies that have similarities with SSI systems. Gu, Lee, & Suh (2009) performed research on the factors that affect the adoption of mobile banking. They concluded that next to perceived ease-of-use and perceived usefulness, trust is also of major influence in the adoption of the technology. Subsequently, Benenson et al. (2014) performed research on user acceptance of 'Privacy-ABC technology' (attribute-based credential) and Privacy Enhancing Technologies (PET) in general. In their research, the authors concluded that understanding of the technology, perceived ease-of-use, and perceived usefulness play important roles in the user adoption of PETs. Furthermore, they found correlations between the understanding of technology and the perceived usefulness. And finally, Harbach, Fahl, Rieger, & Smith (2013) performed research on the acceptance of privacy-preserving online authentication technology. The authors describe the perspective of both users and service providers in a German online authentication innovation. They describe a chicken-and-egg-problem in which users do not find enough utility due to the limitation of supported services and service providers that are not inclined to provide support due to the small user base. The study identified barriers beyond this chicken-and-egg-problem. Lack in understanding of the technology and perceived loss of control were established to cause decreased attitude toward using in the adoption of such a technology.

Service providers as described by Harbach et al. (2013) see the need for a reliable digital identity management system in the future but are held back in adoption through regulatory issues and a lack of user base. Simply distributing the authentication technology is not enough for adoption. Non-technical factors such as the availability of information and services with everyday relevance are necessary prerequisites for the adoption of authentication mechanisms (Harbach et al., 2013).

Table 5.1 provides a list of some of the factors that influence the attitude towards using that were identified for similar privacy-enhancing technologies. The next section will explore which local circumstances and conditions drive or constrain support for SSI. In order to verify this, they will be related to having an effect on one of these factors.

Table 5.1: Privacy-enhancing technology acceptance factors

Acceptance factors
Perception ease-of-use
Perception usefulness
Understanding of technology
Regulatory support
Perception of control
Trust

5.2 Circumstances and conditions

Semi-structured interviews were conducted with several individuals with a proven affinity to humanitarian- or private sector SSI initiatives, specifically those catered to financial inclusion or financial services. By combining the tacit knowledge of the respondents regarding the value-proposition of SSI for identity provision and their experience with implementation and public/private stakeholder involvement, a set of support driving/constraining local circumstances and conditions was deducted. These were associated with the acceptance factors in paragraph 5.1.

Privacy legislation pressure

The decentralization and privacy-enhancing aspects of SSI make the technology prosper in an environment with a strong focus on privacy. The technology is especially interesting for organizations that wish or are pressured to reduce their responsibility for data. Stevens mentioned that in Europe, more and more companies are interested in SSI solutions due to the huge fines that came in to play with the GDPR. The privacy environment is driven directly by the nature of privacy regulations. Oliveros (Appendix C):" I can see that (privacy legislation) being one of the levers for taking SSI more seriously". According to Ebert (Appendix C), the pressure on privacy and data responsibility is ramped up when a government starts to issue huge fines to someone that has not respected a principle from a data protection law. It is in situations like these that SSI as a technology has a clear advantage. By redistributing the control over personal data to the end-user, organizations can reduce the liabilities and risks of having to govern data. According to van der Veen (Appendix C): "It depends on how idealistic stakeholders are in terms of protecting people's privacy. If they are not idealistic then this is probably not the best solution for them. If they are very there is not a lot of other solutions that could equally protect the privacy of the people".

Unfortunately, in many countries, the agenda is still to gather, hoard, and store data, without sharing it. Stronger data protection regulations also reduce the possibilities for the private sector to employ alternative identification systems, such as algorithmic identity. Ideally, it is not only the private sector that is encouraged to offload data responsibility, but also the government itself. Lamers (Appendix C) mentions that the government in the Netherlands is mainly starting to get seriously involved with SSI initiatives due to two internal government programs: "Regie op gegevens" (control over data) and "Wet digitale overheid" (Law digital government). These programs are the result of the government having to change their own way of managing data due to sufficient privacy legislation pressure. This process, according to van der Veen (Appendix C), is at least partially driven by Civil Society Organizations and it also requires some kind of privacy watchdog to hold the government accountable. Privacy legislation pressure is some of the regulatory support that enables the perception of the value of SSI systems.

Information Privacy awareness

Information privacy awareness in countries influences the suitability of a humanitarian SSI system in three ways. Firstly, increased information privacy awareness of the general public in the country puts privacy regulation higher on the political agenda. Van der Veen (Appendix C) remarked that especially in democratic countries, unelected parties with a more privacy-focused election program could gain momentum. Secondly, increased information privacy awareness could drive the private sector to differentiate their products or services in terms of privacy. According to Lamers (Appendix C), the increased societal attention towards privacy and security for citizens and consumers is one of the reasons why SSI is an interesting solution for FSPs in the Netherlands. This thought is underwritten by Oliveros (Appendix C) "If organizations are really serious about it, this (SSI) is about as privacy protecting and as respectful of the privacy as it gets". Thirdly, Oliveros (Appendix C) noticed that the willingness of beneficiaries and end-users to control their own data is important for SSI systems: "If we just transition to a world of SSI, it is also their own motivation of end-users themselves to keep that information as updated as they need. They need to see a benefit for themselves as to why they need to be carrying all their digital credentials". This line of thinking is further confirmed by Harbach et al. (2013): 'users need to be made more aware of immediate problems with their current practice since unlike "functional" technology there is a lack of intrinsic motivation to adopt new authentication technology." For the ability of SSI to rebalance control over data to be perceived as useful, people need to be aware of information privacy.

Online Accessibility

According to Van der Veen (Appendix C):" SSI does not properly work in offline scenarios at the moment". This means that currently, SSI solutions are only appropriate when there is enough online accessibility. Oliveros (Appendix C) elaborates a bit further on this dependency: "the current technology requires that you have either access to a smartphone or some kind of infrastructure that allows you to keep all of those credentials in the hands of the beneficiaries, for which smartphones are the most effective way of doing that now. But if you don't have that infrastructure and the digital literacy level; the understanding among beneficiaries to begin with to maintain their information, then implementation is not as easy". Favorable circumstances and conditions for a humanitarian SSI system thus include a high mobile network coverage, high

mobile phone penetration or central access points, and a proficient digital literacy level. This is essential for the perception of ease-of-use and usefulness to be established.

Identity exclusion motive

For public sector stakeholders the perception of usefulness of using a humanitarian SSI system to facilitate financial and social inclusion for un(der)documented relies a lot on the initial reason for exclusion. Theoretically, a humanitarian SSI system has a lot of benefits to offer as a complementary system in the identity provision of a country, however, it needs to connect to the circumstances in the country to be perceived as a benefit. Stevens (Appendix C) introduces this dependency: "If a government is willingly excluding people from a national government ID and the services that come with that, then it would not have any value for them I would say. If it is because of any other reason, then it might have value for them". Different motives of exclusion in a country are mentioned by Bolton (Appendix C): "The people that currently do not have access to an identity, is actually for a reason. It's either that they are officially denied one because they are not seen as desirable or because there is some sort of cost boundary or burden of evidence that can't be met by that individual. So that actually is a fundamental blocker to that person". Oliveros (Appendix C) acknowledges these motives and adds to it: "It could also be just the fact that the people would not want to be identified. Even if the government allows for some kind of a refugee ID to be used as a means to register for a service, that they might feel not very secure when they share this level of information. Or because they might be so rural, and they are not as well connected because infrastructures might not be in place to allow them to be there (at registration offices)." This creates a spectrum of identity exclusion motives, ranging from intentional to unintentional. Predominantly unintentional identity exclusion allows for a humanitarian SSI system to add the most value. Furthermore, situations with a lack of government capacity in identity provision and cost boundaries would be the best identity exclusion motives to tackle with this system.

Financial service onboarding obstacles

FSPs could use a humanitarian SSI system to onboard new customer segments. For FSPs to perceive this as useful, it depends a lot on the current obstacles they are experiencing in the country when onboarding new customers. Firstly, KYC regulations are the biggest barrier currently for FSPs according to Bolton, Ebert, Oliveros, and Stevens (Appendix C). However, Ebert (Appendix C) noticed that KYC regulations are different from country to country. In some countries KYC regulations can be less strict than others. This is the case in Cameroon according to Ebert (Appendix C): "I looked it up at one point, in Cameroon for example UNHCR mandates are already accepted for opening bank accounts. It is one of those rare cases". Less strict KYC regulations would certainly be an advantageous environment to roll out a humanitarian SSI system. Secondly, FSPs can experience difficulties or lack of infrastructure to verify or register remotely as an obstacle to onboarding. Ebert: "You would really have to find that country, where maybe the government regulation is less of an issue. But a lack of trust by banks and MNOs is more of an issue. Now you can add a layer of trust and verifiability by using SSI". Such circumstances would drive the support for SSI systems. Thirdly, van der Veen (Appendix C) mentioned that some countries have high-risk areas, or low access areas. According to van der Veen:" In quite a number of countries, private organizations are interested to work with humanitarian organizations as they

have better on the ground access to high-risk areas or areas in conflict, where you are really not allowed in. As a private company, it could be very risky to start a business in a certain area, especially if you have never been there or have not been introduced through formal networks." In countries like these, a humanitarian SSI system would be perceived even more useful for FPSs.

SIM card onboarding obstacles

In many countries, MNOs have to comply with the same obstacles as FSPs when issuing new SIM registrations. In some countries, however, the restrictions on SIM registration deviate from financial service restrictions. MNOs would perceive more usefulness in a humanitarian SSI system in circumstances where it could provide not only a way to onboard new customers but also offers solutions for a lack of remote registration and access to high-risk areas.

Degree of information and knowledge of SSI

An environment with understanding of the technology among all stakeholders is beneficial to drive support for a humanitarian SSI system. Firstly this is important due to the correlation of understanding of technology with the perception of usefulness as identified by Benenson et al. (2014). On an organizational level, understanding of SSI is important to get SSI on the agenda. Most important is the understanding of the value proposition of SSI for each stakeholder. On the beneficiary level, even if beneficiaries are aware of privacy, they need to know how they can leverage SSI to safeguard their privacy. Secondly, a lack of understanding of the technical systems can contribute to a perception of control loss, potentially discouraging beneficiaries to adopt the system. Enough availability of information on SSI systems or experience with the technology is beneficial to establish a perception of usefulness and trust.

Humanitarian involvement in Refugee and Asylum seeker registration process

The involvement of HOs in the existing refugee and asylum seeker registration process is also an important circumstance. Oliveros (Appendix C) expresses the following:" In the case of UNHCR I think they have been really successful in getting exemptions for SIM cards because they have this closer work already with the government. It is not because they are doing this purely without the knowledge or the support of the government, to begin with. In a way, they are already working with the government on accepting or registration of beneficiaries. It is not like NGO X, a new one from the Netherlands, can go to Uganda and start registering, it is not the case". This points towards the fact that existing involvement of HOs in the refugee and asylum seeker registration process creates trust for public- and private sector stakeholders. Existing involvement of HOs in these processes would, therefore, make it easier to get support for a humanitarian SSI system.

Identity Information asymmetry

Ebert (Appendix C) identified an important condition for SSI systems during the exploration of potential applications of SSI: "We realized that people-centric identity is really interesting everywhere where you have 2 things: 1 information asymmetries or 2 a lack of central registries". Especially this aspect of information asymmetry between stakeholders is an important condition that really makes or breaks the potential value for different stakeholders. The interoperability of a (humanitarian) SSI system allows for the consolidation of information from a range of different organizations, which as a whole can provide a more complete view or assurance of someone's identity. However, if public-, private sector organizations, and NGOs are dealing with the same

information then there is no value in joining those information streams. It is in particular advantageous if HOs have information on individuals in the country that public- and private sector organizations don't have.

5.3 Humanitarian SSI context assessment framework

The set of support driving/constraining circumstances and conditions can be used to assess the suitability, and which conditions currently prevent support, in a country for the proposed humanitarian SSI solution. To compose such a framework, all the aforementioned conditions and circumstances have been assigned a scale, ranging from inopportune to opportune.

For privacy legislation pressure an inopportune scenario is when there is no data protection legislation whatsoever. In this case organizations have no reason to deviate from centralized identity systems. A still unfavorable scenario is data protection legislation that is focused on consent. Under these circumstances, centralized systems are still prevalent, but organizations are hedged against data breaches. A more favorable scenario is data protection legislation enforcing accountability on the private sector, stimulating the offloading of responsibility for data. An opportune situation is data protection legislation enforcing accountability on the public- and private sector, stimulating the offloading of responsibility for data for all stakeholders.

For a scale of information privacy awareness, Correia & Compeau (2017) publication on privacy awareness provides a good definition. For their definition, Correia & Compeau define “Elements related to information privacy” as: “Technology, regulations or common practices used by companies or individuals to collect, use and share user’s private information. " An inopportune situation would be when the population of a country is unaware of the elements* related to information privacy. A still unfavorable scenario would be when the population of a country has knowledge of the elements* related to information privacy. A more favorable scenario would be when the population of a country has understanding that elements* related to information privacy exist in the current environment. An opportune situation would be when the population of a country can project what impact elements* related to information privacy have in the future.

For the online accessibility in a country, an inopportune situation would be a low mobile network coverage in the country, with low mobile phone penetration and low digital literacy. Without online connectivity, getting control over digital credentials in the hands of beneficiaries is very difficult. A still unfavorable scenario would be an average or high mobile network coverage, but a low penetration rate of mobile phones or central access point and low digital literacy. A more favorable scenario would be a high mobile network coverage, moderate mobile phone penetration with sufficient central access points, and high digital literacy. An opportune situation would be a high mobile network coverage and mobile phone penetration and high digital literacy among users.

For identity exclusion motives of a country, an inopportune scenario would be the intentional exclusion of people because they are not seen as desirable. A moderately unfavorable scenario would be a mix of intentional and unintentional exclusion. A favorable scenario would be identity exclusion mainly due to a burden of cost or burden of evidence that can’t be met by individuals. An opportune scenario would be identity exclusion mainly due to a lack of government capacity or voluntary exclusion due to privacy/ security concerns.

For financial service and SIM registration onboarding obstacles in a country, an inopportune scenario would be very strict KYC regulations as the only major obstacle for onboarding of un(der)documented. A slightly less unfavorable scenario would be KYC restrictions & limited

remote registration. A moderately favorable scenario would be KYC restrictions, limited remote registration & limited access to high-risk areas as obstacles. An opportune situation would be Loose KYC restrictions, limited remote registration & limited access to high-risk areas as the major onboarding restrictions. These conditions would give a humanitarian SSI system the advantage over other systems.

For the degree of information and knowledge of SSI in a country, an inopportune scenario would be no knowledge or available information on the value proposition of SSI and no technical knowledge. A still unfavorable scenario would be when people have some knowledge of the value proposition of SSI systems, but no knowledge of technical aspects and no demonstrated experience. A moderately favorable scenario would be when there is sufficient knowledge and available information on the value proposition and technical aspects of SSI systems. An opportune scenario would be when people and organizations have sufficient available information and knowledge on the value proposition and technical aspects of SSI, including experience or demonstrations of SSI systems.

For the Humanitarian involvement in Refugee and Asylum seeker registration process, the GSMA (2017) distinguished several types of HO involvement in these processes. An inopportune scenario would be registration led purely by the host-government. A still unfavorable scenario would be registration led jointly, but with parallel HO registration. A favorable scenario would be registration jointly led by the government and HOs. An opportune scenario would be registration led by a Humanitarian Agency.

For information asymmetry between major stakeholders in a country, an inopportune scenario would have information asymmetry between stakeholders. A still unfavorable scenario would be low identity asymmetry between major stakeholders. A more favorable scenario would see high information asymmetry between major stakeholders. An opportune situation would have high information asymmetry between stakeholders, especially in relation to HOs.

The identified local circumstances and conditions, together with the established scales of suitability have been compiled in a framework as displayed in figure 5.3. With this framework, the context of a country can be assessed concerning the suitability of a humanitarian SSI system for SIM- and mobile money registration.

Suitability: / Local Circumstance / condition:	Unfavorable:	Moderately unfavorable:	Moderately favorable:	Favorable:
Privacy Legislation pressure	No Data protection legislation.	Consent focused data protection legislation which stimulates hedging against data breaches and data misconduct.	Legislation enforcing private sector data handling accountability which stimulates data responsibility offloading.	Legislation enforcing public and private sector data handling accountability which stimulates data responsibility offloading.
Information Privacy Awareness	Unaware of the elements* related to information privacy	Knowledge of the elements* related to information privacy.	Understanding that elements* related to information privacy exist in the current environment.	Projection what impact elements* related to information privacy have in the future.
Online accessability	Low mobile network coverage, low mobile phone penetration, insufficient access points in rural areas and low digital literacy.	Average / High mobile network coverage, low mobile phone penetration, some central access service points in rural areas and low digital literacy.	High mobile network coverage, average mobile phone penetration, wide spread central access service points in rural areas and some digital literacy.	Full mobile network coverage, high mobile phone penetration also in rural areas,wide spread central access service points and high digital literacy.
Identity exclusion motive	Mainly intentional exclusion.	Mixed intentional/ unintentional exclusion.	Exclusion mainly unintentional due to a burden of proof or cost for individuals.	Exclusion mainly unintentional due to lack of government registration capacity or voluntary exclusion due to privacy / security concerns.
Financial service onboarding obstacles	strict KYC restrictions.	KYC restrictions & limited remote registration.	KYC restrictions, limited remote registration & limited access to high risk areas.	Loose KYC restrictions, limited remote registration & limited access to high risk areas.
SIM card onboarding obstacles	strict KYC restrictions.	KYC restrictions & limited remote registration.	KYC restrictions, limited remote registration & limited access to high risk areas.	Loose KYC restrictions, limited remote registration & limited access to high risk areas.
Degree of information and knowledge of SSI	No understanding of SSI technology or value proposition. Not much available information.	Some knowledge and information on SSI value proposition, low technical understanding. No exposure and experience with the technology.	Sufficient understanding of SSI technology and value proposition. Low exposure to the technology.	Broad spread understanding of SSI value proposition and technical understanding. Exposure / experience with the technology.
Humanitarian involvement in Refugee and Asylum seeker registration process	Host Government-Led registration	Joint-Led, Parallel HO registration	Joint-Led	Humanitarian Agency-Led
Identity information asymmetry	Identity information symmetry between stakeholders	Low identity information assymetry between stakeholders	High Identity Information assymetry between stakeholders	High Identity Information assymetry between stakeholders. Especially with HOs.

Figure 5.3 Humanitarian SSI context assessment framework

5.4 Assessing Kenya's local circumstances and conditions

To assess the current local circumstances and conditions in Kenya for the proposed humanitarian SSI system, the assessment framework in figure 5.3 is filled in with the conclusions from the system analysis.

In terms of privacy legislation pressure in the country, the new GDPR inspired data protection bill has just recently been accepted. However, important parts that stimulate data responsibility and accountability for public stakeholders in the country have been taken out. While a big step has been taken in the right direction, it will take more time before enforcement by the office of the Data Protection Commissioner will be at capacity to create pressure on private sector stakeholders. Currently, there is no incentive for public- and private stakeholders to offload data responsibility. The agenda is still to hoard, store, and not share personal data.

Information privacy awareness in the country is starting to develop. Big data misconduct scandals such as the meddling in elections by Cambridge Analytica has gotten privacy discussions going in the country. With these ongoing discussions in the country, people are getting more aware of the elements related to information privacy. However, people are probably not fully aware of the extent to which these elements exist in their current environment. As many people still rely on digital lending apps, which are known to greatly intrude on the privacy of users.

