03-11-2020

STRATEGY LUNCH #3 Statement: Sovrin and SSI has currently no value for the 121 platform

Attendees: Ruben van der Valk, Jannis Visser, Elwin Schmitz, Orla Canavan, Diderik van Wingerden, Maarten van der Veen, Lars Stevens (note taker)

The problem

NLRC/510 identified (amongst others) the following problems in the humanitarian sector:

1. **Lack of interoperability** in humanitarian programs regarding identification, registration and inclusion, leading into sector wide inefficiencies
2. **Lack of proof-of-identity** is blocking identification and registration of most vulnerable
3. **Lack of (data) security** in most identification & registration systems in the humanitarian sector because they are centralized and most organizations not well equipped to secure them
4. **Lack of responsible data use**, processes within humanitarian organizations do not incentivize data minimization and most systems are not developed on privacy-by-design principles, allowing organizations to collect, store and share more data than necessary

The idea

The world is rapidly becoming more connected and digital. The humanitarian sector is using more CVA which increases the digitizing of aid and sharing personal information with financial service providers. In this context, NLRC/510 believed that self-sovereign identity could tackle these four problems:

1. A person affected would need to create one SSI and get different validated identity attributes which could be used with multiple organizations, given the following assumptions are valid:
   1.1. Person affected is or can become digitally literate to create, use, update and delete their identities
   1.2. Person affected has the device and internet connectivity to create, use, update and delete their identities
   1.3. Organizations want (digital) interoperability on identification, registration and inclusion with other organizations
   1.4. Organizations trust validated identity attributes issued by other organizations
   1.5. Organizations are or can become digitally literate to issue, validate and accept identity attributes as a means of identification/authentication
2. SSI could be used by one organization and/or the sector, then grow to a foundational purpose as being adopted by government, given the following assumptions are also valid:
   2.1. Governments are likely to accept and adopt SSI
   2.2. Industry will prefer SSI because of quick authentication and a formerly untapped customer base
3. SSI is decentralized, Sovrin has a strong governance framework and blockchain is tamper proof, given the following assumptions are valid:
   3.1. It can be used and remains to be used in a decentralized way
   3.2. Personal data is not stored on the blockchain but safely somewhere else
4. SSI is developed using privacy-by-design principles, this will force organizations to consider responsible use of data and thus result into less data collected, stored and share, given the following assumptions:
   4.1. Interoperability will benefit from a minimal subset of registration data for each person affected, organizations will develop this
   4.2. People affected can easily stop sharing personal information
   4.3. Organizations will not have to share datasets with others outside of the system

03-11-2020

The test

- NLRC/510 and TYKN together explore technologies and support research.
- A mock-up is developed and tested in Ukraine together with Dorcas.
- A follow up project (DIF) is already granted before the results come in.
- NLRC/510, Tykn and consortium partners agree on software requirements and start building it.
- Tykn develops the back-end, NLRC/510 the front-end and system around it. All code is published on Github.
- NLRC/510 starts validating some assumptions regarding desirability of people affected and aid workers in Ethiopia, Malawi and Kenya.
- NLRC/510 continues to develop the system.
- System is piloted in Netherlands and Kenya

The reflection

Due to the project set-up NLRC/510, Tykn and consortium partners started to build without validating the riskiest assumptions. This reflection is about those assumptions.

Lack of interoperability

Whether a person is or can become digitally literate (1.1) and has the means to use digital identities (1.2) was validated through co-design sessions in Netherlands, Malawi, Ethiopia and Kenya. 1.1. is partly validated as people do seem to be able to register but results are in an early stage. We will not be able to test whether people are able to continue use, update and delete their identities. 1.2 was disproved for the pilot context (rural, African). In Malawi, Ethiopia and Kenya, there was limited internet connectivity and very low smartphone penetration. As such, NLRC/510 decided to focus on an offline scenario and had to halt further development of SSI. NLRC/510 and TYKN looked at the potential to develop a solution for feature phones and applied for funding, this was not granted. There is no feature phone solution today.

In some settings organizations want (digital) interoperability (1.3), but this assumption cannot be generalized. For example, KRCS opted for community targeting and review, Tearfund Malawi opted to validate only a subset of people affected, Caribbean branches used video-calling and NLRC worked with a pre-targeted list from a partner organization. In other words, in none of the pilots people affected end up with validated identity attributes. Hence, it looks like organizations want to either have a human in the loop or work with partner organizations who know the people affected instead of digitally accepting their identities. One exception may be found in biometric identifiers but this introduces a whole other set of risks. As such, it is contestable whether other means of digital authentication such as federated identities (OAUTH e.g.) would add significant value.

Organizations would need to trust each other, their processes and the validated identity attributes they create (1.4). NLRC/510 has found that even within consortia this trust may be lacking. Technology on its own may create the possibility, but there is a need for coordination between organizations to materialize trust and get it working in practice. There is no previous experience with this. One could argue that in a disaster setting strong coordination is crucial to streamline efforts, avoid duplication and optimize resources. This requires coordination not just on registration but also on targeting, selection criteria, amounts, other types of aid etc. The coordination mechanisms in place could be undermined if this is not centrally organized. Technically, an organization would at least have to be able to request a mandatory aid track-record from each person affected. So far NLRC/510 and TYKN have not been able to develop this functionality. In other words, deduplication using SSI is not easy.