Online accessibility in the country is generally quite good compared to other countries. Kenya has rapidly developed a digital and technological ecosystem, dubbing it as "Silicon Savannah". The mobile network coverage rate is high, and the mobile phone penetration in the country is also high. The government is putting out tenders to cover the last rural areas with mobile network coverage. With 80 percent of adults in Kenya relying on mobile money, it is expected that there is at least some digital literacy in the country. However, if there is enough digital literacy among vulnerable and marginalized communities in the country did not become clear in the system analysis.

The reason for un(der)documentation in the country and the motive for identity exclusion appears to be quite mixed in Kenya. On the unintentional side, the barrier to getting an identity is quite high in Kenya. There seem to be a lot of people who are not able to meet the burden of evidence that is required in the registration process. Additionally, while the costs of registration for an identity are lower than most other countries, for people below the poverty line (which is around 36% of the population in Kenya) this is still a significant barrier. However, exclusion with an intentional motive also appears to be an issue in the country. Reports of marginalized groups having to undergo different registration procedures indicate this. Additionally, there appear to be signs of a lack of political will to include un(der)documented in financial and social systems. The inactivity of alien cards issuance and renewals certainly seem to indicate this.

Very strict KYC regulations are currently the most pressing onboarding obstacle for private sector stakeholders. With KYC compliancy required for both SIM- registration and mobile money in the country, this is the case for both FSPs and MNOs. Furthermore, due to the fragmentation and lack of interoperability of identity provision systems, it is currently not possible for MNOs and FSPs to verify documents other than the national ID card remotely. The ability of SSI to remotely verify

credentials is therefore interesting for the private sector. During the system analysis, there was no indication of high-risk areas being an onboarding obstacle for FSPs and MNOs in the country.

Understanding of SSI technology in Kenya is still limited. There has been engagement of SSI initiatives with public- and private sector stakeholders and the country has a team specifically dedicated to exploring opportunities of blockchain. It can thus be assumed that there is understanding of the value proposition of a using a humanitarian SSI system and at least some individuals within public and private organizations have a sufficient understanding of SSI. However, technical understanding, especially on an organizational level is most likely limited. Hands-on experience and demonstration of the technology are also limited.

The refugee and asylum seeker registration process in Kenya is classified as joint-led. The UNHCR supports in registration efforts. However, UNHCR certificates are not acknowledged as sufficient for private sector services and KYC compliancy. The registration efforts of the UNHCR are therefore parallel to the alien registration of the government. This means that the door is already open for humanitarian agencies to assist in identity provision to some degree, but are not yet relied upon to assist with financial and social inclusion yet.

Identity information asymmetry between stakeholders in the country is high. Many HOs are actively providing aid services in the country, all with their own targeting and registration efforts. HOs have on the ground capacity used to feed need assessments. For un(der)documented people, this information is most certainly not available to national authorities and private sector stakeholders.

The current state of circumstances and conditions in Kenya, at least those that are identified by the respondents as being enabling or constricting for support among public- and private stakeholders for the proposed system, is displayed in figure 5.4.

Suitability: / Local Circumstance / condition:	Unfavorable:	Moderately unfavorable:	Moderately favorable:	Favorable:
Privacy Legislation pressure	No Data protection legislation.	Consent focused data protection legislation which stimulates hedging against data breaches and data misconduct.	Legislation enforcing private sector data handling accountability which stimulates data responsibility offloading.	Legislation enforcing public and private sector data handling accountability which stimulates data responsibility offloading.
Information Privacy Awareness	Unaware of the elements* related to information privacy	Knowledge of the elements* related to information privacy.	Understanding that elements* related to information privacy exist in the current environment.	Projection what impact elements* related to information privacy have in the future.
Online accessability	Low mobile network coverage, low mobile phone penetration, insufficient access points in rural areas and low digital literacy.	Average / High mobile network coverage, low mobile phone penetration, some central access service points in rural areas and low digital literacy.	High mobile network coverage, average mobile phone penetration, wide spread central access service points in rural areas and some digital literacy.	Full mobile network coverage, high mobile phone penetration also in rural areas,wide spread central access service points and high digital literacy.
Identity exclusion motive	Mainly intentional exclusion.	Mixed intentional/ unintentional exclusion.	Exclusion mainly unintentional due to a burden of proof or cost for individuals.	Exclusion mainly unintentional due to lack of government registration capacity or voluntary exclusion due to privacy / security concerns.
Financial service onboarding obstacles	strict KYC restrictions.	KYC restrictions & limited remote registration.	KYC restrictions, limited remote registration & limited access to high risk areas.	Loose KYC restrictions, limited remote registration & limited access to high risk areas.
SIM card onboarding obstacles	strict KYC restrictions.	KYC restrictions & limited remote registration.	KYC restrictions, limited remote registration & limited access to high risk areas.	Loose KYC restrictions, limited remote registration & limited access to high risk areas.
Degree of information and knowledge of SSI	No understanding of SSI technology or value proposition. Not much available information.	Some knowledge and information on SSI value proposition, low technical understanding. No exposure and experience with the technology.	Sufficient understanding of SSI technology and value proposition. Low exposure to the technology.	Broad spread understanding of SSI value proposition and technical understanding. Exposure / experience with the technology.
Humanitarian involvement in Refugee and Asylum seeker registration process	Host Government-Led registration	Joint-Led, Parallel HO registration	Joint-Led	Humanitarian Agency-Led
Identity information asymmetry	Identity information symmetry between stakeholders	Low identity information assymetry between stakeholders	High Identity Information assymetry between stakeholders	High Identity Information assymetry between stakeholders. Especially with HOs.

Figure 5.4: Kenya circumstances and conditions assessment

5.5 Requirements sub-conclusion

Using the findings of this chapter the second research sub-question can be answered:

"What are local circumstances and conditions in Kenya that drive or constrain the support of important public- and private sector stakeholders to facilitate SIM- and mobile money registration of un(der)documented through a humanitarian SSI system?"

By consulting TAM literature and by exploring tacit knowledge of several SSI affiliated respondents an assessment framework of local circumstances and conditions has been composed. By applying this framework to the findings of the system analysis, the following can be concluded regarding the local circumstances and conditions in Kenya:

- There is a lack of the perception of usefulness among national public- and private sector stakeholders for SSI technology in Kenya, at least in part due to the lack of information privacy awareness and privacy legislation pressure. Information privacy awareness and privacy legislation pressure should be increased to nurture more support.

- The online accessibility in Kenya is relatively good infrastructure wise. This doesn't seem to be an immediate blocker for the ease-of-use and perception of usefulness in the country. Improving digital literacy in the country could be a way to further drive up the perception of ease-of-use and usefulness to create support.

- The motive of identity exclusion in the country constricts the perception of usefulness for national authorities. Intentional identity exclusion in Kenya needs to be discouraged, in order for humanitarian SSI systems to fully be perceived as useful.

- Onboarding restrictions, both for financial services as for mobile network services, are very strict in Kenya. These need to be made more manageable in order to unlock more perception of usefulness and to allow for regulatory support.

- The low availability of information, knowledge, and experience with SSI systems in the country need to be improved. Especially direct exposure to stakeholders is required in order to create understanding and trust.

- The humanitarian involvement in identity provision, such as for refugee and asylum seeker registration, is still limited. Expanding the involvement could be a way to improve trust.

Together these requirements form several "levers" which can be influenced by HOs to increase the support for humanitarian SSI systems. No distinction has been made to what extent each requirement can constrain or drive support.

6. Design

The requirement chapter concluded in a set of required changes to the circumstances and conditions in Kenya. The artefact that is to be designed should cover as much of these changes as possible to allow for more support to emerge. This chapter is focused on answering the third sub-question: *"What support nurturing principles can help HOs to nurture more support for in-name SIM- and mobile money registration of un(der)documented through humanitarian SSI systems in Kenya?"*

In order to answer this question, semi-structured interviews were used as a research method, as displayed in figure 6.1. During the interviews with several individuals affiliated to humanitarian and/or financially inclusive SSI initiatives (the same respondents as for the requirement chapter), the respondents were challenged to identify potential lines of action for HOs to create these more favorable circumstances and conditions. The jointly generated ideas of the respondents were grouped and aggregated, which resulted in the composition of five support nurturing principles.

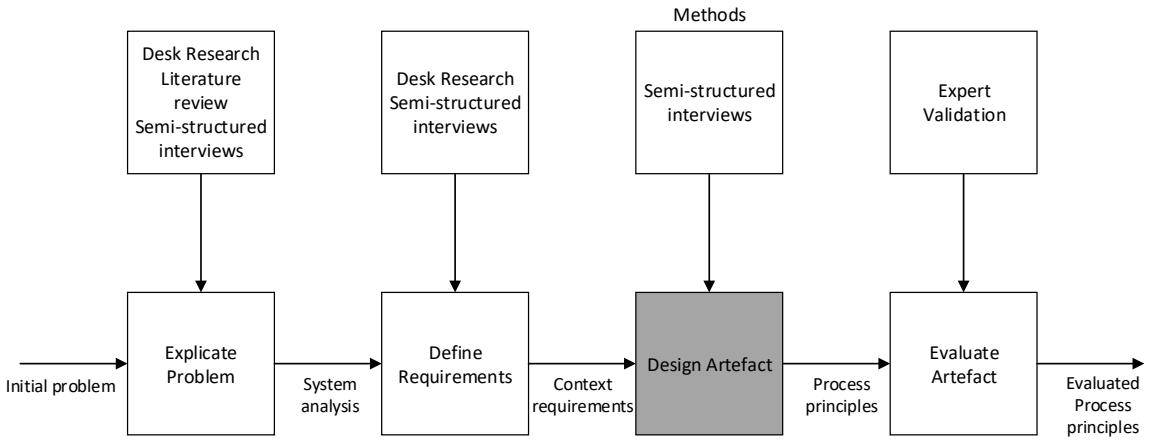

Figure 6.1: Design Methods

In order to arrive at the set of support nurturing principles, this chapter is structured as follows: Paragraph 6.1 describes the generated support nurturing principles. The design takes in to account the exploration of humanitarian support nurturing options with the respondents and Kenya specific characteristics as identified in the system analysis. Subsequently, in paragraph 6.2 the design phase is concluded.

6.1 Designing humanitarian support nurturing approach

In the semi-structured interviews, the respondents were challenged to explore options for the humanitarian sector to create these favorable and opportune conditions and thus create more support from public- and private sector stakeholders for a humanitarian SSI system as a way to

facilitate SIM- and mobile money registration. By synthesizing the tacit knowledge of the respondents and aggregating these insights into more broadly-defined principles, support nurturing principles have been formulated which applies to the local circumstances and conditions in Kenya.

6.1.1 Support nurturing principle #1: Advocate for flexible KYC and financial/social inclusion of un(der)documented

From the identified circumstances and conditions, the strict onboarding obstacles for FSPs and MNOs in the country together with the mixed motives of identity exclusion in the country are the most direct blockers for the proposed system. From what we have already seen in functional humanitarian SSI systems, there is room for HOs to advocate for more flexible KYC regulations. Several respondents describe that HOs are a complementary unit to the government and they have the ability to lobby for things. In the functional systems, HOs already succeeded in this to a certain extent. For example, several pilots have managed to get limited functionality and temporary access to SIM cards for beneficiaries. Oliveros (Appendix C) believes that advocating is a big part of what HOs can do to nurture better circumstances for a humanitarian SSI system: "Advocating for the most vulnerable. Advocating for cash transfer programming as a good way to provide aid, advocating for access to sim cards and mobile money, and providing an alternative way to meet the current requirements of KYC and SIM card regulations." Under the current circumstances, HOs must focus on lobbying for flexible KYC and (limited) inclusion specifically for the purpose of humanitarian aid services. Oliveros (Appendix C) describes under what conditions government authorities are most likely to accept flexible KYC regulations:" In the event of life-saving and short time period type of things I think the government might be motivated to say: Organizations such as UNHCR, who are overseeing refugees that may not have official IDs from the government, we will relax the KYC requirements for them so they can provide cash. Because the government otherwise would be constrained to provide this type of support for people who are in need. I think there is a potential for HOs to lobby, under the narrative: We are fulfilling our mandate of lifesaving things during an emergency, to support governments when they couldn't."

6.1.2 Support nurturing principle #2: Create intrinsic motivation by stimulating privacy

During the interviews with the respondents, it became evident that extrinsic motivation for more private identity solutions, such as SSI, is most likely not enough for public sector stakeholders in Kenya to support SSI over traditional centralized systems. In some way or another, intrinsic motivation for more private solutions has to be created in the country. In the current circumstances and conditions, privacy issues are not fully established on the national political and organizational agendas. There needs to be a change in thinking to drive up the information privacy awareness and privacy legislation pressure in Kenya. HOs can play a role in this through lobbying, this is the case according to Stevens and others (Appendix C): "That is essentially what humanitarian organizations do. They lobby and they are a complementary unit to the government." Van der Veen (Appendix C) underscores the importance of involving CSOs in this process: "If the acceptance is not there (for national authorities), I think national CSOs, maybe supported by international organizations, can drive this changing thinking." This is further substantiated by Van der Veen (Appendix C): "In the EU with the GDPR it was also the government that needed to change their own system. Not just the private sector, but also the government. This is not just driven by the government but also by civil society groups. In a well-functioning democracy, CSOs

have quite a lot of power to public policy." Due to the mandate of HOs, it cannot intensively focus on the internal affairs of a country, therefore involving and harnessing national CSOs to mainly drive the change in thinking seems appropriate. Most CSOs in Kenya however fall short in terms of technical understanding and capabilities and have trouble keeping up with the latest technological developments. Therefore, it is important to keep national CSOs informed as HOs. Networks between CSOs in Kenya, such as KICTANet, CONCISE, and BAKE could be leveraged to more efficiently spread the change in thinking. According to Ebert (Appendix C): "In advocacy, it is always good to advocate to someone, which goes home and then advocates to someone else." National CSOs are already pressuring the government with civil law cases, as can be seen with the Huduma Namba initiatives. A very well placed and informed civil law case from a CSO regarding data misconduct could also drive up pressure according to Bolton (Appendix C). Other national actors that could potentially be involved in this process are unelected parties. Van der Veen (Appendix C):" Unelected parties could have quite high power, especially if they get a critical mass of support in the country. They could have these privacy issues within their election program."

6.1.3 Support nurturing principle #3: Protect core values by sticking to mandates in humanitarian demonstration

During the semi-structured interviews, most of the respondents indicated the necessity for proofs of concept or demonstration of SSI as a technological solution. Among others this is brought up by Ebert (Appendix C):" I think building something and then advocating at the same time and building proofs of concept. This has to go hand-in-hand. Advocacy separate from implementation is not super-efficient I would say".

Due to the unique mandate of many HOs, demonstration has to be at least adjacent to humanitarian services. According to Oliveros (Appendix C): "One of the key things we need to be careful of is to be seen as HOs duplicating the work of what the government should be doing. This is not the case, so we need to be really clear in our communication on that." Also, according to Oliveros (Appendix C): "Once you start saying: This is an identity that really encapsulates the acceptance of many of these services, it becomes difficult to really push for as HOs. Part of it is because of mandates, at the end of the day we as HOs are not necessarily mandated to give identities, we are here to provide assistance." By sticking to use-cases adjacent to aid services in humanitarian demonstration of SSI, core values of both HOs and the government can be protected. HOs keep operating within their mandate of providing lifesaving assistance and the governments' mandate of legal identity provision is not directly put under pressure.

One way to demonstrate the technological solution to national stakeholders is by further scaling the current functional systems. Focusing on targeting and registration for humanitarian services is one way to demonstrate SSI within the humanitarian mandate. According to Bolton (Appendix C): "Something that certainly would put pressure on would be to have a few big humanitarian organizations coming together, using a shared SSI as a pilot to provide services to people that are in legitimate need. If those people would lack a government-issued identity for whatever reason." In Kenya, there is currently room for HOs to negotiate some flexibility of KYC regulations for limited functionality services as long as it is for purposes within their humanitarian mandate. For

example, for cases of lifesaving assistance during a limited period of time. This is underwritten by Oliveros (Appendix C):" What would help for them to accept the technology is for it to be used in practical terms, particularly by HOs that are dealing with disasters and things, where they can see how SSI can really empower but also solve some of these privacy issues, compliance and otherwise. Then the acceptability of that would be stronger".

According to Oliveros (Appendix C):" This may be smaller scale, but scale none the less. They get to see that the security and technology is robust, the processes for beneficiaries that are receiving functional credentials or ids." While still limited to aid provision, it is still a way to demonstrate the technology to public- and private stakeholders. Stevens (Appendix C) further highlights how this could affect government support: "If you create a system in such a way that you demonstrate the value of such a system. Where you use interoperable standards. And you are willing to share that technology, so the government might learn from it. Then that could smoothen collaboration." This indicates that humanitarian demonstration could improve the available information and experience with SSI in the country and create understanding in the process for both public stakeholders and beneficiaries. It can also contribute to improving privacy awareness and digital literacy among beneficiaries. Finally, it also has the potential to disarm some of the identity exclusion motives in the country. According to Bolton (Appendix C): "This (humanitarian demonstration) would be stronger if those people are essentially clearly Kenyan, but can't prove it. And if you could show to the government that you can reach these kinds of people with such a system and provide evidence, be clear and accountable and thorough. And show you are not promoting financial terrorism etc." By doing this the humanitarian sector can prove that the proposed system has the potential for addressing unintentional cases of identity exclusion in the country.

A second way to demonstrate the technological solution to national stakeholders can be to demonstrate use-cases adjacent to humanitarian aid services, which are less regulatory pressing and create low friction with government identity mandate. Oliveros (Appendix C): "you can do SSIs, but it does not necessarily have to be linked to regulatory compliance in many cases. We have organizations such as the Australian Red Cross that tries to do SSI for volunteers for instance. In terms of keeping their training credentials. That is less governed by law of regulation. But if you can agree with a group of people that you will accept digital ids for instance, then that might be a good acceptable way as well. So, it could be a stepping stone in terms of some of the acceptability in this case."

6.1.4 Support nurturing principle #4: Broaden the agenda to leverage interest of the private sector

For a transition to a more foundational purpose, such as SIM- and mobile money registration for un(der)documented people, eventually steps have to be made that diverge from the humanitarian mandate. For that, private sector stakeholders seem to be in a good position. According to van der Veen (Appendix C): "Probably, the first one to shift their interest will be mobile network providers and financial service providers. If they are onboarded in pilots to prove the concept. We do see in other countries that financial service providers are the main ones testing identity systems. So, it would be easiest to move them on the axis of interest". Increasing the stakes for the private sector

in Kenya will create additional intrinsic motivation in the country for the national authorities to support the system. This thought is brought up by Van der Veen (Appendix C): “I guess if the private sector has really high stakes then they would also be using their power to talk to the government to get such a system approved”. Certainly, the entanglement of public- and private sector interests in the country and the close engagement between public- and private stakeholders in the country could allow for significant pressure on- and interest for public sector stakeholders when stakes get high enough for the private sector. Van der Veen (Appendix C): “I guess commercial interest or money, in general, would be a big component of moving organizational interest. I don’t know if that is a very sound method. But at least the private sector would be able to see the benefits if it would increase their operational efficiency”. The proposed system already provides some value by dealing with some of the onboarding obstacles for SIM- and mobile money registration, such as the opening of new customer segments and a remote way of verifying information. However, this new customer segment is likely limited in magnitude and only temporarily in nature due to the humanitarian mandate. However, during the interviews, it became clear that due to the open and interoperable nature of SSI systems, there are plenty of opportunities to expand on the commercial interest for the private sector. Lamers (Appendix C) mentioned the innovative perspective as a key incentive for private sector stakeholders: “From an innovation perspective, we (FSPs) are looking at new business models and new potential markets. SSI is interesting for us because there are new business opportunities for us”. By broadening the agenda to private sector business models additional commercial incentives can be created by tackling more of the onboarding obstacles for FSPs and MNOs.

One way to make the proposition of a humanitarian SSI system more attractive to MNOs and FSPs is to implement verifiable transaction data to complement the data of HOs. Oliveros (Appendix C) introduces this extension: “If we start providing digital IDs and then these transactions that beneficiaries have been doing with FSPs are recorded in a way that they could take to an FSP or MNO and they are able to see that actually these communities and these individuals are being responsible with their use of cash or money in general. We see that there is actually value in the data that shows the behavior and the transactions that the beneficiaries have been doing”. This extension would allow for a more complete identity profile and could provide an alternative way to meet the current requirements of KYC and SIM card regulations.

A second way of extending the system to create more interest from private sector service providers would be to include KYC sharing as a use-case. Due to the strict KYC regulations in Kenya, the cost of due diligence for MNOs and FSPs is substantial. Lamers (Appendix C) identified sharing KYC compliancy through verifiable digital credentials as one of the promising use-cases of SSI for FSPs and MNOs. Ebert (Appendix C) Describes the extension as follows:” If not only you could get your credential from a HO to register for a SIM card, but also you could get your SIM registration credential from an MNO you are already registered with and use it elsewhere. This shared KYC through SSI is where then if you use my credential from MNO x to register with FSP x, MNO x gets a little bit of a fee and you essentially share the cost of KYC across the whole ecosystem that would be a huge benefit. “

By broadening the agenda to related SSI use-cases focused on addressing the onboarding obstacles for FSPs and MNOs, significant support can be created among these private sector stakeholders. This may lead to these stakeholders lining up as proponents, creating more internal pressure in the country to support the proposed system. Both extensions are as Ebert (Appendix C) describes: "privacy compliant ways to monetize your user-database. You issue a credential to a user, if they use it to access another service, the requester pays a fee and you get part of that fee". As such these developments probably don't fall within the mandate of HOs. However, Ebert (Appendix C) clarifies that you don't necessarily have to build it yourself, you can build partnerships to do this, such as ID2020."

6.1.5 Support nurturing principle #5: Delay government commitment by initiating network effect through identity provision mandated stakeholders

With the high barrier to getting identity, the strict KYC regulations, and the seemingly low sense of urgency due to questionable identity exclusion motives in Kenya acceptance among national authorities can take a substantial amount of time. Stevens (Appendix C) describes the need for a network effect to take off: "In essence, you need to create a network effect. That you create by having people use it. The bigger the number of people that are using it, the stronger the case for government becomes." Delaying commitment of the government can be a good way to circumvent this lack of acceptance in the short term and still start a network effect. This can either be done by involving stakeholders with a mandate of identity provision they already accept or by temporarily avoiding the national authorities altogether. Oliveros (Appendix C) emphasizes how mandates somewhat ease acceptance for national authorities: "What we are seeing is that if you have a mandate, then that makes it a lot easier to implement something. So, the UNHCR for instance, because of their mandate of refugees, they can provide digital IDs for refugees. And that is accepted because the process of registering refugees is being done with the government officials usually." The UNHCR certificate, while they have a mandate of refugee identity provision in the country and are involved in the refugee and asylum seeker registration process of the country, is still a parallel registration.

Involving UNHCR certificates in a humanitarian SSI system as a credential could be interesting to demonstrate the technology, to create exposure to the government by a trusted organization, and to start a network effect. According to Ebert (Appendix C): "If the UNHCR refugee mandate would be a digital credential, then this verifiability would come with the credential. This would be a benefit of using SSI for this. Because the case where the UNHCR would do the same as the Kenyan government and open their database up for ID checks by any financial service provider, I don't think that would happen. So, there I think SSI would be interesting." However according to Bolton (Appendix C): "For the UNHCR for example, it could be very bureaucratic and slow-moving. I could imagine it could be very difficult to put this (integrating the UNHCR certificate in an SSI system) in as it took quite a long time to get this refugee identity recognized at all (in Kenya). People registered in a refugee identity cannot access national services anyway (in Kenya)."

Stevens describes the potential need to move away from national governments into international use-cases when acceptance is low (Appendix C):" If the national government is hard to get onboard you essentially don't have a choice. You have to demonstrate it to them. Demonstrating that with

international services is the only thing you could do I would say." Bolton (Appendix C) mentions the possibility of creating a network effect in more favorable countries: "Certainly, having the technology in another country work would be helpful." Instead of relying on cooperation of an identity mandated government, the cooperation of the UNHCR international refugee mandate could be leveraged. According to van der Veen (Appendix C): "So especially around migrants and cross-border travel, being able to not having to reregister yourself every time. It could be a compelling use-case for SSI. If each of the supporting organizations in each country has the capabilities to read the identity and to determine the trust they have in it. Which could be challenging. But at least there, there would be not one single government that will block the use of such an identity system." This idea of initiating the network effect by demonstrating the proposed system in countries where there is more humanitarian involvement in refugee and asylum seeker registration is also mentioned by Ebert (Appendix C): "I looked it up at one point, in Cameroon, for example, UNHCR mandates are already accepted for opening bank accounts. I saw some report that said that some banks still do not accept it because they don't trust it. You would really have to find that country, where maybe the government regulation is less of an issue. But a lack of trust by banks and MNOs is more of an issue. Now you can add a layer of trust and verifiability by using SSI." In this way, a network effect can be initiated in countries where regulations are less of a blocking factor. That way, national authorities in Kenya can get better informed, can see a demonstration of the technology, and might allow acceptance to emerge in the country.

6.2 Sub-conclusion of design

This chapter provides an answer to the third research sub-question:

"What support nurturing principles can help HOs to nurture more support for in-name SIM- and mobile money registration of un(der)documented through humanitarian SSI systems in Kenya?"

This was accomplished through the creative participation of several respondents during the conducted semi-structured interviews. In collaboration with the respondents, several approaches for HOs to improve the support limiting circumstances and conditions in Kenya were generated. These insights were synthesized and aggregated in more generally formulated support nurturing principles. The support nurturing principles were subsequently substantiated with information gained from the system analysis. This resulted in a set of five support nurturing principles as displayed in figure 6.2.

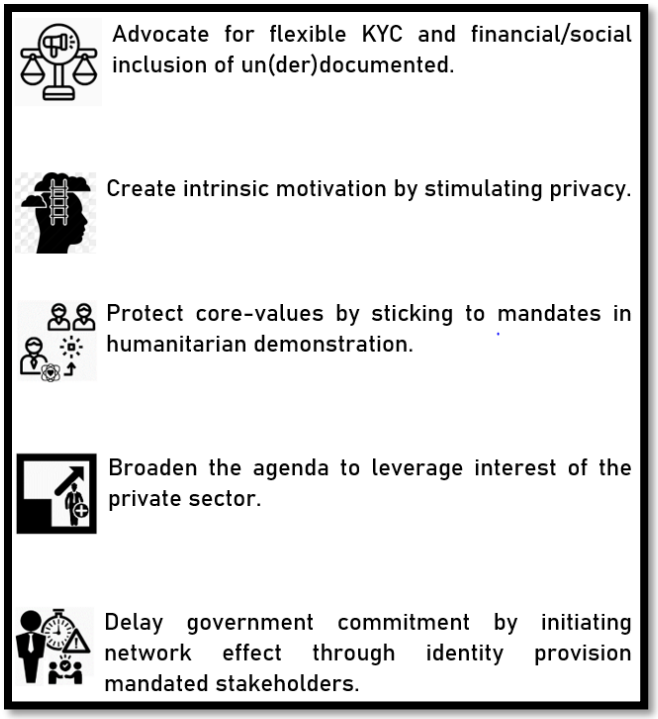

Figure 6.2: Support nurturing principles version 1

7. Evaluation

Before the support nurturing principles are fit for use by the humanitarian sector, they need to be exposed to some form of evaluation. This chapter is focused on the following sub-question: *"Are the support nurturing principles of value in a humanitarian context?"*

In order to answer this question, expert validation is used as displayed in figure 7.1. An expert-interview protocol has been employed, this can be found in appendix D. Two experts, one anonymous individual affiliated with a high-profile HO and the other individual affiliated to ID2020, have been consulted with whom the 5 support nurturing principles were assessed. Based on the expert input, refinements were applied to two of the principles. As a result, this chapter concludes in five evaluated support nurturing principles provided with affiliated implications and risks.

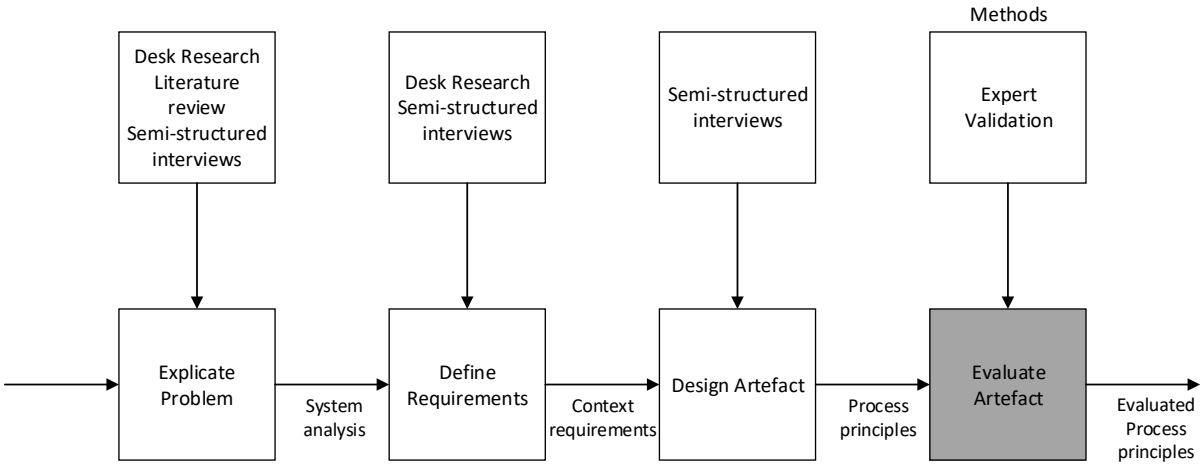

Figure 7.1: Evaluation methods

To arrive at a set of evaluated support nurturing principles this chapter is structured as follows: The assessment of the designed support nurturing principles is presented in paragraph 7.1. The interviews also resulted in final refinements to the support nurturing principles, which are presented in paragraph 7.2. Finally, in paragraph 7.3 a sub-conclusion is presented on the evaluation of the support nurturing principles.

7.1 Support nurturing principles assessment

The feedback obtained in the expert interviews is presented here one by one for each support nurturing principle and a segment for overall feedback has been added. The assessment focused on three things: Firstly, on the usefulness of the support nurturing principle to create support among public- and private sector stakeholders for a humanitarian SSI system. Secondly, on possible risks and disadvantages related to the support nurturing principle. Thirdly, on the usability of the support nurturing principle for the humanitarian sector.

7.1.1 Assessment #1: Advocate for flexible KYC and financial/social inclusion of un(der)documented

Both experts believe this support nurturing principle to be relevant and usable by the humanitarian sector in order to increase support for a humanitarian SSI system. The anonymous respondent emphasizes that advocacy for social and financial inclusion of un(der)documented is already being done by HOs to a certain degree. According to the anonymous respondent, the main argument that will drive governments to instate any kind of identity system is the economic benefit that is going to come when providing people with identities. Both consulted experts agree that there is an argument to be made for flexible KYC advocacy and for fundamentally rethinking the criteria for KYC in Kenya. However, both experts recognize that changing regulation will take a significant amount of time. Slavin adds to this by describing that loose KYC regulation should not be the end goal: "The purpose of KYC guidelines remains relevant. The question becomes how can you achieve it while preserving user privacy and control." Both experts agree that a more productive shorter-term form of advocacy should be aimed at advocating for more defined KYC requirements that are in line with technological developments, so that different ways of meeting the current criteria for KYC can be explored. This is emphasized by the anonymous respondent: "it is better to identify within the current KYC framework what data sets needs to be accumulated in order to create an appropriate picture of the beneficiary so that they might satisfy those KYC restrictions."

7.1.2 Assessment #2: Create intrinsic motivation by stimulating privacy

The usefulness of the second support nurturing principle is perceived differently by both experts. Slavin believes realizing privacy is a critical end goal of a humanitarian SSI system across all layers: "At government level, at the CSO level and also among beneficiaries". This indicates that stimulating privacy is an important part to nurture support for a humanitarian SSI system. The anonymous respondent, however, thinks that stimulating privacy is a very long-haul game. He describes that privacy itself is not going to drive a government to instate any form of identity system. The respondent also states: "Privacy through DIDs can only be fully safeguarded when the services themselves are set up to enable that. At this particular time, they are not." The anonymous respondent does see a role for HOs in ensuring that public knowledge is at a level where individuals understand the importance and relevance of data, not only how to protect data but also how to use it. Slavin acknowledges this support nurturing principle as something that should be done by the humanitarian sector. Especially given to the unique positions of HOs, which operate in context and work with beneficiaries that no other organizations do, HOs should be a part of the privacy conversation. HOs could do a better job of doing digital literacy training with beneficiary communities so they understand for instance: what are some of the risks involved with sharing your data. Slavin advises that as HOs become increasing contributors to the privacy conversation, they ought to continue to engage with outside privacy, as privacy as a topic is complex and quickly evolving.

7.1.3 Assessment #3: Protect core values by sticking to mandates in humanitarian demonstration

The third support nurturing principle is received in a positive way by both experts. Slavin confirms the importance of using lateral services to create and demonstrate more awareness and more functionality for humanitarian SSI systems: "If HOs can show governments that using these

models of D-ID they are reaching more people, they can go a long way towards proving the concept." Sticking to core values, especially "Doing no harm", mitigates a lot of risks that are associated with these technologies. This should constantly be the bottom line. The anonymous respondent attests to this idea but suggests a different formulation of the support nurturing principle: "Identifying small scale prototype initiatives and demonstrate them in line with humanitarian core values." Furthermore, the anonymous respondent confirms that adjacent use-cases such as educational certification platforms are a viable way of demonstrating SSI technology due to its low barrier to entry. There are several things HOs should be aware of when demonstrating even within the humanitarian boundaries. One risk has to do with overinflating the inclusion ability of SSI. When illustrating the comparison of how many more people HOs are reached using SSI over traditional systems, it needs to take into account that some of these people were already getting access to aid using alternative informal methods (such as through guardianship or a friend). In addition to that Slavin emphasizes that when branching out to lateral services HOs need to be cautious to prevent function creep in terms of unintentionally creating more exclusion. However, this should be mostly prevented by sticking to core values. The respondents agree that this support nurturing principle is usable for the humanitarian sector, especially because SSI is very relevant for use in the already existing registration and targeting of HOs, and HOs can more easily test them within the humanitarian enclave instead of a larger government-approved process.

7.1.4 Assessment #4: Broaden the agenda to leverage interest of the private sector

Both experts believe this to be a useful support nurturing principle to nurture support for a humanitarian SSI system, but only in the right context. Working with private sector stakeholders to further identify key value propositions that would benefit them is useful to increase the stakes for these organizations. The anonymous respondent agrees with the statement that private sector stakeholders have a significant influence on political decision making in African countries. However, both respondents acknowledge that there is a difference in agenda, meaning that the type of influence and the exercise of private sector influence may not always be in line with humanitarian interests. Slavin warns that by making the extension of an SSI program in the humanitarian sector rely too much on a business case, it creates a risk for the exclusion of commercially less-interesting areas. This goes against the humanitarian core value of neutrality. Both Slavin as well as the anonymous respondent see this as part of a potential humanitarian strategy. They especially see value in the extension of a verifiable transaction history as a way to both increase the interest for the private sector and to alleviate some of the onboarding restrictions. Slavin warns however that when extending the system with more functionality, non-correlatability should be a focus. Mitigation of the mosaic effect, the ability to reidentify using discrete pieces of data, should be built in the design of the system especially when it is extended with more functionality.

7.1.5 Assessment #5: Delay government commitment by initiating network effect through identity provision mandated stakeholders

The experts are skeptical about the usefulness of this support nurturing principle. Slavin argues that to provide functional ID, government involvement is not always necessary. Though governments and traditional trust anchors will continue to remain key stakeholders in the ID space, in the future more forms of ID verified by a greater variety of trust anchors will likely begin to

evolve. This indicates that you don't have to be dependent on the government to start this development. However, it is definitely not applicable in every context, as in some cases governments could be the biggest contributor. The anonymous respondent is mostly skeptical about starting a network effect through the integration of something like the UNHCR refugee certificate as a verifiable credential. According to the respondent: "Refugees and asylum seeker registration is a very specific environment and governments actively exclude refugees from national financial services due to the temporality of the refugee in that country. Not all, but many don't want refugees to have access to financial services because they don't want refugees to be more permanent than they should be. If the government is not cooperating because they don't want people to access the financial system, it is not because of the way in which I am delivering the identity." This implies that relying on other identity provision mandated stakeholders in Kenya, such as the UNHCR, will not significantly strengthen the case for private service access for refugees and asylum seekers in the country. However, Slavin still sees potential to prove the concept and to start a network effect in more favorable countries, with less strict onboarding obstacles. In his opinion, adoption of the proposed system will not follow the same steps in every country and both experts agree that when network effects start to take hold in neighboring countries (as a proof of value), that will ease the emergence of support for these systems in Kenya.

7.2 Support nurturing principle refinements

During the assessment by the two consulted experts, several refinements and nuances came up that should be applied to a final design. This justifies the composition of a second version of the support nurturing principles in order to provide a more complete answer to the main research question. In this paragraph, the refinements are discussed.

With respect to the first support nurturing principle, the experts agreed with the support nurturing principle, but both suggested that the emphasis of advocacy should be on working with the Kenyan government to define ways of satisfying the current KYC criteria. Flexible KYC suggests that KYC should be loosened for access in specific contexts, for example in order to provide life-saving assistance. While this is also relevant to advocate for, loose KYC criteria should not be the end-goal. As such the second version of the first support nurturing principle will include this aspect of advocating for better-defined KYC rules.

The second support nurturing principle is left unchanged. This is despite one of the experts being doubtful of the usefulness of this support nurturing principle as according to him privacy is not the deciding factor in driving governments to instate any form of identity system, the economic benefit is. In addition to this, he adduced that full privacy through SSI and DIDs is currently not possible due to the side of existing services not being set up to support this. This research does not deny these issues, instead, it makes the argument that an intrinsic sense and pressure of privacy among national stakeholders is required to on the one hand make the privacy that comes with SSI a deciding factor to drive governments to choose for this specific type of IdM over centralized identity systems and on the other hand to ensure that these type of systems can actually safeguard privacy across the whole ecosystem.

The third support nurturing principle is also left unchanged. The support nurturing principle was positively received by both experts. The anonymous respondent suggested to formulate this

support nurturing principle differently, however, in the suggested formulation the protection of core values aspect is underappreciated. This is a crucial aspect because it is both the core values of HOs and government core values that are protected in this support nurturing principle.

The fourth support nurturing principle remains yet again unchanged as it was well-received by both experts.