If organizations are or can become digitally literate (1.5) to work with SSI is difficult to validate. This opens up the wider question of digital transformation in the sector and is very much organization and person dependent. NLRC/510 believes some organization will find this easier than others. From experience in this project it is apparent that we should check all of our (technical and non-technical) assumptions and that any system launched in the humanitarian should take this into account by providing adequate and pragmatic learning resources.

Lack of proof-of-identity
NLRC/510 has supported thesis research on the potential for functional SSI to become foundational within Kenya. The conclusions from this research disproof assumptions 2.1 and 2.2 for the Kenyan context. The government first needs to prioritize privacy and act on it, the privacy movement (although growing) is yet to small to force any changes. Humanitarian organizations can lobby and demonstrate but this will be a long-term effort. NLRC/510 and KRCS also experienced this in practice when Safaricom was denied to provide sim-cards for people without formal identification in our pilot setting, even after 1.5 years of lobbying. It is debatable if these results are generalizable. However, Kenya is quite digitally advanced and has some data protection jurisprudence. In many other contexts where humanitarians work the conditions are less favorable.

Lack of (data) security
Technically it is possible to use and keep using SSI (3.1) in a decentralized way but this requires people affected to own smartphones or create secure and decentralized cloud storage solutions. There is a risk that these cloud storage solutions will become centralized themselves. Personal data is indeed not stored on the blockchain (3.2) but elsewhere. The security level is very much dependent on where elsewhere is, if decentralized than at least risk is reduced for widespread loss of personal information. However, if personal data is stored centrally, for whatever reason, the same risks will apply as for centralized identity systems even if the pipework is SSI based.

Lack of responsible data use
It is difficult to test whether organizations will want to standardize their data collection across the sector (4.1). NLRC/510 observed that Kobo and other mobile data collection tools enable organizations more than ever to collect and digitize surplus data. In pilot contexts, the amount of data collected was brought down out of technical necessity. Our system is not (yet) specialized for survey questions making it difficult to add them, plus testing the interface will work better with a shorter survey. One could argue that self-registration in general could minimize data because more people will provide better information if surveys are well orchestrated. This does not have to be an effect of SSI.

Technically it is possible for people to break up the data sharing agreement with organizations in a SSI system. The lack of technology, digital literacy and power imbalance between people affected and organizations may in practice block people from actually doing so. Other than that, legal reasons and donor obligations require organizations to still keep financial and personal information for set durations.

Throughout development, NLRC/510 was repeatedly requested to enable humanitarian organizations to download personal information (4.3) as .csv or .xls files to be able to properly run CVA programs. Printing lists, doing analysis in excel are still very much the norm and would have to be embedded as functions in the system. From experience with RedRose, EspoCRM and other corporate applications a better role-based access system, logging and UX could have a more profound effect on limiting the sharing of datasets.

Conclusions

- NLRC/510 intended to develop and use SSI but at the moment our system does not use SSI
- Ideologically, giving cash as aid and enabling people to own their data, increases the autonomy and dignity of people in need. NLRC/510 still very much believes that.
- The focus for SSI was more solution than problem oriented, these problems still stand.
- Technically, SSI is feasible and usable given good internet connectivity and smart devices.
- Practically, SSI in the humanitarian sector is currently not feasible. It is unlikely that it will yield significant scale in the short- to midterm.
- It remains unclear if there is a need for reusable digital identification/authentication. If that need is confirmed, a new choice should be made between fully decentralized (SSI), federated and/or centralized identity solutions. This choice should be informed by context, needs and strategic value.
- Privacy-by-design is important but not a goal in itself, it is a design philosophy that should be used in any (digital) product development. Given you value data protection. Not everyone will value data protection in the same way.
- Effective and immediate results could be booked by simpler and less resource intensive solutions. This can lead to more understanding and interest to later adopt more serious privacy enhancing technology. One could think of advisory, educating aid workers to protect excel sheets, adequate document management, corporate policies for devices, role-based access management, properly writing consent statements, logging tools and following up on rule breaches etc.
- The practical experience in applying privacy-by-design principles should be merged with the advisory role of data responsibility officers to be embedded in all 510 products/services.
- SSI development is resource intensive and requires an innovative approach while NLRC/510 works in a conservative sector
- NLRC/510 has tried its hardest and many learnings are taken from this and can be put into other products and services
- NLRC/510 should stop working towards SSI, take out the SSI components in existing systems and continue to work with a central data storage

Met opmerkingen [WD1]: The architecture of the 121 platform is actually not central data storage: each NGO runs their own instance of the platform, hence also have their own database with the data of only their programs and PAs. Scaling the 121 platform (or the registration module of it) could actually lead to some of the advantages that SSI/Sovrin promised by adding interoperability between instances.