Finally, during the assessment of the fifth support nurturing principle, it became clear that starting a network effect in Kenya by relying on identity provision mandated stakeholders, especially in the area of refugees and asylum seekers, is not as promising as initially seemed to be the case. Changing the way in which identity or registration information is delivered will most likely not change the stance of the Kenyan government on service access. Especially not in the case of refugees and asylum seekers, as it is in the interest of the government to deliver a message of temporality. However, during the assessment, it became evident that network effects can still be initiated in other countries with less strict onboarding obstacles. Due to this, the second version of the fifth support nurturing principle will be limited to delaying government commitment by initiating network effects in other countries.

7.3 Evaluation Sub-conclusion

This chapter answers the fourth research sub-question:

"Are the support nurturing principles of value in a humanitarian context?"

In order to answer this question, two industry experts were consulted. In interviews with these experts, the five support nurturing principles were assessed on usefulness, usability in the humanitarian sector, and on related disadvantages and risks. As a result of the assessment, two significant refinements were applied to the support nurturing principles. Firstly, both experts acknowledged the usefulness of advocating for flexible KYC to enable shorter-term demonstration options, however during the assessment it became clear that this should not be the longer-term end goal. Instead advocating should have an emphasis on further defining existing KYC regulations to be more up to date with new identity management solutions. Secondly, the assessment led to the conclusion that relying on identity provisioned stakeholders, other than the Kenyan government, only delays government commitment when it is kept outside of the Kenyan borders. This is especially the case when establishing a network effect through refugees and asylum seekers. After refinement, all five support nurturing principles were found to be of value in a humanitarian context. The evaluated support nurturing principles, provided with identified implications and risks, is displayed in figure 7.2. The support nurturing principles that were refined in the evaluation chapter are marked with an asterisk. Affected requirements were highlighted bold in the implications section.

	Humanitarian support nurturing approach			
	#	Process principle	Implications	Risks
	1*	**Advocate for further defining of KYC, flexible KYC and financial/social inclusion of un(der)documented***	• Allow for existing **onboarding obstacles** to be met by innovative solutions. • Allow for further KYC exemptions for humanitarian purposes, enabling further demonstration oppertunities. • Discourage intentional exclusion and thus improves the **identity exclusion motive** in the country.	• Changing regulation does require long term commitment. • Flexibility in KYC could lead to encouraging a less rigorous system.
	2	**Create intrinsic motivation by stimulating privacy**	• Stimulate **information privacy awareness** and **digital literacy**. • Stimulate **privacy legislation pressure**. • Increase intrinsic economic and societal value of privacy and private systems.	• Stimulating privacy is a long term process. • Privacy is a complex and quickly evolving topic. A lack of continuous due dilligence from involved HOs can do more harm then good.
	3	**Protect core-values by sticking to mandates in humanitarian demonstration**	• Allows for a proof of value/concept with minimal political obstacles. • Creates exposure of the technology to public- and private sector stakeholders, more direct exposure is possible through lateral services. • Increases **information and understanding of SSI**. • Increase **information privacy awareness** and further increases **online accessibility** factors such as **digital literacy** among beneficiaries in practice. • Can potentially emphasize value of rectifying unintenional exclusion, disarming intentional **identity exclusion motives**.	• Overinflating the value in terms of inclusion potentioal of SSI. • Function creep and unintenional exclusion when scaling to lateral services. • Risk of losing innovation budget.
	4	**Broaden the agenda to leverage interest of the private sector**	• Alleviates **onboarding obstacles** by enriching identities with private sector data. • Can create direct commercial incentives, by including SSI use-cases such as KYC sharing. • Creates **exposure of SSI technology** to private sector stakeholders. • Increased private sector interest creates pressure on government stakeholders on a national level.	• Due to differences in core values between HOs and the private sector, friction can arise between neutrality and commercial interest. • There is a risk of correlatability of data when extending functionality.
	5*	**Delay government commitment by initiating network effects abroad***	• Expand through the way of minimal political resistance. • Allows for proof of value/concept, increasing **degree of information and knowledge of SSI**.	• Missing out on government capacity and expertise.

Figure 7.2: Final version of support nurturing principles (refined after validation, implications on requirements in bold)*

8. Conclusions and Discussion

In this chapter, the results of the study are concluded and discussed. In paragraph 8.1 an answer to the main research question is formulated through the confluence of the in the research covered sub-questions. Paragraph 8.2 goes into the implications which the research suggests for the scientific community and society. Subsequently, paragraph 8.3 covers the limitations of the conducted research. Then paragraph 8.4 the research is reflected on. Followed by paragraph 8.5, that describes the options for further research. Finally, in paragraph 8.6 recommendations are done for the research partners.

8.1 Conclusions

This research is aimed to further explore opportunities for humanitarian SSI systems to increase the efficiency of humanitarian aid by creating social and financial inclusion. By employing a Design Science Research and systems engineering approach the research problem as identified in chapter 1 was scoped down to the following main research question:

"How can humanitarian organizations nurture support for humanitarian SSI systems as a way to facilitate in-name SIM- and Mobile money registration for un(der)documented in Kenya?"

In order to make this main research question more manageable, it was divided into four sub-questions. These sub-questions were addressed in chapters 4 to 7. Together they form an answer to the main research question. The 4 sub-questions will briefly be addressed below:

Sub-question 1: *"What is the socio-technical context of the Kenyan identity (registration) ecosystem?"*

In order to answer this sub-question a combination of desk research, literature review, and semi-structured interviews have been conducted. This resulted in a system analysis of the Kenyan identity ecosystem. This takes into account: technical systems, the institutional environment, and the stakeholder landscape. This has resulted in three lists of bullet points, describing a bird's eye view of the state of technical, institutional and stakeholder circumstances and conditions in the country. Furthermore, during the system analysis, it became clear that national stakeholders, both national authorities and FSPs/MNOs, have significant blocking power and essential resources that are required for a transition to a more foundational purpose. However, from the perspective of these stakeholders there does not seem to be enough interest and sense of urgency to fully support the development of a humanitarian SSI system. As a result of these insights, the scope of the research was slightly adjusted. Where initially the research had the intention of a full process design, it now is focused on exploring how support can be nurtured by HOs using process principles. Accordingly, the rest of this research is focused on this process challenge of creating more support among public- and private sector stakeholders in the country.

Sub-question 2: *"What are local circumstances and conditions in Kenya that drive or constrain the support of important public- and private sector stakeholders to facilitate SIM- and mobile money registration of un(der)documented through a humanitarian SSI system?"*

For this second sub-question, semi-structured interviews were used together with desk-research. Six respondents, with an affiliation to (humanitarian) SSI development, were consulted. The respondents were challenged to identify support driving and constraining circumstances and conditions for a (humanitarian) SSI system. These insights were checked against Technology Acceptance Modeling factors. Using the combined tacit knowledge of the respondents an assessment framework was composed. The findings gained during the technical-, institutional- and stakeholder analysis sub-conclusions were used to fill out the framework for the case of Kenya. Based on this assessment, which is displayed in figure 8.1, several possible changes to the local circumstances and conditions in Kenya were identified using this framework to increase the support of public- and private sector stakeholders for a humanitarian SSI system as a way to facilitate SIM- and mobile money registration of un(der)documented. The local circumstances and conditions #1, #2, #4 - #8 as displayed in figure 8.1 were found to be unfavorable or moderately unfavorable for the Kenya case. Therefore, improving on these identified circumstances and conditions in Kenya provides a way to increase the support of public- and private sector stakeholders in the country for the proposed humanitarian SSI system.

Suitability: / Local Circumstance / condition:	Unfavorable:	Moderately unfavorable:	Moderately favorable:	Favorable:
Privacy Legislation pressure	No Data protection legislation.	Consent focused data protection legislation which stimulates hedging against data breaches and data misconduct.	Legislation enforcing private sector data handling accountability which stimulates data responsibility offloading.	Legislation enforcing public and private sector data handling accountability which stimulates data responsibility offloading.
Information Privacy Awareness	Unaware of the elements* related to information privacy	Knowledge of the elements* related to information privacy.	Understanding that elements* related to information privacy exist in the current environment.	Projection what impact elements* related to information privacy have in the future.
Online accessability	Low mobile network coverage, low mobile phone penetration, insufficient access points in rural areas and low digital literacy.	Average / High mobile network coverage, low mobile phone penetration, some central access service points in rural areas and low digital literacy.	High mobile network coverage, average mobile phone penetration, wide spread central access service points in rural areas and some digital literacy.	Full mobile network coverage, high mobile phone penetration also in rural areas,wide spread central access service points and high digital literacy.
Identity exclusion motive	Mainly intentional exclusion.	Mixed intentional/ unintentional exclusion.	Exclusion mainly unintentional due to a burden of proof or cost for individuals.	Exclusion mainly unintentional due to lack of government registration capacity or voluntary exclusion due to privacy / security concerns.
Financial service onboarding obstacles	strict KYC restrictions.	KYC restrictions & limited remote registration.	KYC restrictions, limited remote registration & limited access to high risk areas.	Loose KYC restrictions, limited remote registration & limited access to high risk areas.
SIM card onboarding obstacles	strict KYC restrictions.	KYC restrictions & limited remote registration.	KYC restrictions, limited remote registration & limited access to high risk areas.	Loose KYC restrictions, limited remote registration & limited access to high risk areas.
Degree of information and knowledge of SSI	No understanding of SSI technology or value proposition. Not much available information.	Some knowledge and information on SSI value proposition, low technical understanding. No exposure and experience with the technology.	Sufficient understanding of SSI technology and value proposition. Low exposure to the technology.	Broad spread understanding of SSI value proposition and technical understanding. Exposure / experience with the technology.
Humanitarian involvement in Refugee and Asylum seeker registration process	Host Government-Led registration	Joint-Led, Parallel HO registration	Joint-Led	Humanitarian Agency-Led
Identity information asymmetry	Identity information symmetry between stakeholders	Low identity information assymetry between stakeholders	High Identity Information assymetry between stakeholders	High Identity Information assymetry between stakeholders. Especially with HOs.

Figure 8.1: Circumstances and conditions assessment framework filled out in yellow for Kenya case.

Sub-question 3: *"What support nurturing principles can help HOs to nurture more support for in-name SIM- and mobile money registration of un(der)documented through humanitarian SSI systems in Kenya?"*

The generation of design options was done through a creative process in the semi-structured interviews. The same six respondents were challenged to generate possible strategies for HOs to improve the identified local circumstances and conditions. The insights of the respondents were aggregated, combined, and substantiated with information of the system analysis, resulting in the first version of five support nurturing principles as displayed in Table 8.1.

#	Support nurturing principle:
1	Advocate for flexible KYC and financial/social inclusion of un(der)documented.
2	Create intrinsic motivation by stimulating privacy.
3	Protect core-values by sticking to mandates in humanitarian demonstration.
4	Broaden the agenda to leverage interest of the private sector.
5	Delay government commitment by initiating network effect through identity provision mandated stakeholders.

Table 8.1: First version of support nurturing principles

Sub-question 4: *"Are the support nurturing principles of value in a humanitarian context?"*

This sub-question has the function of ensuring that the five designed support nurturing principles actually have value for HOs to create a more SSI supportive environment in Kenya. This is done by consulting two experts. In the expert assessment, the five support nurturing principles were found to be of value in a humanitarian context. However, based on the expert input, two refinements were made to the first and fifth support nurturing principles. This has resulted in the final version of the support nurturing principles, provided with implications and risks, as displayed in figure 8.2.

	Humanitarian support nurturing approach			
	#	Process principle	Implications	Risks
	1*	**Advocate for further defining of KYC, flexible KYC and financial/social inclusion of un(der)documented***	• Allow for existing **onboarding obstacles** to be met by innovative solutions. • Allow for further KYC exemptions for humanitarian purposes, enabling further demonstration oppertunities. • Discourage intentional exclusion and thus improves the **identity exclusion motive** in the country.	• Changing regulation does require long term commitment. • Flexibility in KYC could lead to encouraging a less rigorous system.
	2	**Create intrinsic motivation by stimulating privacy**	• Stimulate **information privacy awareness** and **digital literacy**. • Stimulate **privacy legislation pressure**. • Increase intrinsic economic and societal value of privacy and private systems.	• Stimulating privacy is a long term process. • Privacy is a complex and quickly evolving topic. A lack of continuous due dilligence from involved HOs can do more harm then good.
	3	**Protect core-values by sticking to mandates in humanitarian demonstration**	• Allows for a proof of value/concept with minimal political obstacles. • Creates exposure of the technology to public- and private sector stakeholders, more direct exposure is possible through lateral services. • Increases **information and understanding of SSI**. • Increase **information privacy awareness** and further increases **online accessibility** factors such as **digital literacy** among beneficiaries in practice. • Can potentially emphasize value of rectifying unintenional exclusion, disarming intentional **identity exclusion motives**.	• Overinflating the value in terms of inclusion potentioal of SSI. • Function creep and unintenional exclusion when scaling to lateral services. • Risk of losing innovation budget.
	4	**Broaden the agenda to leverage interest of the private sector**	• Alleviates **onboarding obstacles** by enriching identities with private sector data. • Can create direct commercial incentives, by including SSI use-cases such as KYC sharing. • Creates **exposure of SSI technology** to private sector stakeholders. • Increased private sector interest creates pressure on government stakeholders on a national level.	• Due to differences in core values between HOs and the private sector, friction can arise between neutrality and commercial interest. • There is a risk of correlatability of data when extending functionality.
	5*	**Delay government commitment by initiating network effects abroad***	• Expand through the way of minimal political resistance. • Allows for proof of value/concept, increasing **degree of information and knowledge of SSI**.	• Missing out on government capacity and expertise.

Figure 8.2: Final version of support nurturing principles (refined after validation, implications on requirements in bold)*

Based on the performed research process as just described the following conclusions can be drawn with regard to the main research question: *"How can humanitarian organizations nurture support for humanitarian SSI systems as a way to facilitate in-name SIM- and Mobile money registration for un(der)documented in Kenya?" :*

The scaling of humanitarian Self-Sovereign Identity systems, especially when transitioning to a more foundational purpose, such as the facilitation of SIM- and mobile money registration, relies on the cooperation and joint-development of stakeholders within an already existing and

functioning identity ecosystem. With identity being deeply rooted in a broad spectrum of different organizations, simply one-sidedly introducing a technological solution in Kenya such as SSI will result in insufficient support to realize such a system.

From an international perspective SSI, as an identity management system, is currently perceived to be a very interesting, private, promising and function creep resistant solution to solve un(der)documentation and exclusion in a user-friendly way. However, this sense of value is not always shared by national stakeholders, which operate in a completely different socio-technical environment. As a result, HOs should not currently assume the same level of support from national stakeholders to drive these initiatives.

This research argues that support among these national stakeholders can be nurtured by HOs by understanding the local circumstances and conditions in Kenya and to nurture support by shaping more favorable circumstances and conditions in the country. To do this, five support nurturing principles were identified which can be used by HOs. These principles, as displayed in figure 8.2, were found to be appropriate for use in the humanitarian sector by two experts.

Over the course of the research process other related findings were produced:

The assessment framework in figure 8.1 provides insight in the suitability of several local circumstances and conditions in a country for a humanitarian SSI system. This could be used in further scientific work to assess other countries. However, this framework does come with several limitations as discussed in this research. The scientific contribution from this framework should therefore not be interpreted as a full assessment guide, but it's nine assessment categories as displayed in table 8.2 do provide a base to understand and assess suitable circumstances in countries similar to Kenya.

Table 8.2: Categories of local circumstances and conditions assessment framework.

#	Local circumstances and conditions assessment categories:
1	Privacy legislation pressure
2	Information privacy awareness
3	Online accessibility
4	Identity exclusion motive
5	Financial service onboarding obstacles
6	SIM card onboarding obstacles
7	Degree of information and knowledge of SSI
8	Humanitarian involvement in refugee and asylum seeker registration
9	Identity information asymmetry

Refugees and asylum seekers are a part of the un(der)documented group which at first glance seems alluring to integrate in a focused SSI use-case to demonstrate the technology, initiate a network effect, and improve the local circumstances and conditions while delaying the commitment of the Kenyan government. Added to this is the fact that there is already some humanitarian involvement in the registration process of this group by the UNHCR. However, due to the continuous inflow of refugees and asylum seekers in the country, this has become a political

issue. It is in the interest of Kenya as a host country to send a message underlining the temporality of their stay. Due to this, HOs should not focus their development efforts of humanitarian SSI systems specifically on refugees and asylum seekers, despite that being a promising use-case.

The support for a humanitarian SSI system for in-name SIM and mobile money registration goes hand in hand with a political issue: The extent to which governments want to include these people in the first place. This is a technology-agnostic issue, but nevertheless dictates support for humanitarian SSI systems. This research attempted to tackle both issues at once, but in reality, before getting stakeholders to support a specific way to deliver identity, there must be support to provide identity in the first place. Humanitarian SSI systems are currently driven through international interests; However, for a more foundational purpose, intrinsic motivation on national level for SSI systems and for identity inclusion in general needs to be created.

8.2 Implications

The findings in this research have implications on both scientific and societal levels. The implications are presented accordingly.

8.2.1 Scientific implications

This research contributes on a scientific level in several ways. The research continues in line with earlier humanitarian research by exploring the potential of (humanitarian) SSI to create inclusion. It contributes to this by combining the knowledge of several industry experts. In this way, it provides novel insights in some important circumstances and conditions in a country that can drive or inhibit the acceptance of inclusion focused SSI systems. Furthermore, it provides a framework using which the state of these circumstances and conditions can be assessed in a country, be it that the country is similar to Kenya in terms of political structure and stableness.

Furthermore, the research shows how some of the challenges resulting from the widespread and diverse identity stakeholder landscape can be harnessed using support nurturing principles. Finally, SSI research concluded that implementation very much needs to be dictated per use-case and the context in which it is to be implemented. This research provides a practical example of how a process design can contribute to dealing with context-dependency.

8.2.2 Societal implications

This research also contributes on a societal level in several ways. Firstly, it contributes directly to organizations active in humanitarian SSI initiatives, such as the “121” consortium. The research provides a first exploration, from a process perspective, in the further scaling of humanitarian aid systems. Integrating the five identified support nurturing principles into a more complete process design has the potential to increase the chance of succeeding in advance, by shaping circumstances and conditions so that support among crucial public- and private sector stakeholders is more likely. Furthermore, this research contributes to society by laying the foundations for an easier pathway from functional to foundational SSI systems, potentially allowing for more inclusion in countries tormented by identity exclusion.

8.3 Limitations

Several limitations arise for this research due to the choice of research scope and research methods:

Research scoping limitations

The scope of the research is focused on creating the right environment in a country to allow for support to emerge among national public- and private stakeholders. However, by choosing to isolate circumstances and conditions as a way to create support, it has left out other aspects such as inter-stakeholder relations that could be leveraged.

Secondly, the scope of this research is only focused on how to nurture support. While this is a significant part, it does not entail a full process design. By leaving other process aspects out of the design scope, it cannot be ensured that the designed support nurturing principles do not interfere with other process challenges.

Thirdly, the scope of this research is focused around the case of Kenya. This means that when generalizing the findings of this research to other countries, it is limited to countries in a similar situation. For example, it will be hard to generalize the findings to countries which find themselves in geopolitical sitations of extreme conflict such that private sector services can not function properly. Or for that matter to countries with an authoritarian government or a functioning foundational identity system.

Design Science Research limitations

The research used a DSR inspired approach. However, demonstration of the artefact was left out of scope due to feasibility reasons and due to the nature of the artefact. This means that the evaluation has only been performed on a theoretical level. The results of the designed support nurturing principles in a practical situation are still to be determined.

System analysis limitations

For the exploration of stakeholder interests and perceptions in the stakeholder analysis, the research mostly relied upon the insights of industry experts, instead of interviewing the stakeholders themselves. This may have introduced a bias, as the respondents could be more ideological with regard to certain aspects in their assessment as proxy compared to some of the actual stakeholders.

Secondly, the Kenyan identity ecosystem is an extremely large system lacking well defined boundaries. Due to the mere size of the system and the limited resources available to this system, only a birds-eye-view was provided with this system analysis. For a more complete analysis, the analysis should be split up in the analysis of smaller sub-systems.

Requirements limitations

The requirements in this research take the form of several circumstances and conditions that need to be improved to allow for more support among public- and private sector stakeholders for a humanitarian SSI system. However, no distinction has been made to what extent specific circumstances limit support. As a result, this research only provides insight into several ways to create support, but not to what extent they create it, what the best way is to create it, and no prioritization between support driving or constricting factors has been made. Additionally, no full program of requirements was made to which an artefact was evaluated in a later stage.

Assessment framework limitations

The assessment framework was discussed during the expert interviews. One aspect that was identified by one of the experts, that should be reflected in the framework, is the trust of institutions. The respondent noticed that especially the trust towards HOs is an important factor. This should be included in a second version of the framework. In this research a second version was not composed, as the respondent identified that the trust in HOs in Kenya is very high. Therefore, it would not have provided additional options for the design for an artefact for Kenya in particular. However, this should be taken into account when assessing other countries.

The generalizability of the assessment framework is limited to countries in a somewhat similar situation to Kenya. HOs should do additional extensive due diligence in identifying whether a country is suitable for this humanitarian innovation. This research and the resulting framework can be used to support this process, but should by no means be interpreted as a full guide.

Design limitations

The generation of the design was done in conjunction with (humanitarian) SSI innovators. By relying only on the input of these respondents a certain bias was introduced. On the one hand, by relying purely on the insights of affiliated individuals' solutions were designed that have a high chance to be actually of use for the humanitarian sector. On the other hand, it may have left out other innovative options.

Semi-structured interviews limitations

Four limitations were identified with respect to the semi-structured interviews. Firstly, due to the Covid-19 pandemic that broke out during this research, all interviews were conducted through online (video) calls. Due to the nature of online interviews, the interviewer tends to miss out on non-verbal communication and goes at the expense of interview quality in general. Secondly, the number of respondents which I reached during my interview (six), is not as much as anticipated in earlier stages. This may have been in part due to the ongoing pandemic. Thirdly, during my interviews I noticed that my research contains several sensitive topics for respondents that have an ongoing collaboration with foreign governments. Especially around the topic of intentional exclusion and corruption this resulted in very neutral responses, not voicing their actual opinion by remaining politically correct. Fourthly, interviews were mostly done with respondents related to SSI initiatives. In order to get a more complete perspective of stakeholder perspectives, government and private sector stakeholders in Kenya should have been interviewed. Fifthly, the same respondents of the semi-structured interviews were used throughout different phases of the research. On the one hand this was useful to guide respondents in to the generation of design alternatives, by involving them in the thought process. On the other hand, a case can also be made for separating respondents among the different research steps. As this can potentially reduce bias in the research.

Evaluation and Expert validation limitations

The validation by experts in this study may suffer from a limited number of respondents. Only two experts were consulted during the expert validation interviews. While these experts were highly qualified, including the perspective of more experts could have resulted in a more thorough evaluation of the artefact.

8.4 Reflection

When looking at the underlying problem of un(der)documentation in most countries, including Kenya, the nature of this problem is not a technical one, as there are plenty of technical solutions available to provide people with a foundational form of identity; rather, the core of the issue can be traced back to political roots and institutional failure. This is illustrated by many other (African and Western) countries having drastically higher rates of registration among their population, without resorting to alternative forms of identity management. This raises the question of whether providing another technical alternative, in the form of a (humanitarian) SSI system, is the best way of addressing this problem. These systems do provide advantages over traditional identity management systems, such as increased privacy, more function-creep resistance, and higher transparency. However, currently, these are mainly advantages valued by the humanitarian sector and not directly contributing to solving the lack of identity. From a systemic perspective, technological change is probably not the most optimal way to address this issue, but solutions in the institutional realm are.

From the perspective of the humanitarian sector, however, a different light is shed on the problem. Bringing about direct institutional change in a foreign country is out of reach for HOs. Their options remain limited to complementary roles. Even so, introducing a purely technical complementary solution in a foreign country, especially in something as fundamental, foundational, and delicate as identity does not seem fruitful per se, as it can be perceived as a somewhat colonialistic approach. There are several aspects unique to SSI and distributed systems that do justify the choice to engage in humanitarian innovation. The most important aspect being the relative neutrality of the technology. Due to the distributed nature of SSI technology, there is no single party that controls or solely profits from the platform. This creates a level playing field between all stakeholders, ensures transparency about the subject system for all stakeholders, and allows for trusted and verifiable interactions between these stakeholders. Therefore, it can act as a vehicle to facilitate institutional change. This is especially the case if such a system is developed in collaboration with national stakeholders, and by open-sourcing the development. In this case, the choice to engage in humanitarian innovation seems justifiable, not only because SSI has the potential to leverage information asymmetry between national stakeholders as a technical solution to the identified problem, but also because it provides a unique type of open collaboration which engages stakeholders to get around the table to jointly address this issue. This second aspect gives humanitarian SSI innovation an edge over introducing traditional centralized systems as a solution.

Even though the usefulness of pursuing an SSI solution is justifiable for the humanitarian sector, that is not to say that it is without risk. Jacobsen & Fast (2019) describe in their research that governance of access to digital data collected from humanitarian subjects with technological solutions has changed: “access is no longer only about challenges of gaining access to vulnerable populations, but also about challenges of preventing access to vulnerable digital bodies and their use for aggressive purposes”. This should raise the question for humanitarian innovators if this is an innovation that they want to pursue and whether they can manage to do so in a responsible way. Theoretically, an SSI system should be more resistant to function-creep and thus more resistant to use for these aggressive purposes. This perception was also adopted during this research. However, this does assume a proper implementation, which is not only in the hands of HOs. And even though

the final system may be function-creep resistant, the process of getting to that point will probably be full of missteps and leaks. This is especially the case when innovating with a novel technology such as blockchain technology. In addition to this, Sandvik, Jumbert, Karlsrud, & Kaufmann (2014) point out an important difference with private sector innovation: "humanitarian actors operate in environments that are intrinsically dynamic and unstable and that diverge from the typical environment in which technology is designed, such as the private sector. In the emergency context, the failure rates of sophisticated technologies are likely to be high." What particularly contributes to this uncertainty regarding the responsibleness of this innovation is the necessity of involvement of public- and private organizations when aiming for in-name service registrations, as these organizations are not subject to humanitarian principles. According to Sandvik et al. (2014), this creates a dilemma: "victims of disasters are by nature in a vulnerable position, making them potentially easy targets for private companies' interests and easy victims of breaches to their right to privacy, as they may be pressed in situations of emergency to accept things they wouldn't have otherwise." This can even create problems that fall outside of the end-points of the SSI system, as at some point personal information has to be handed over for private sector service registration. In addition to this, Sandvik, Jumbert, Karlsrud, & Kaufmann (2014) warn that introducing technologies like SSI creates dependencies such as the availability of network coverage, cell phone ownership, sufficient technical and financial literacy among the beneficiaries. Ultimately, this can be seen as a tradeoff between protection versus efficiency. On the one hand, humanitarian aid can be provided more efficiently by facilitating private sector services for un(der)documented people through self-sovereign identities. On the other hand, this same un(der)documentation might be what protects these people from further marginalization and abuse, and sticking to direct in-kind aid may be the safer choice. This is an especially difficult trade-off for SSI technology because the very system design is supposed to protect its subjects from abuse originating in function-creep and lack of privacy. However, the process of getting to a level of technology maturity in which humanitarian values can comfortably be ensured takes time. This leads me to believe that if HOs choose to further pursue this innovation, the responsible way of doing so is by keeping as much of this maturity process within the boundaries of the humanitarian sector. Within these boundaries, the risks that come with such a maturity process can be absorbed and defused by humanitarian principles such as 'do no harm', neutrality and impartiality. In contrast, when transitioning to a foundational purpose too early, stakeholders that are not accountable to these principles may be tempted to abusive behavior.

Finally, if HOs decide that humanitarian SSI innovation is worth pursuing and decide that it is manageable to do that in a responsible way, that raises the question of whether this is appropriate in the context of other African countries as well. This research acknowledges that every country requires its own unique approach and in some countries pursuing a humanitarian SSI innovation is simply not worth it. That is the reason why the support nurturing principles are presented uniquely for Kenya and why the assessment framework is applicable in a more general setting. However, for example, in countries with authoritarian governments, the assessment framework will not provide any base for a support nurturing approach. Several of the requirements, such as favorable information privacy awareness, are linked to an increase in the perception of value for public- and private sector stakeholders. However, this is based on an assumption of a democratic society. In an authoritarian society, public sector stakeholders will not experience extra pressure

due to an increase in civil information privacy awareness. Secondly, countries in extreme conflict are most likely not suitable for this approach as well. As private sector service provision may not be in a reliable functioning state. Concluding, this research does provide a framework using which HOs can generate unique support nurturing approaches for other countries. However, the generalizability is limited to countries in a somewhat similar situation to Kenya. HOs should do additional extensive due diligence in identifying whether a country is suitable for this humanitarian innovation. This research and the resulting framework can be used to support this process, but should by no means be interpreted as a full guide.

8.5 Further Research

Based on the identified limitations and questions that came up during this research several recommendations can be provided in terms of future research opportunities:

How to structure and manage collaboration with a full process design when a suitable stakeholder landscape state has been reached?

Due to the scope limitations of the research, there is still a need for a process design beyond the nurturing of support. Creating the right circumstances and conditions is just one of the process challenges which creates the right foundations to initiate a longer process. For (humanitarian) SSI systems to transition to a more foundational purpose, especially in the case of financial and social inclusion, long-term collaboration is required. A broader process design is needed to ensure and manage the participation of stakeholders, structure commitment, and define process rules for different phases of the process. When designing a more complete process design, it is important that interviews with the actual stakeholders are performed, instead of using proxies of respondents involved in the industry.

Does internationally initiated identity innovation discourage national stakeholders?

During the research it became clear that currently, humanitarian SSI initiatives are mostly internationally driven. A complementary identity system in a country is quite a drastic change and potentially giving up control to foreign powers is something that most countries are very wary off. It is interesting to explore if this fear of losing sovereignty could lead countries to be hesitant to international SSI collaborations. Additionally, it could explore if countries would be more open to humanitarian SSI initiatives when engagement is initiated and led by national HOs.

Are un(der)documented people willing and capable to control their own identity in Kenya?

The focus of this research has mostly left the capabilities of un(der)documented and beneficiaries out of scope. It was briefly mentioned by one of the respondents that the willingness of people to control their own identity is an important circumstance which might be an influential factor when establishing a humanitarian SSI system somewhere. In the end of the day, if the people do not want to or are not capable to control their own identity that completely renders humanitarian SSI useless for every stakeholder. This could be explored in a survey study with beneficiaries of humanitarian organizations.

What is the impact of trust in humanitarian institutions on the support for humanitarian SSI?

During the expert validation the circumstances and conditions assessment framework was discussed. During one of the interviews the respondent mentioned that trust in institutions might have significant impact in the nurturing of support. According to him, this is one of the reasons why Kenya is an interesting country to try these humanitarian SSI systems in, as humanitarian organizations in the country are generally trusted by the people. It would be interesting to explore if and to what extent this is the case.

8.6 Recommendation for 510 NLRC & "121" consortium

Based on the findings of this research, several recommendations can be made for 510 and the stakeholders of the 121 consortium. The main takeaway of this research is that the stakeholder landscape in Kenya is currently not in an optimal state to transition a humanitarian SSI system towards a more foundational purpose, such as the facilitating of in-name SIM- and mobile money registration. In addition to this, during the reflection on this research, it became clear that realizing this innovation in a responsible way does not go without risks and managing trade-offs. This means that stakeholders should continue to do further research on this topic, most notably on the willingness and capability of un(der)documented people in Kenya to control their own identity. Advancing too far with this innovation without determining a favorable willingness and capability could result in the further aggravation of crisis and poverty situations.

Before venturing outside of the boundaries of humanitarian aid in a collaborative form with public- and private stakeholders, it would be advisable for 121 and its stakeholders to focus on nurturing a more favorable and supportive stakeholder landscape. In order to reach this, a sequenced strategy is advised which splits up measures in different phases.

First phase

Engagement for an open discussion with the Kenyan KYC authorities such as the Communications Authoritiy, the FRC, and the CBK should be sought, preferably by partnering with other big HOs and development organizations, to discuss the further defining of KYC requirements (first support nurturing principle). This is a low risk and low barrier course of action. Discussions should focus on defining datasets that can satisfy the current KYC regulations.

In the reflection section and throughout the research it became clear that if this innovation is to be advanced in a responsible manner, further development needs to stay within the boundaries of humanitarian aid for the time being. In order to demonstrate the value of these systems, to spread understanding and experience of SSI technology 121 should continue with scaling functional SSI systems (third support nurturing principle). By negotiating flexible KYC exemptions (first support nurturing principle), 121 can proof its concept by facilitating CTPs. However, it is important that beneficiary risk in this phase should be contained by HOs. That means that in-name registrations should be avoided for the time being, obstructing the role of the private sector services for self-procurement and limiting it to payment facilitation. Throughout the pilots, HOs can further drive the privacy narrative and test digital literacy among beneficiaries. Finally, these pilots should provide insight to government stakeholders into the additional inclusion potential that these SSI systems have in terms of reaching actual Kenyan undocumented citizens, without overinflating the numbers. A second low barrier to entry functional purposed SSI system that 121 stakeholders,

specifically the KRCS, should develop to demonstrate the technology and to create direct SSI exposure to public sector stakeholders is an educational credential SSI system. 121 stakeholders should focus on further identifying lateral services like these to demonstrate SSI within the boundaries of humanitarian aid.

Stimulating privacy in Kenya (second support nurturing principle) should be a main focus for two reasons. Firstly, information privacy awareness and privacy legislation pressure are two intrinsic motivators to increase support for the proposed development. Secondly, a proper SSI implementation needs to be embedded in a broader privacy-focused context to prevent data abuse outside of the systems' end-points. To stimulate privacy in the country, dialogue engagement can initially best be sought with national CSOs. By providing these national organizations with more technical know-how and understanding of privacy, the discussion around privacy in the country can be further provoked. This narrative can be further driven through leveraging of the CSO networks such as CONCISE, KICTANet, and BAKE. 121 stakeholders need to understand that this change in thinking is a long term process that ultimately does not only influence the acceptability and support among crucial stakeholders but is also of importance to ensure responsibleness of innovation in the second phase.

Second phase

In the second phase, stakeholders should start alignment for a transition to a more foundational purpose, for which loosening the onboarding requirements of private sector services should be a point of focus. Advocacy for financial- and social inclusion of the un(der)documented population should be intensified (first support nurturing principle). Several arguments should be leading here. Firstly, the economic argument: Formally including these groups will lead to an increase in economic growth and tax revenue. Secondly, the humanitarian argument: Allowing these people to be included, facilitates these individuals to re-establish their livelihoods, reduces vulnerability, and reduces poverty in a dignified manner. In order to significantly pressure the national government to reduce onboarding restrictions, advocacy should be a joint effort between major HOs under the narrative of the humanitarian-development nexus, international development organizations, initiatives such as the World Bank Group, ID4D, and other organizations focused on sustainable development goals. It also applies here that national CSO networks (CONCISE, KICTANet, and BAKE), and unelected political parties can be leveraged to further accelerate this narrative.

Furthermore, a more foundational purpose will require an increased commitment of the private sector. In this second phase, public-private partnerships should be leveraged to broaden the agenda to further capture the interest of the private sector (fourth support nurturing principle). The most obvious system extension which can be developed, potentially by 121s' private sector participants, is the integration of verifiable transaction records. The development of this functionality should take place before the transition to a more foundational purpose has been put in motion, as there are risks of correlatability and other early development risks. A second more ambitious system extension that could be put on the agenda is that of verifiable KYC compliance sharing. Sharing beneficiary KYC compliance status could be integrated and demonstrated for national FSPs and MNOs, such as Safaricom and banks like CBA and CBK. These system extensions would further

alleviate some of the onboarding obstacles for the private sector and if this is done in an open way where the private sector could learn from and potentially roll out KYC compliance sharing for traditional customers, then that creates extra interest. Especially Safaricom is a very influential party to public decision making, so this stakeholder should be focused on when broadening the agenda.

Optional phase

Only when the actions in the first two stages are ineffective in generating enough support among public sector stakeholders in the country, 121s' stakeholders could choose to use the fifth support nurturing principle. In this case, they would temporarily freeze the engagement with- and required commitment from the Kenyan government and focus their resources on development in another country with a more favorable institutional environment, to further establish the appropriateness of SSI as a technological solution. However, it is advisable that this remains an option of last resort, as the public sector in Kenya remains a crucial and valuable ally in a transition to a more foundational purpose. Subsequently, few African countries are more suitable for this innovation when taking in to account the state of technical systems. Especially considering the potential aggravation of crisis situations when introducing humanitarian technological innovations in an immature technical environment, as discussed in the reflection chapter. In that respect, Kenya is in a unique situation due to its high mobile phone penetration and mobile network coverage. In addition to that, trust in humanitarian institutions and government engagement with blockchain technology in Kenya is relatively high. Resorting to proving the concept abroad should therefore be approached critically.

Appendix A: Reference list

Abraham, A. (2017). *Self-Sovereign Identity*. Styria: E-Government Innovationszentrum.

Achuka, V. (2020). Concern over rise in terror attacks in northern Kenya. *Daily Nation*. Retrieved from https://www.nation.co.ke/news/Concern-over-rise-in-terror-attacks/1056-5418374-format-xhtml-gc0gkx/index.html

Allen, C. (2016). The path to self-sovereign identity. *Life with Alacrity*.

Arasa, R. (2015). Determinants of know your customer (KYC) compliance among commercial banks in kenya. *Journal of Economics and Behavioral Studies*, *7*(2), 162–175.

Baars, D. S. (2016). *Towards self-sovereign identity using blockchain technology*. University of Twente.

Bacon, J., Michels, J. D., Millard, C., & Singh, J. (2017). Blockchain demystified. *Queen Mary School of Law Legal Studies Research Paper*, (268).

Benenson, Z., Girard, A., Krontiris, I., Liagkou, V., Rannenberg, K., & Stamatiou, Y. (2014). User acceptance of privacy-ABCs: an exploratory study. *International Conference on Human Aspects of Information Security, Privacy, and Trust*, 375–386. Springer.

Bloomberg. (2019). Nigeria to Give All of Its 200 Million People Identity Numbers. Retrieved November 30, 2019, from https://www.dailymaverick.co.za/article/2019-09-20-nigeria-to-give-all-of-its-200-million-people-identity-numbers/

Cameron, K. (2008). A user-centric identity metasystem. *Microsoft Corp*.

Caribou Digital. (2019). *Kenya's Identity Ecosystem*. Retrieved from https://www.cariboudigital.net/wp-content/uploads/2019/10/Kenyas-Identity-Ecosystem.pdf

Central Bank of Kenya. (2016). *2016 FinAccess Household Survey*.

Central Bank of Kenya. (2019). *2019 FinAccess Household Survey*.

CLGF. (2017). *The local government system in Kenya*. Retrieved from http://www.clgf.org.uk/default/assets/File/Country_profiles/Kenya.pdf

Communications Authority of Kenya. *THE KENYA INFORMATION AND COMMUNICATIONS ACT*. , (2015).

Correia, J., & Compeau, D. (2017). Information privacy awareness (IPA): a review of the use, definition and measurement of IPA. *Proceedings of the 50th Hawaii International Conference on System Sciences*.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: a comparison of two theoretical models. *Management Science*, *35*(8), 982–1003.

Dunphy, P., & Petitcolas, F. A. P. (2018). A first look at identity management schemes on the blockchain. *IEEE Security & Privacy*, *16*(4), 20–29.

El Maliki, T., & Seigneur, J.-M. (2013). Online Identity and User Management Services. In *Computer and Information Security Handbook* (pp. 459–484). Elsevier.

Gaitho, M. (2019). For the conflict of interest law to work, President must lead way. Retrieved January 24, 2020, from https://www.nation.co.ke/oped/opinion/Uhuru-must-lead-way-for-the-conflict-of-interest-law-to-work/440808-5388410-a31vvt/index.html

Gatuyu, J. (2018). Kenya needs unified identity registration. *Business Daily Africa*. Retrieved from https://www.businessdailyafrica.com/analysis/ideas/Kenya-needs-unified-identity-registration/4259414-4846478-119h6iqz/index.html

Genc, D. (2017). *" The Blockchain" in Humanitarian Aid: A Critique of Humanitarian Innovation*.

Government of the Republic of Kenya. (2007). *Kenya Vision 2030*. Retrieved from http://vision2030.go.ke/inc/uploads/2018/05/Vision-2030-Popular-Version.pdf

Greenwood, F., Howarth, C., Escudero Poole, D., Raymond, N., & Scarnecchia, D. (2017). *The Signal Code: A Human Rights Approach to Information During Crisis*. Retrieved from https://hhi.harvard.edu/sites/default/files/publications/signalcode_final.pdf

Gressin, S. (2017). The equifax data breach: What to do. *Federal Trade Commission*, *8*.

GSMA. (2017). *Refugees and Identity: Considerations for mobile-enabled registration and aid delivery*.

Gu, J.-C., Lee, S.-C., & Suh, Y.-H. (2009). Determinants of behavioral intention to mobile banking. *Expert Systems with Applications*, *36*(9), 11605–11616.

Gwer, F., Odero, J., & Totolo, E. (2019). *Digital credit audit report: Evaluating the conduct and practice of digital lending in Kenya*. Retrieved from https://fsdkenya.org/publication/digital-credit-audit-report-evaluating-the-conduct-and-practice-of-digital-lending-in-kenya/

Harbach, M., Fahl, S., Rieger, M., & Smith, M. (2013). On the acceptance of privacy-preserving authentication technology: the curious case of national identity cards. *International Symposium on Privacy Enhancing Technologies Symposium*, 245–264. Springer.

ICRC, & Brussels Privacy Hub. (2017). *Handbook on Data Protection in Humanitarian Action*. Retrieved from https://shop.icrc.org/handbook-on-data-protection-in-humanitarian-action.html?___store=default

IHRC & NRC. (2017). *Recognising Nairobi's Refugees*. Retrieved from https://hrp.law.harvard.edu/wp-content/uploads/2017/11/recognising-nairobis-refugees_nrc_ihrc_november2017_embargoed.pdf

Iivari, J. (2015). Distinguishing and contrasting two strategies for design science research. *European Journal of Information Systems*, *24*(1), 107–115.

International Telecommunication Union. (2016). *Review of national Identity programs*. Retrieved from https://www.itu.int/en/ITU-T/focusgroups/dfs/Documents/09_2016/Review of National Identity Programs.pdf

Jacobsen, K. L., & Fast, L. (2019). Rethinking access: how humanitarian technology governance blurs control and care. *Disasters*, *43*, S151–S168.

Johannesson, P., & Perjons, E. (2014). *An introduction to design science*. Springer.

Kakah, M. (2019). Huduma Namba 'prone to hacking', says expert. *Daily Nation*. Retrieved from https://www.nation.co.ke/news/Huduma-Namba---Sh6-billion-spent-on-archaic-system--/1056-5286368-xmfkg8z/index.html

Kenya National Government Communication Centre. (2019). *NATIONAL INTEGRATED IDENTITY MANAGEMENT SYSTEM*. Retrieved from http://www.hudumanamba.go.ke/wp-content/uploads/2019/03/NIIMS-BROCHURE-suggested-edits.pdf

KHRC. (2019). *DIGITAL IDENTIFICATION DOCUMENT (ID) & CITIZENSHIP CONSULTATIVE MEETING*. Retrieved from https://www.khrc.or.ke/publications/198-report-of-digital-identification-citizenship-workshop-naivasha/file.html

KNCHR. (2007). *An Identity Crisis? A Study on the Issuance of National Identity Cards In Kenya*. Retrieved from http://www.knchr.org/Portals/0/EcosocReports/KNCHR Final IDs Report.pdf

Lee, J. (2012). *Cash Transfers in Emergencies*.

LeVan, A. C., Hassan, I., Isumonah, V., Kwaja, C., Momale, S., Nwankwor, C., & Okenyodo, K. (2018). *Study on Marginalized Groups in the Context of ID in Nigeria*.

McKinsey. (2019). *Digital identification: A key to inclusive growth*. Retrieved from https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth

Meyling, J. (2019). *A Self-Sovereign Identity for financially inclusive Cash-based Assistance*. Maastricht Graduate School of Governance.

Moore, J. (2018). Cambridge Analytica Had a Role in Kenya Election, Too. *The New York Times*. Retrieved from https://www.nytimes.com/2018/03/20/world/africa/kenya-cambridge-analytica-election.html

Mühle, A., Grüner, A., Gayvoronskaya, T., & Meinel, C. (2018). A survey on essential components of a self-sovereign identity. *Computer Science Review*, *30*, 80–86.

Mukami, L. (2019). Regulator approves Airtel, Telkom merger. *Daily Nation*. Retrieved from https://www.nation.co.ke/business/Airtel-Telkom-merger-approved/996-5384504-yrou3az/index.html

Njanja, A. (2018). Airtel, Telkom eat into Safaricom market share. *Business Daily Africa*. Retrieved from https://www.businessdailyafrica.com/corporate/companies/Airtel--Telkom-eat-into-Safaricom-market-share/4003102-4807336-8h6mpl/index.html

Njoroge-Kibe, L., & Kageni, E. (2019). Kenya: Anti Money Laundering 2019, International Comparative Legal Guides. Retrieved October 15, 2019, from https://iclg.com/practice-areas/anti-money-laundering-laws-and-regulations/kenya

OCHA. (2017). *The new way of working*.

OCHA. (2019). *DATA RESPONSIBILITY GUIDELINES*. Retrieved from https://centre.humdata.org/wp-content/uploads/2019/03/OCHA-DR-Guidelines-working-draft-032019.pdf

Open Society Justice Initiative. (2019). *Kenya's National Integrated Identity Management System*. Retrieved from https://www.justiceinitiative.org/uploads/8f3b665c-93b9-4118-ad68-25ef390170c3/briefing-kenya-nims-20190923.pdf

Othman, A., & Callahan, J. (2018). The Horcrux protocol: a method for decentralized biometric-based self-sovereign identity. *2018 International Joint Conference on Neural Networks (IJCNN)*, 1–7. IEEE.

Privacy International. (2017a). *Fintech: Privacy and Identity in the New Data-Intensive Financial Sector*.

Privacy International. (2017b). *Track, Capture, Kill: Inside Communications Surveillance and Counterterrorism In Kenya*. Retrieved from https://privacyinternational.org/report/43/track-capture-kill-inside-communications-surveillance-and-counterterrorism-kenya

Sandvik, K. B., Jumbert, M. G., Karlsrud, J., & Kaufmann, M. (2014). Humanitarian technology: a critical research agenda. *International Review of the Red Cross*, *96*(893), 219–242.

Stevens, L. (2018). *Self-Sovereign Identities for Scaling Up Cash Transfer Projects: Designing a blockchain based digital identity system*.

Strauß, S. (2011). The Limits of Control -- (Governmental) Identity Management from a Privacy Perspective. In S. Fischer-Hübner, P. Duquenoy, M. Hansen, R. Leenes, & G. Zhang (Eds.), *Privacy and Identity Management for Life* (pp. 206–218). Berlin, Heidelberg: Springer Berlin Heidelberg.

The World Bank. (2018). ID4D Data: Global Identification Challenge by the Numbers. Retrieved from http://id4d.worldbank.org/global-dataset

Tobin, A. (2018). *Sovrin: What Goes on the Ledger?* Retrieved from https://sovrin.org/wp-content/uploads/2018/10/What-Goes-On-The-Ledger.pdf

Tobin, A., & Reed, D. (2016). The inevitable rise of self-sovereign identity. *The Sovrin Foundation*, *29*.

Transparency International. (2020). Corruption Perception Index 2019. Retrieved January 23, 2020, from https://www.transparency.org/cpi2019

UN. (2015). Sustainability development goals. Retrieved November 26, 2019, from https://www.un.org/sustainabledevelopment/sustainable-development-goals/

UNHCR. (2018a). *From proGres to PRIMES*.

UNHCR. (2018b). UNHCR now accepting proposals on digital identity. Retrieved January 12, 2020, from https://www.unhcr.org/blogs/unhcr-accepting-proposals-digital-identity/

UNHCR, & GSMA. (2019). *DISPLACED & DISCONNECTED*.

USAID. (2017). *IDENTITY IN A DIGITAL AGE: INFRASTRUCTURE FOR INCLUSIVE DEVELOPMENT*. Retrieved from https://www.usaid.gov/sites/default/files/documents/15396/IDENTITY_IN_A_DIGITAL_AGE.pdf

van Bokkem, D., Hageman, R., Koning, G., Nguyen, L., & Zarin, N. (2019). Self-sovereign identity solutions: The necessity of blockchain technology. *ArXiv Preprint ArXiv:1904.12816*.

van Wingerde, M. (2017). *Blockchain-enabled self-sovereign identity*. Master's thesis, Tilburg University, School of Economics and Management.

W3C. (2019). Decentralized Identifiers (DIDs) v0.13. Retrieved October 15, 2019, from https://w3c-ccg.github.io/did-spec/

Wang, F., & De Filippi, P. (2020). Self-sovereign identity in a globalized world: Credentials-based identity systems as a driver for economic inclusion. *Frontiers in Blockchain| Www. Frontiersin. Org*, *2*.

Wolfond, G. (2017). A blockchain ecosystem for digital identity: improving service delivery in Canada's public and private sectors. *Technology Innovation Management Review*, *7*(10).

World Bank Group. (2016). *ID4D Country Diagnostic: Kenya*. Retrieved from http://documents.worldbank.org/curated/en/575001469771718036/pdf/Kenya-ID4D-Diagnostic-WebV42018.pdf

World Bank Group. (2017). *THE STATE OF IDENTIFICATION SYSTEMS IN AFRICA*. Retrieved from http://documents.worldbank.org/curated/en/156111493234231522/pdf/114628-WP-68p-TheStateofIdentificationSystemsinAfricaASynthesisofIDDAssessments-PUBLIC.pdf

World Bank Group. (2018). Identification For Development (ID4D) Global Dataset. Retrieved October 2, 2019, from https://development-data-hub-s3-public.s3.amazonaws.com/ddhfiles/94586/wb_id4d_dataset_2018_0.xlsx

World Bank Group, & GSMA. (2016). *Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation*. Retrieved from https://secureidentityalliance.org/publications-docman/public/4-july-2016-report-digital-identity/file

Appendix B: Literature review selection

To explore the existing knowledge regarding Self-Sovereign Identity a literature review has been performed. Most of the developments in SSI have been in recent years. Therefore, only publications from 2016 and on were selected. Additionally, publications focusing on the combination of SSI and blockchain technology were preferred. Articles solely focusing on one specific SSI system design and no overarching conclusions were avoided. Finally, only publications in English were selected.

The following search query was employed on research databases google scholar and Scopus:

' "Self-Sovereign Identity" OR ("Self-Sovereign Identity" AND "Blockchain") '

This search query returned 654 results, of which 7 were selected. Backward snowballing was applied in these articles to find 6 additional relevant articles. Finally, this was supplemented with 2 previous related research efforts conducted at 510. In total this concluded to the following 15 selected publications:

Reference:	Title:
(Abraham, 2017)	Self-Sovereign Identity
(Allen, 2016)	The path to self-sovereign identity
(Baars, 2016)	Towards self-sovereign identity using blockchain technology
(Dunphy & Petitcolas, 2018)	A first look at identity management schemes on the blockchain
(Meyling, 2019)	A Self-Sovereign Identity for financially inclusive Cash-based Assistance
(Mühle, Grüner, Gayvoronskaya, & Meinel, 2018)	A survey on essential components of a self-sovereign identity
(Othman & Callahan, 2018)	The Horcrux protocol: a method for decentralized biometric-based self-sovereign identity
(Schanzenbach, Bramm, & Schütte, 2018)	reclaimID: Secure, Self-Sovereign Identities using Name Systems and Attribute-Based Encryption
(Stevens, 2018)	Self-Sovereign Identities for Scaling Up Cash Transfer Projects: Designing a blockchain based digital identity system
(Stokkink & Pouwelse, 2018)	Deployment of a blockchain-based self-sovereign identity
(Tobin & Reed, 2016)	The inevitable rise of self-sovereign identity

(van Bokkem, Hageman, Koning, Nguyen, & Zarin, 2019)	Self-sovereign identity solutions: The necessity of blockchain technology
(van Wingerde, 2017)	Blockchain-enabled self-sovereign identity
(Wang & De Filippi, 2020)	Self-sovereign identity in a globalized world: Credentials-based identity systems as a driver for economic inclusion
(Wolfond, 2017)	A blockchain ecosystem for digital identity: improving service delivery in Canada's public and private sectors

Table B.1: Selected SSI literature

Appendix C: Semi-Structured Interviews

C.1: Internal Interview Protocol

The interviews were conducted with three objectives in mind. Firstly, to validate and supplement the social environment of stakeholders that were identified in the system analysis. Secondly, to identify collaboration enabling factors that could potentially be implemented as artefact requirements. Thirdly, to explore potential design directions from the perspective of humanitarian organizations.

Initially, respondents were selected internally within the NLRC organization. Three individuals were selected with an affiliation to SSI and the current 121 pilots in Kenya.

Name:	Organization:	Function:	Date:
Maarten van der Veen	510 NLRC	Founder & Strategic lead	10-03-2020
Lars Stevens	510 NLRC	Technical Project Manager	10-03-2020
Ted Bolton	510 NLRC	Kenya Country Lead	10-03-2020

Table C.1: List of internally conducted interviews

The semi-structured interview consists of two parts. Each part was provided a short introduction text which can be found below. The questions of the interview and the structure can be found in Appendix C.2. Finally, the summaries of the internal-interviews can be found in Appendix C.3. The full interview transcripts can be seen upon request.

Introduction internal interviews part 1:

"The research I am conducting is aimed at exploring the possibilities for humanitarian organizations to scale a functional Self-Sovereign Identity system to a more foundational purpose. More specifically, my research is aimed at how such a development process could be brought about in Kenya.

From a humanitarian perspective, rebalancing the control over data through the use of SSI technology has the potential to be more inclusive and can potentially solve the Identity gap challenge. A complete foundational purpose of such a system would mean it could provide access to a wide variety of services, among which humanitarian services, private services, and government services. Allowing users to participate in everyday life.

I have conducted a system analysis in which I discovered several aspects of social complexity that could potentially inhibit such a development. Through this interview I would like to explore your thoughts on this matter, to validate or supplement my ideas. "

The second part of the interview is more directed in nature. Respondents will be presented a visual representation of the stakeholder dynamics as established in the system analysis. The questions will be directed using this diagram.

Introduction internal interviews part 2:

"In the second part of this interview, I will present you a figure, in which my understanding of the current situation of stakeholder power and interest relations is displayed. This, in regard to the realization of a foundational (humanitarian) SSI system. I am interested in how and if important stakeholders can be moved to the upper right quadrant of the diagram. As this has implications for a potential collaborative composition of stakeholders to drive scaling to a foundational purpose. At this time, to my understanding, humanitarian organizations and other international development organizations, are the only two stakeholders with a sense of urgency, interest, and resources to work towards realizing SSI for a foundational purpose."

C.2: Questions Internal interviews

#	Question	Aim	Answer format	Time limit
Part 1: Open-ended, Introduce research focus				2 min
1	Could you briefly introduce your role regarding the current 121 pilots in Kenya?	Establish involvement	Open-ended, no direction	1 min
2	How did you experience collaborating with public and private stakeholders in Kenya during the current pilot?	Identify/validate starting point	Open-ended, no direction	3 min
3	To your understanding, what is the value proposition for private service providers and government organizations to support registration through an (humanitarian) SSI system?	Identify/validate incentives	Open-ended, no direction	4 min
4	To your understanding, what possible barriers do you foresee in collaboration for a foundational purpose?	Identify/validate barriers	Open-ended, no direction	4 min
5	Under the current circumstances in Kenya, do you think this value proposition provides enough incentive for private and public stakeholders over other identity management systems.	Identifiy requirements	Open-ended, no direction	4 min
Part 2: Directed questions, based on Introduced Power-Interest relations diagram				2 min
6.1	Would you agree with this representation of stakeholders that could potentially be involved in the scaling towards a foundational purpose?	Validate multi-actor field	Closed question	3 min
6.2	Which stakeholders do you experience to be most important for reaching a foundational purpose?	Enrich multi-actor field	Open, directed	
7.1	For all of the identified stakeholders, would you say they have sufficient understanding of SSI as a solution?	Identifiy process requirements	Closed question	3 min
7.2	Could HOs influence this lack of understanding and would that bring about changes in the P/I diagram?	Explore design directions	Open, directed	
8.1	Do you think that private organizations in Kenya experience data governance responsibilities as a liability?	Identifiy process requirements	Closed question	3 min
8.2	Could HOs influence this and would that bring about changes in the P/I diagram?	Explore design directions	Open, directed	
9.1	Do you think national Civil Society Organizations can contribute to realizing such a system?	Identifiy process requirements	Closed question	3 min
9.2	Could HOs influence the involvement and the impact of national Civil Society Organizations and would that bring about changes in the P/I diagram?	Explore design directions	Open, directed	
10	Could the integration of other internationally controlled registration services be a first step towards a foundational purpose?	Explore design directions	Open, directed	3 min

Table C.2: Questions internal interviews

C.3: Internal Interviews summaries

Interview summary 1: Maarten van der Veen, Strategic lead, 510 NLRC

#	Question	Answer:
	Part 1: Open-ended, Introduce research focus	
1	Could you briefly introduce your role regarding the current 121 pilots in Kenya?	Founder and strategic lead of 510. Person who started the idea behind 121. Led proposal development, incl the GSMA proposal for Kenya.
2	How did you experience collaborating with public and private stakeholders in Kenya during the current pilot?	No direct involvement with public / private stakeholders.
3	To your understanding, what is the value proposition for private service providers and government organizations to support registration through an (humanitarian) SSI system?	**Private service providers**: 1 : Commercial incentive in onboarding more customers. 2: CSP branding advantages. 3:improved access in low access regions as HOs have better ground access. **Government**: 1 : Capacity support, reduce workload of government by using HO capacity, especially in refugee camps 2: benefit of learning how SSI can protect people.
4	To your understanding, what possible barriers do you foresee in collaboration for a foundational purpose?	1: Loss of control for the government. Decreased access to data when compared to centralized systems. 2: There is a technical barrier as SSI does not properly work in offline scenarios at the moment.
5	Under the current circumstances in Kenya, do you think this value proposition provides enough incentive for private and public stakeholders over other identity management systems.	1: Depends on how idealistic they are in terms of privacy protection. As there are not a lot of alternatives that could equally protect the privacy of the people. 2: It also depends on the strength of civil society to demand more control.
	Part 2: Directed questions, based on Introduced Power-Interest relations diagram	
6.1	Would you agree with this representation of stakeholders that could potentially be involved in the scaling towards a foundational purpose?	The classification of international development organizations / humanitarian organizations is a bit artificial. Most of the NGOs do work in borh areas. HOs / international development organizations are high in power when it comes to influencing international standards and best practices. Not so much when it comes to having governments change their interest.
6.2	Which stakeholders do you experience to be most important for reaching a foundational purpose?	National authorities. As these have to be onboard for a foundational purpose. If acceptance is there, then private organizations, especially FSP are essential to drive development. Alternatively, if acceptance is not there, national CSOs, maybe supported by international organizations are essential to drive a change in thinking.
7.1	For all of the identified stakeholders, would you say they have sufficient understanding of SSI as a solution?	Even though in Kenya a lot of blockchain pilots are conducted, in general there is little understanding of the possibilities and limitations of SSI.
7.2	Could HOs influence this lack of understanding and would that bring about changes in the P/I diagram?	Yes. MNOs and FSPs will be the first ones to increase their interest. They would be easiest to move on the axis of interest. In other countries FSPs are the main organizations testing identity systems. Building the capacities through knowledge of existing CSOs might not be the way to go as they already have an existing specific focus. Maybe establishing a new one which is really aiming to improve the privacy of peopl in Kenya would be more powerfull.
8.1	Do you think that private organizations in Kenya experience data governance responsibilities as a liability?	In the upcoming GDPR inspired data protection bill they took out some critical parts. Especially those parts that would require the government to change their way of handling data. Some additional risk has been shifted to the private sector, but not so much for the public sector. Another international use-cases would be the involvement of some big global tech companies. But it could hurt their business model.
8.2	Could HOs influence this and would that bring about changes in the P/I diagram?	Commercial interest or money in general would be a big component of moving organizational interest.
9.1	Do you think national Civil Society Organizations can contribute to realizing such a system?	CSOs can create acceptance and pressure the government. Through lobbying and advocacy.
9.2	Could HOs influence the involvement and the impact of national Civil Society Organizations and would that bring about changes in the P/I diagram?	International organizations can support CSOs in their advocacy.
10	Could the integration of other internationally controlled registration services be a first step towards a foundational purpose?	Especially around migrants and cross-border travel are compelling use-cases for SSI. It could be challenging, and there would not be one single government that will block the use of such an identity system. It wouldn't be included in the national identity scheme. Additionally, if big global tech companies would onboard the idea it could really help. These tech companies could be another influencer, but SSI could hurt also hurt their business model.
	Other usefull insights:	1: The grey area we are exploring: can identity, especially when it is co-created by trusted organizations, be sufficient to give people temporarily or partial service that they are currently lacking. 2: there is a chicken-and-egg problem: if every person in the country would really see the benefit of an identity that they can own. Then businesses and government will be quick to adopt. The problem is getting people to adopt it, when there are not much services that support it. 3: a proper SSI implementation and regulation would make it more difficult for one party to hold the majority of the data. and this could be a disincentive for parties that are currently thriving on the lack of privacy.

Interview summary 2: Ted Bolton, Kenya country lead, 510 NLRC

#	Question	Answer:
	Part 1: Open-ended, Introduce research focus	
1	Could you briefly introduce your role regarding the current 121 pilots in Kenya?	Original Kenya project initiator. Previous project manager. Currently works on the contextualizing side of the 121 project. And on the pilot environment with KRCS and other stakeholders in Kenya.
2	How did you experience collaborating with public and private stakeholders in Kenya during the current pilot?	Mainly working with the private sector, most of the time with Safaricom. As we want to use M-PESA for our pilots. Potential uses are discussed with them. They are up to the engagement. Government is much more resistant. The engagement with the government ranges from having workshops in which an interest is expressed for the identity scheme up to trying to arrange private meetings and receiving flat "no's" in terms of what we want to do.
3	To your understanding, what is the value proposition for private service providers and government organizations to support registration through an (humanitarian) SSI system?	For organizations like Safaricom: 1. Commercial interest due to onboarding of new market segment. 2.Efficiency gain in registration efforts. 3. leveraging HO capacity in hard to reach areas. 4. CSR gains due to collaboration with humanitarian sector. In contrast, Governments: 1. argument of the humanitarian side is that there are people that don't have identity and you could use these digital identity solutions as an easier way to provide them with services
4	To your understanding, what possible barriers do you foresee in collaboration for a foundational purpose?	1. Government interest in terms of being a state actor is to have as much control over citizenship as possible. I cannot think of why any government would voluntarily pass over the ability of inferring some kind of statehood with fundamental services to a non-governmental actor. 2. Preexisting government efforts. Such as the IPRS, Huduma Namba, but also the single registry.
5	Under the current circumstances in Kenya, do you think this value proposition provides enough incentive for private and public stakeholders over other identity management systems.	For an organization like Safaricom issuing cellphones, SIM cards to people that they are currently not allowed to provide services to because of KYC requirements is enough commercial interest. There is a fundamental thing with government that the people that currently do not have access to an identity, is actually for a reason. Until there is a proven system that provides services to un(der)documented that are clearly Kenyan. The government will probably not be inclined to accept it.
	Part 2: Directed questions, based on Introduced Power-Interest relations diagram	
6.1	Would you agree with this representation of stakeholders that could potentially be involved in the scaling towards a foundational purpose?	Identity beneficiaries / users do not understand the benefits of SSI systems yet. Idealogically it would be in their interest, but practically they don't realize this. Additionally, local authorities probably have a bit more blocking power.
6.2	Which stakeholders do you experience to be most important for reaching a foundational purpose?	National Government for sure.
7.1	For all of the identified stakeholders, would you say they have sufficient understanding of SSI as a solution?	Definitely not. Maybe some individuals do, but on an organizations level the issue is not on the agenda. As a result it is struggling getting grounded within organizations.
7.2	Could HOs influence this lack of understanding and would that bring about changes in the P/I diagram?	Yes, the agenda in terms of technical facilitation is very important. 1. You would need to really advocate with government for them to change their agenda. 2. Technical expertise within organizations and the ability to act on it could be build through tehnical advisory support, but this wouldnt be enough. Technical understanding should be combined with a body of proof. They have to be conviced the concept works.
8.1	Do you think that private organizations in Kenya experience data governance responsibilities as a liability?	The data protection bill only just came in. From what I have seen there hasn't really been any offloading the responsibility of governing personal data. The agenda still seems to be to gather information, hoard and don't share information. Because data is valuable for sure.
8.2	Could HOs influence this and would that bring about changes in the P/I diagram?	I think there is a lot HOs could do. If there were one scandal with the government. Especially with the single registry or huduma namba and then a very well placed and informed civil law case from a CSO. That would bring proper pressure. There are currently some scandals on data, but there are not really severe cases (such as with adhaar).
9.1	Do you think national Civil Society Organizations can contribute to realizing such a system?	CSOs can pressure through lawsuits
9.2	Could HOs influence the involvement and the impact of national Civil Society Organizations and would that bring about changes in the P/I diagram?	Technical advisory support, advocacy
10	Could the integration of other internationally controlled registration services be a first step towards a foundational purpose?	The UNHCR refugee identity could be very slow moving and bureaucratic process. And people registered in a refugee identity can not access national services anyway. Having the technology in another country work would help. Having global tech companies work with it would also help. As it would add credibility to the system. People in Kenya would probably subscribe for a "whatsapp identity" instead of a "121 identity".
	Other usefull insights:	1: The only organization that is really critically involved between the operational and foundational identity is the government. 2. At a certain point if they are not able to enact such a system and that means that individuals do not get access to services. I think that is a where the hand is forced, where essentially, they have to appreciate that another service is doing it and they have to recognize for example a humanitarian service that allows people to access humanitarian relief or aid. 3. A body of evidence is required that proofs the technology.
	Kenya situation specifics	1. high barrier to get an identity. Due to burden of proof and cost. Terrorism and immigration could be a part of it. 2. Kenyan government is trying to retain or increase control over identity provision. 3.The mobile money business will probably struggle to deal with enhanced privacy regulations. At least it's contractors. 4. From a formal side there is some entanglement of interest. For example the government stake in Safaricom. 5. People dont trust the new government initiative huduma namba. Lots of rumors about corruption or issues with the facilitation. Lots of wasted money. 6. In general TB agrees with CSOs lacking connections and resources to be involved in the design of the country's identity system.

Interview summary 3: Lars Stevens, Technical project manager 121, 510 NLRC

#	Question	Answer:
	Part 1: Open-ended, Introduce research focus	
1	Could you briefly introduce your role regarding the current 121 pilots in Kenya?	Product owner of 121 and technical project manager
2	How did you experience collaborating with public and private stakeholders in Kenya during the current pilot?	n/a
3	To your understanding, what is the value proposition for private service providers and government organizations to support registration through an (humanitarian) SSI system?	1. If they want to onboard un(der)documented people and trust the process of the SSI system then it would improve efficiency in their registration process. (commercial incentive and efficiency incentive). 2. Government might be interested in the increase of GDP and collectable taxes it could cause. 3. Capacity support in registration. The government might not be able to identify these people, while HOs are.
4	To your understanding, what possible barriers do you foresee in collaboration for a foundational purpose?	1. If the government is willingly excluding people a national government ID and the services that come with that, then it would not have any value for them. 2. Loss of control goes against the core mandate of the government. 3. government has lack of sense of urgency. Making capacity, funding difficult for the government to co-develop such a system. 4. still a technical barrier: integrating APIs with this system. 5. if your entire business model depends on the analysis of personal data and third-party tracking of information that makes it more difficult to accept. 6. KYC compliancy is required to make the identity usefull.
5	Under the current circumstances in Kenya, do you think this value proposition provides enough incentive for private and public stakeholders over other identity management systems.	No
	Part 2: Directed questions, based on Introduced Power-Interest relations diagram	
6.1	Would you agree with this representation of stakeholders that could potentially be involved in the scaling towards a foundational purpose?	Users only have an indirect interest, no direct interest. Development partners have high interest, as their business is aimed at creating a network effect.
6.2	Which stakeholders do you experience to be most important for reaching a foundational purpose?	National authorities, due to law and constitution, regulatory support but also, they have the mandate for identity within the country.
7.1	For all of the identified stakeholders, would you say they have sufficient understanding of SSI as a solution?	n/a
7.2	Could HOs influence this lack of understanding and would that bring about changes in the P/I diagram?	They could, it is essentially what HOs do. They lobby and they are a complementary unit to the government.
8.1	Do you think that private organizations in Kenya experience data governance responsibilities as a liability?	n/a
8.2	Could HOs influence this and would that bring about changes in the P/I diagram?	HOs can lobby for this.
9.1	Do you think national Civil Society Organizations can contribute to realizing such a system?	Both national CSOs and HOs can pressure the government
9.2	Could HOs influence the involvement and the impact of national Civil Society Organizations and would that bring about changes in the P/I diagram?	LS agreed that providing CSOs with more technical understanding and knowledge can enable them to take a more active role in development.
10	Could the integration of other internationally controlled registration services be a first step towards a foundational purpose?	In essence you have to create a network effect. If national government is hard to get on board. You have to demonstrate it to them, which could be through international services.
	Other usefull insights:	1. Convincing government requires a body of proof which demonstrates the value of such a system. Preferably using interoperable standards and sharing such a system with the government, including them in the learning process.

C.4 External Interview Protocol

Interviews with participants from external organizations were conducted. Due to a slight change in the research scope, the interview protocol was changed to reflect the scope more appropriately. These interviews were conducted to further identify incentives and barriers. Secondly, to identity which local circumstances and conditions are favorable to get public and private stakeholders to support registration through a humanitarian SSI system for functional SIM cards and mobile money accounts. And thirdly to identify possible approaches for HOs to nurture such circumstances.

Respondents from external organizations were selected for these interviews. Participants with an affiliation to SSI to create financial/social inclusion were approached. This resulted in a mixture of participants from private and humanitarian organizations.

Name:	Organization:	Function:	Date:
David Lamers	Rabobank	Innovation consultant	07-04-2020
Johannes Ebert	Gravity.earth	Co-founder	16-04-2020
Joseph Oliveros	IFRC	Senior Officer CTP innovations	24-04-2020

Table C.3: List of externally conducted interviews

The semi-structured interview consists of two parts. Each part was provided a short introduction text which can be found below. The questions of the interview and the structure can be found in Appendix C.5. Finally, the summaries of the external-interviews can be found in Appendix C.6. The full interview transcripts can be seen upon request.

Introduction external interviews part 1:

To start, I will briefly introduce myself and my research. I am a student at Delft Technical University. As part of my masters in complex systems engineering, I am doing research in collaboration with 510. 510 wants to explore if and how digital identities, when co-created by trusted HOs in an SSI system, could facilitate un(der)documented people to gain access to private sector services. In specific they are interested in enabling un(der)documented people to get in-name SIM cards and mobile money accounts, as this would both improve the efficiency of humanitarian relief and quality of life for people of concern.

Introduction external interviews part 2:

I am trying to explore how support among public and private stakeholders can be created for initiatives like these. I believe that the value proposition of a humanitarian SSI system depends a lot on local circumstances and conditions. The aim of my research is to provide insight in these local conditions and circumstances. And identifying approaches for the humanitarian sector to nurture these conditions.

C.5 Questions external interviews

#	Question	Aim	Answer format	Time limit
Part 1 Value proposition focussed				2 min
1	Could you briefly introduce yourself, what you do and your affiliation with SSI as a subject.	Establish involvement	Open-ended, no direction	1 min
2	From the perspective of FSPs and MNOs, what do you see as the most important incentives for supporting a (humanitarian) SSI as registration method for private sector services and what are barriers to support it?	Identify incentives / disincentives	Open-ended, no direction	5 min
3	From the perspective of national authorities, what do you see as the most important incentives for supporting a (humanitarian) SSI as a registration method for private services and what are barriers to support it?	Identify incentives / disincentives	Open-ended, no direction	5 min
Part 2 Circumstances & Conditions focussed				2 min
4	Are there according to you specific local circumstances or conditions that block support for humanitarian SSI?	Identify blocking local conditions/ circumstances	Open-ended, no direction	5 min
5	What would be ideal local circumstances to create support among stakeholders for a humanitarian SSI?	Identify required local conditions / circumstances	Open-ended, no direction	5 min
6	What can HOs do to create conditions favorable for humanitarian SSI support in countries like this?	Explore design directions	Open-ended, no direction	3 min

Table C.4: Questions external interviews

C.6 External interviews summaries

Interview summary 4: David Lamers, Blockchain/SSI specialist, Rabobank

#	Question	Answer
Part 1 Value proposition focussed		
1	Could you briefly introduce yourself, what you do and your affiliation with SSI as a subject.	Blockchain/ SSI specialist at Rabobank.
2	From the perspective of FSPs and MNOs, what do you see as the most important incentives for supporting a (humanitarian) SSI as registration method for private sector services and what are barriers to support it?	Incentives: 1. Efficiency gain in own services. 2. Remote validation. 3. Compliancy advantages. 4. Privacy demand. 5. New business models. 6. Societal contribution / CSR Disincentives: 1. Lack of available data. 2. Lack of technical capacity at third parties to share data. 3. Interoperability issues.
3	From the perspective of national authorities, what do you see as the most important incentives for supporting a (humanitarian) SSI as a registration method for private services and what are barriers to support it?	Incentives: 1. Internal government innovation programs and legistlation: Programma Regie op Gegevens and wet digitale overheid both increase the interest of government in SSI. Barriers: 1. Lack of institutional framework to form requirements.
Part 2 Circumstances & Conditions focussed		
4	Are there according to you specific local circumstances or conditions that block support for humanitarian SSI?	1. Strictness of AML and KYC regulations. 2. Low trust in HOs 3.
5	What would be ideal local circumstances to create support among stakeholders for a humanitarian SSI?	1. Government openness to innovation. 2. Privacy pressure towards government
6	What can HOs do to create conditions favorable for humanitarian SSI support in countries like this?	Advocacy.
	Other usefull insights:	1. There is a chicken-egg problem where not enough data issuers are available and not enough users. 2. Limited service provision greatly reduces KYC risk. 3. Too much privacy pressure, might also disencourage data issuers to issue credentials. 4. ZKP could be leveraged to satifsy KYC regulations, such as blacklists, in a more private way.

Interview summary 5: Johannes Ebert, Co-founder and CEO, Gravity.earth

#	Question	Answer
	Part 1 Value proposition focussed	
1	Could you briefly introduce yourself, what you do and your affiliation with SSI as a subject.	Co-founder and CEO of Gravity.earth. A decentralized identity company based in Nairobi. Gravity.earth is focused on creating 'financial identities' for small business owners using a combination of decentralized cloud and SSI systems.
2	From the perspective of FSPs and MNOs, what do you see as the most important incentives for supporting a (humanitarian) SSI as registration method for private sector services and what are barriers to support it?	Incentives: 1. Opening up a new customer segment. (They can tap in to a new market, they would reduce their compliance risk. They know full well that refugees have SIM cards that are bought by someone else. And if there was a crackdown, they could be in trouble. Both on the business side and on the compliance side there would be additional value.) 2. verifiability and authenticating refugee status.3. Less compliancy risk 4. new business models (sharing KYC compliance) Disincentive: 1. KYC regulations.
3	From the perspective of national authorities, what do you see as the most important incentives for supporting a (humanitarian) SSI as a registration method for private services and what are barriers to support it?	Disincentive: A political issue, the government does not want the refugees to be fully included and be able to access all the private services. Lack of political will is a big big barrier.
Part 2 Circumstances & Conditions focussed		
4	Are there according to you specific local circumstances or conditions that block support for humanitarian SSI?	1. Functioning existing systems already in place for the use case. I am not so familiar with the case in Uganda, but I know that they very quickly register people and enroll them in the government administered identity system and everyone has some sort of an ID card and can use it to open a bank account and SIM card. So, if there is already something in place that works, that blocks SSI.
5	What would be ideal local circumstances to create support among stakeholders for a humanitarian SSI?	1. You would really have to find that country, where maybe the government regulation is less of an issue. In Cameroon for example UNHCR mandates are already accepted for opening bank accounts. 2. People centric identity is really interesting everywhere where you have 2 things: information asymmetries or a lack of central registries: either due to privacy or practical reasons they were/will never be established. 3. Government identity API's in place can make people used to validating ID. 4. Approachable, flexible and innovating government institutions like the communications authority. 5. data protection laws and huge fines making data governance a liability: Maybe in a while, after there has been a case where huge fines were issued by the government to someone that has not respected a principle from the new data protection law and then it might change..
6	What can HOs do to create conditions favorable for humanitarian SSI support in countries like this?	Advocacy is a big one. Advocacy separate from implementation is not super efficient. Involving Civil society, but also more mainstream CSO organizations. In advocacy it is always good to advocate to someone, which goes home and then advocates to someone else: Leverage networks to spread advocacy.
	Other usefull insights:	1. The people on the other side they are interested in the data. If you tell them you verified someone's ID, they usually trust you. Verifiability is not the most important thing. 2. Getting issuers to sign credentials is hard. 3. Existing API's are not built to support SSI. 4. In WFP discussions with the communication authority the tech operators were like: Yes we can use refugee mandates for registration, but we have no way to verify them.

Interview summary 6: Joseph Oliveros, Senior Officer CTP innovation, IFRC

#	Question	Answer
	Part 1 Value proposition focussed	
1	Could you briefly introduce yourself, what you do and your affiliation with SSI as a subject.	cash transfer programming innovations senior officer within the IFRC. My role is to identify how innovation and technology could be used by national societies to scale up their cash. Works on the DIGID project.
2	From the perspective of FSPs and MNOs, what do you see as the most important incentives for supporting a (humanitarian) SSI as registration method for private sector services and what are barriers to support it?	Incentive: 1. I think the major motivation is certainly to earn profit from providing such services. New customer segment is one incentive. 2. For repeat use: There are areas where they are constantly experiencing the same hazards and risks and therefore, they are so vulnerable to flooding, and so you will know that that assistance will be there for those certain communities for a period of time. 3.The volume for cash transfer programming is quite huge: we are starting to see that the FSP sector are starting to really differentiate themselves, not just on the service. And they are targeting HOs because of the volume that is being carried out through with them is huge. Barriers: 1. The acceptability of digital ID as an appropriate KYC requirement
3	From the perspective of national authorities, what do you see as the most important incentives for supporting a (humanitarian) SSI as a registration method for private services and what are barriers to support it?	Incentive: 1. Part of it is the understanding that the national ID system is not highly proliferated yet. And it would either take time, because even with paper-based / analog stuff, there is still a huge amount of the population that don't have it. Then there are people that don't want it, from a security or protection standpoint. So, in the absence of not being able to provide such things, in the event of life saving and short time period type of things. I think the government might be motivated. It comes down to capacity as well. Barriers: 1. This mandate that they will need to provide legal identification to begin with.
Part 2 Circumstances & Conditions focussed		
4	Are there according to you specific local circumstances or conditions that block support for humanitarian SSI?	1. Institutions are subject to regulatory requirements. One of them is KYC. Unfortunately, it also depends on how strict the KYC requirements are. In particular Kenya, they require that you need to have an official ID in order to be considered for SIM registration and the opening of an M-PESA mobile money accounts. 2. The implementation is not as easy because of the current technology that require that you have either access to a smart phone or some kind of infrastructure that allows you to keep all of those credentials in the hands of the beneficiaries, for which smartphones are the most effective way of doing that now. But if you don't have that infrastructure and the digital literacy level; the understanding among beneficiaries to begin with to maintain their information and the other thing is the willingness to maintain their information.
5	What would be ideal local circumstances to create support among stakeholders for a humanitarian SSI?	1. If organizations are really serious about privacy, this is about as privacy protecting and as respectful of the privacy as it is. I can see that (privacy legislation pressure) being one of the levers for taking it more seriously.
6	What can HOs do to create conditions favorable for humanitarian SSI support in countries like this?	1. have this conversation with the government to begin with. To clarify what to do and to clarify that our intent is not to duplicate their efforts to roll out 2. Advocating for access to sim cards and mobile money and providing an alternative way to meet the current requirements of KYC and SIM card regulations. 3. You can do SSIs, but it does not necessarily have to be linked to regulatory compliance in many cases. We have organizations such as the Australian Red Cross that tries to do SSI for volunteers for instance. In terms of keeping their training credentials. these are some of the more practical ways to be used and accepted without having to really go for huge lobbying in terms of acceptance. 4. I think that we as HOs need to show we are the model for the ones that follow data responsibility and data ethics. Because the onus is on us to really show that we have these principles. We are not here to make money off of the data of these beneficiaries. We are not here to sell this information to FB or google to make more money of their information. I think yes from an advocacy standpoint, it should be spearheaded by HOs. 5. What would help for them to accept such technologies is for it to be used in practical terms, particularly by HOs that are dealing with disasters and things where they can see how this thing can really empower but also solve some of these privacy issues, compliance and otherwise. Then the acceptability of that would be stronger.
	Other usefull insights:	1. If we start providing digital IDs and then these transactions that they have been doing with FSP are recorded in a way that they could take to an FSPs and be able to see that actually these communities and these individuals are being responsible with their use of cash or money in general. 2. We see that there is actually value in the data that shows the behavior and the transactions that the beneficiaries have been doing. If that is a way for them to access additional services, then I think there is a much higher value for creating these digital ID credentials. 3.One of the key things we needed to be careful of is to be seen as HO duplicating the work of what the government should be doing. This is not the case, so we needed to be really clear in our communication on that. 4. What we are seeing is that if you have a mandate, then that makes it a lot easier to implement something. So UNHCR for instance, because of their mandate of refugees, they can provide digital ids for refugees. And that is accepted, because the process of registering refugees is being done with the government officials usually. 5.on UNHCR: They have a project that is ongoing now to do that. In a way they already categorize it as digital ID, because their current system uses biometrics. It is not SSI currently. But they are looking at SSI, they have an ongoing project for that. 6.. The second reason why Kenya is interesting is the government having tried to implement a digital ID solution, of which you should think that this should be solving all of the KYC requirements. Why don't we just increase the efforts of the government to be able to give identities to everyone. But again there are barriers to getting a national id to begin with. And you have to respect the individuals that don't want to have the national id, because of protection, privacy concerns, security.

Appendix D: Expert Validation

D.1 Expert interview protocol

Interviews with experts have been conducted in order to validate the findings of the research. One of the respondents chose to remain anonymous due to a lack of clearance from the corresponding communications department. In order to assure that the experts have proficient authority to validate the design artefact, two respondents were selected from world-leading organizations with a proven affinity to digital identity initiatives in both a humanitarian and a development context. In order to facilitate a profound validation session, the respondents were provided with a document a week in advance. This document outlined a summary of the research including an introduction, a description of the research intent, the circumstances and conditions assessment framework, and elaborated support nurturing principles. Furthermore, they were provided with the purpose of the interview and guidelines for the assessment of the support nurturing principles. The list of conducted expert interviews is presented in table D.1.

Name:	Organization:	Function:	Date:
Anonymous	A top 5 HO	CBT Research manager	20/05/2020
Aiden Slavin	ID2020	Chief of staff	20/05/2020

Table D.1 List of conducted expert interviews

The interview consists of two parts. Each part was provided a short introduction text which can be found below. The questions of the interview and the structure can be found in Appendix D.2. Finally, the summaries of the expert-interviews can be found in Appendix D.3. The full interview transcript can be seen upon request.

Introduction expert interviews part 1

So, to start off I'd like to go over a short introduction and the purpose of this interview: As stated in the brief research summary I send you, There are several HOs that are currently exploring if digital identities, when co-created by trusted HOs in a self-sovereign identity system, could facilitate un(der)documented people to gain access to private sector services. As this purpose somewhat transcends the boundaries of humanitarian aid it requires the involvement of national public- and private sector stakeholders. My research specifically is aimed at exploring how HOs can nurture support for humanitarian SSI systems as a way to facilitate in-name SIM- and mobile money registration for un(der)documented people in Kenya. Using semi-structured interviews with humanitarian SSI initiatives I identified several circumstances and conditions which either block or could enable support for the proposed system. I designed several support nurturing principles for the humanitarian sector to nurture more favorable circumstances and conditions. That finally brings me to the purpose of this interview: I would like to validate my ideas by running it by you.

Introduction expert interviews part 2

In this part of the interview, I would like to assess the designed support nurturing principles with you. To do this in a structured way I think it is best to first run through the 3 questions that I am

interested in and then one by one go through these questions with you for each support nurturing principle.

D.2 Interview Questions

#	Question	Aim	Answer format	Time limit
Part 1: Introduction and assesment framework				2 min
1	Could you very briefly introduce yourself and your affiliation with digital identity or SSI in a humanitarian context?	Establish involvement	Open question	1 min
2	What are your thoughts on the circumstances and conditions assessment framework presented in figure 1 (the assessment framework)?		Open question	5 min
Part 2: Validating design				2 min
3	Before we dive in to the assessment of each individual process principle, do you have any general thoughts on the 5 designed process principles?	Validate design	Open question	5 min
4	Is the principle useful to increase support for a humanitarian SSI system?	Validate design	Open question	5 min
5	Do you foresee any risks or disadvantages?	Validate design	Open question	5 min
6	Is it appropriate for use by the humanitarian sector?	Validate design	Open question	5 min

Table D.2: Questions expert interviews

D.3 Expert-Interview Summaries

Expert validation interview 1: Anonymous HO, CBT research manager

#	Question	Answer
	Part 1: Introduction and assesment framework	
1	Could you very briefly introduce yourself and your affiliation with digital identity or SSI in a humanitarian context?	Last year I was Project manager on the blockchain innovation program of HO X. I have been working on identity for development and humanitarian assistance worldwide. I am working on the subject on a regular basis.
2	What are your thoughts on the circumstances and conditions assessment framework presented in figure 1 (the assessment framework)?	I do not believe that the aim should be to loosen KYC restrictions. I think what we need to do is create systems that satisfy strict KYC environments. If we loosen KYC restrictions then we are being counterproductive. In the grand scheme of things, if you have a looser KYC environment then it is easier to provide forms of identity and register people. However at the same time you create oppertunities for counter productive ways of acting and you are encouraging a less rigurous system. - There is a difference between the financial exclusion of refugees and asylumseekers and other un(der)documented. Refugees and asylumseekers are financially excluded due to temporality. When a refugee enters a host nation, the host nation has a statement to make. From their perspective if they allow these individuals to open bankaccounts and become financially included, they reduce the temporality of the refugee situation. UNHCR certificates could viably be used to access financial services, unfortunately it is a political decision that drives the fact that they are not allowed.
	Part 2: Validating design	
3	Before we dive in to the assessment of each individual process principle, do you have any general thoughts on the 5 designed process principles?	/
4	Usefulness principle A	We already advocate for social and financial inclusion of the un(der)documented so yes that is applicable. I feel there are three of four key points which you could highlight underneath that principle which really say: this is why you should advocate for it. One is a economic argument. Assesment of data requirements to satisfy local KYC. Define refine and understand the local context with respect to onboarding in financial services.
5	Risks or disadvantages principle A	Changing the regulation will take far to long. Yes we should be asking for flexible KYC or appropriatly designed KYC restrictions. However the core is: it is better to identify within the current KYC framework what data sets needs to be accumulated in order to create an appropriate picture of the beneficiary so that they might statisfy those KYC restrictions.
6	Appropriateness for humanitarian sector Principle A	✓
7	Usefulness principle B	What is gonna drive a government to instate any form of identity system is not privacy itself. It is the economic benefit that is gonna come when providing people their identities. - Ensure that public knowledge is at a level where individuals understand the importance and relevance of data. It is actually about how data can be used not only about how data should be protected.
8	Risks or disadvantages principle B	1. It is a very long haul game. 2. Privacy through DIDs can only be fully safeguarded when the services themselves are set up to enable that. At this particular time they are not.
9	Appropriateness for humanitarian sector Principle B	Primary advocacy when it comes to identity systems should actually be on economic benefits for the governments.
10	Usefulness principle C	1. I agree with this. What I would actually say is: Identify small scale prototype initiatives and demonstrate them in line with humanitarian core values. With really small tests you can show proofs of value. 2. I think from my perspective educational certification platforms is probably the lowest barrier to entry for SSI.
11	Risks or disadvantages principle C	You have to risk capital. Ultimately if you contain the risks appropriately, this should be seen as an innovation budget.
12	Appropriateness for humanitarian sector Principle C	Yes it is. We already register people, how we record the registration is relevant to specifically self-sovereign data systems. We can test them within our small enclave. We don't have to test them in a larger government approved process.
13	Usefulness principle D	1. I don't disagree with this one. Work with the private sector to identify key value propositions that would benefit them. 2. (On private sector in african countries having influence on political decision making):they will obviously have influence. 3. (On broadening the agenda to verifiable transaction history as a way to meet current requirements): It could possibly yes, agreed. Whether the use of the phraseology 'broadening the agenda' I dont think so. It is better described as refining and defining the agenda to be clear about the purpose. - It is about applying creative practices to defining data sets or data forms that would supplement those KYC requirements.
14	Risks or disadvantages principle D	The type of influence and the exercise of their (the private sector) influence may not always be in line with humanitarian interests. I am not going to deny the existence of corruption eventhough I havent experienced it myself.
15	Appropriateness for humanitarian sector Principle D	✓
16	Usefulness principle E	The reality is: If the government is standing in my way because they don't want people to access the financial system it is not because of the way in which I am delivering the identity.
17	Risks or disadvantages principle E	The UNHCR registration and provision of documentation is used as a way to access the wider humanitarian services for refugees and asylum seekers. That is a very specific environment and governments actively exclude refugees from national financial services due to the temporality of the refugee in that country. Not all, but many dont want refugees to have access to financial services because they dont want refugees be more permanent that they should be.
18	Appropriateness for humanitarian sector Principle E	I do believe that a network effect can drive the adoption of a technology. What that is based on is a proof of value of some sort. But if you are looking for legal identities to be created on the back of some form of attestable document it has to have quite an adoption before that is available.

Expert validation interview 2: Aiden Slavin, Chief of staff, ID2020

#	Question	Answer
	Part 1: Introduction and assesment framework	
1	Could you very briefly introduce yourself and your affiliation with digital identity or SSI in a humanitarian context?	I am currently chief of staff at ID2020. It is a public-private partnership that is working to improve lives through digital identity. We do that in three ways: Traditional advocacy, running programs aswell as doing some technical market shaping work. Before I joined ID2020 I did some work as a consultant with the IFRC on a pilot project that was trying to pilot blockchain technology to try to understand what the benefits and the risks are of using DLT for cash transfer programs. I have also done independent consulting with Sovereign foundation.
2	What are your thoughts on the circumstances and conditions assessment framework presented in figure 1 (the assessment framework)?	It is really interesting looking at it in this way. - (on the identity exclusion motive aspect):"I think that is a fantastic point. The reason why I asked about that aspect specifically is because I think that that really gets at the root of why doing identity in different ways is so challenging. and it is not so much that realising ID from a technical standpoint, that ofcourse is difficult. But what is really challenging, and I think Kenya is a great example of this, is exclusion that is already happening in social and political systems on the ground. I think regardless of type of ID you are working with, wether it is SSI or federated or traditional forms of analog ID, you will always have those problems of exclusion. - "Another point that I came accros when I was going through the table, I think it is imporant to include one row which reflects the trust in institutions from the beneficiaries perspective. " - "I love the point of legislation pressure, I think that that notion of liability is huge in this space. " - Another thing I would raise is the degree to which data is spread around different actors. "Slavin continues to emphasize on how information assymmetry within layered stakeholders also contributes to this.
	Part 2: Validating design	
3	Before we dive in to the assessment of each individual process principle, do you have any general thoughts on the 5 designed process principles?	/
4	Usefulness principle A	I think this would be really relevant.
5	Risks or disadvantages principle A	"I think so much of what made KYC important when it became a thing for large FSPs is still relevant. You would want some barriers to entry in order to access and use financial tools. But ofcource there are different ways to be able to achieve those end. And the Self-sovereign way to that, i think you could argue, would be sufficient to achieve those ends. But a lot of the stickie points and some of the risks will only come up when there is more practical implementations of this idea. " - "I think that is the more productive way of seeing it: How can we use different models of ID in order to achieve the criteria that already exist. There may be an argument for fundamentally rethinking their criteria, but I think it is a lot quicker way to achieve this end would be to explore different ways of meeting the current criteria. "
6	Appropriateness for humanitarian sector Principle A	✓
7	Usefulness principle B	I think that that is really important. And I think that it is something that should be done across all layers of the spectrum. At government level, at the CSO level and also among beneficiaries. I think this should be a process of teaching and learning aswell as communication because privacy means such different things depending on position.
8	Risks or disadvantages principle B	Privacy is such a complex and quickly evolving topic. If HOs are going to become more part of the conversation, they should be first educating themselves and increasing dialogue with privacy experts. One risk if you have organizations going out that dont necessarily completely understand privacy and its meaning.
9	Appropriateness for humanitarian sector Principle B	I should hope that it would be. I think that the humanitarian sector has expertise in areas of implementation that no other organizations do. I don't think that HOs at present state have the expertise inhouse on privacy that the ought to. I think that that is something that they could do a better job of. But I do think that given that some of these HOs operate in context and work with populations that no organizations do, they of course have a role to play in the conversation. Equally though, i think that the beneficiaries, the people that they serve should be a part of that diaglogue. They should be helping to create understanding of: what importance does privacy have to them and what do they really care about. I think so often privacy is unclear when it is not seen as a means to an end. So what is the end that the beneficiaries actually have in mind with privacy. - HOs need to do a better job of understanding what privacy could look like for beneficiaries, why it is important for beneficiaries. And I think that on the other side of things, HOs could do a better job of doing digital literacy trainings with beneficiary communities so they understand for instance: what are some of the risks involved with sharing your data.
10	Usefulness principle C	The humanitarian principle of Doing no harm is really a great guiding principle in this context. If that is constantly your bottom line that in and of itself can be a great way to mitigate a lot of the risks that these technologies create. I think that is an excellent point, i love the idea of using lateral services to create more awareness and more functionality for these tools.
11	Risks or disadvantages principle C	If HOs can show governments that using these models of ID they are reaching more people, that would be fantastic. One risk I see there is in the data collection. It would have to be a comparison of how many more people HOs are reaching that truly were not getting access before. A lot of the beneficiaries, in Kenya for instance that dont have an officially recognized ID, they still access aid. like you mentioned earlier: they have a SIM card, it is just not recognized in their name. There are still ways for them to access aid, by nominating a guardian. I think it is one thing to be carefull of there, in terms of not overinflating the importance of this technology. - Slavin emphasized that when scaling to lateral services such as educational credential providing, HOs need to be catious to prevent function creep in terms of unintentionally creating more exclusion.
12	Appropriateness for humanitarian sector Principle C	✓
13	Usefulness principle D	I think this is an important tool for HOs, but I don't think this is advisable that they do this in every context. If making a business case becomes an necessary qualification to extending an SSI program in the humanitarian sector, you will begin to see certain parts of population not get access to service. - "If the private sector will begin to see value here, that will make a much stronger case when it comes to governments accepting it. "
14	Risks or disadvantages principle D	"Part of the core values of HOs is: we must deliver service regardless. The private sector does not have that as part of their basic mandate. They have a profit motive and there are a lot of communities that the HOs serve for which the business case is really weak. " Commercial interest is a good way to include the private sector, but they have a different agenda compared to HOs. When leveraging that you need to watch out for the downsides. - The extension of credentials for transaction history is really interesting. One thing that needs to be in place there is non-correlatability. A true to form SSI system is a part of that, but mitigating the mosaic effect, the ability to reidentify using discrete pieces of data, building that in the design of the system is really important there.
15	Appropriateness for humanitarian sector Principle D	I think this is an important tool for HOs, but I don't think this it is advisable that they do this in every context.
16	Usefulness principle E	I think the idea behind the credential is really good which implies: you dont have to be dependent on the government in order to make this leap. But I dont think in every context it makes sense to delay government commitment. In certain contexts it would make sense to actually bring the government in. - (on humanitarian credentials being sufficient in other countries) The same is actually the case in Egypt, they have started accepting UNHCR credentials as sufficient to get access to a SIM card. - I don't think we are gonna see adoption following the same steps in every place: Some countries, and less so countries: FSPs often self-govern, they will determine that a UNHCR credential or a Red Cross credential is sufficient. And then you will see a network effect take hold in that country. And then maybe its neighbours begin to take notice.
17	Risks or disadvantages principle E	I think in certain cases government will be your most important stakeholder. So the risk on missing out on an opportunity. Sometimes governments do have relevant expertise in scaling identity systems.
18	Appropriateness for humanitarian sector Principle E	✓