Working Note: Universal Recommendations for Implementation of Digital Identity Solutions for Refugee Populations

Authors: Balazs Nemethi (b@taqanu.com), Vilas Dhar (vilasdhar@gmail.com)
Date: April 22, 2019

To refugees and internally displaced peoples in the throes of escape from violence and persecution, ensuring the physical safety of identification documents often takes lowest priority over physical safety, political asylum, and basic needs . Nevertheless, the ability to identify oneself transcends the transactional necessities of registration, protection, and access to services - identity is often tied to dignity - a sense of belonging, place, and power.

As technologists and policy makers in the space, we continue to see the concept of digital identity continue to grow in scope and promise - in commercial and developed settings through increasing government and civil participation in voluntary identification protocols, and in developing environments through the use of Aadhar or similar national government service delivery mechanisms.

Nevertheless, digital identity as a technology implementation for refugee populations continues to struggle. Due to technology complexity - numerous vendors offering limited solutions, lack of regular access to connectivity, language and localization issues, and difficulty accessing enterprise level software development expertise - any solution that shows promise at pilot stage invariable collapses under the needs of addressing multiple disparate populations. Even when technology stacks scale, implementation risks and the necessity to train multiple stakeholders on proper use often collapses under limited resource sets. And at a conceptual level, digital identity solutions attempt to solve a critically dynamic problem set - meaning that current solutions rarely solve tomorrow's problems.

In this note, prepared as a summary of ongoing work and research for purposes of inclusion in UNHCR's Digital Identity Summit, we lay out the theoretical underpinnings of a multi tier approach to a global digital identity solution - beginning first with the characteristics of a properly developed basic technology approach to verification and authentication, and then scaling through intermediate and advanced tiers of functionality. Our hope is that this phased approach meets the demands of a system that grows over time to operate globally , with concentric rings of functionality and data protection bridged using interlocking pilots connecting the entire framework.

This note ends with a series of working recommendations - intended to mature with continuing research and discussion - that may guide further conversation in the service of implementing these principles in a working pilot.

Recommendations for a multi-tiered approach to deployment of a digital identity platform:

1) Basic characteristics of a first tier identity system:
    a) Despite mainstream effects to decentralize, the need for a central authority and verification mechanism dictates the creation of a centralized **data storage module** to offer the ability to map agent behaviours participating in the early versions of the system. Because this structure offers simple management of authority and clear source of verifications, initial implementation of the system can enjoy the ease of audit, point of service delivery implementation, and high levels of data validation and integrity.
    b) The first element of identity shall be a **unique identifier** issued to everyone regardless of status or background. The format of this identifier is a unique numerical identifier or machine-readable QR code format - easily distributed via physical or digital means - even at the point of registration (ie, field printer). The intention of this identifier is to establish first connections and enable unverified participants of the system to access basics functionality (similarly, as a punch card enabled access to services/buildings). From a technology perspective, the issuance of these identifiers shall be the most basic decentralized identity connected to the central database only to ensure future interoperability and experience with issuance and authentication of such basic identities.
    c) The next element of identity functionality concerns the ability to attach data to the identifier for stronger **authentication and verification** purposes turning the unique identifier into a personalized one. Using the linked identifiers UNHCR agents should be able to add data to the storage such as biometric, personal data and documentation in their respective formats with the appropriate levels of security using encrypted means for data transfers.
    d) Following this step a user is registered and have the capability to authenticate against its personal identifier. We acknowledge the need for a conversation on personal data management, but believe this can be deferred to later stages of implementation.
    e) The digital identifier is a **universal** and unique **token**, with many onramps for authentication(ie, fingerprint, iris, facial scan, pin&pass) - create cooperation in the market of devices or make it all smartphone based to avoid dependency. Guiding principle: Usability should be the first priority for l**ow-value transactions**, increasing the complexity of authentication as transaction importance increase. *(In the west we can spend up to 30EUR with a tap of a card, then we shall not require iris scans for every transaction)*
    f) Development of basic **vendor-side** application that addresses the basic level of services necessary for low hanging fruit implementation - basic service delivery, camp access, food rations, medical care, etc. - integration for UNHCR wide delivery
    g) **Role definition** - who can access (read and write), verify, change various types of data - POS, camp administrators, central data workers, etc.
    Parts of the data will be required to be sharable with other agencies and moving

data should be easy for future interoperability between the central and personal identities.

2) Intermediate
    a) **3rd party vendor authentication** - Invite 3rd parties to interact with the personal identifiers following verification of the person/organisation and authorize certifying authority within organizations - distribute trust with UNHCR at its centre with sole authority to provide privileges - central proof/trust/authentication mechanism.
    b) **Vendor segmentation** - Landscape scans of vendor roles and access needs (Ie, other iNGOs, resettlement agencies, government authorities, financial services) The ability to share segmented parts of data must be a concern and the management of this must be core to the system. Earlier enabled SDKs must be capable to offer this service as well as the ability to pass data into the management of the user if required and possible.
    c) UNHCR must create the ability to monitor and block actors with wrong intentions - ie, UNHCR must act as a **gatekeeper** to the user's identity data to avoid mismanagement.

3) Advanced
    a) **Transportability of identity** (and data) - The adaptation of a tiered based identity and management system will enable the system to align with local/global interoperability standards (and privacy regulations) as it can offer porting mechanism from its central database.
    b) **Privacy regulations** - As privacy regulations are introduced in a growing number of countries the system introduced here shall be aligned with those. Safeguarding personal data and core services for the initial centralized management must be located in the jurisdiction(s) with the highest standards for privacy.
        i) **Personal ownership** of data leads to a decentralized data management. This form of data storage eliminates the creation of data "honey pots", however, it opens new opportunities for individuals to mistakenly open their data storage for unauthorized services. To prevent this, we propose that storage of data is decentralized, however, given data sets require higher level authentication from the party created the dataset.
    c) **Interoperability** with global (technical) standards - Governments and global organisations are all working towards digital identity systems, however, there is no clear direction what privacy protocol will be adopted in the future to store and manage data. To prevent misalignment we propose the introduction of decentralized identifiers (DIDs) and other required services to create a future proof open-source standard based solution that will have the capability to align with local privacy regulations and standards.
    d) **Transparency** - UNHCR technology stack is facing the question whether to use open-source or black boxed technology. As parts of the suggested stack are still in research phase we propose the use of a black box based solution that is

based on open-source standards. Through this method we will have the opportunity to open-source the entire stack once security is proven.

The working conclusions and questions set forth above provide a roadmap for considerations for any pilot or test of digital identity solutions over time - and serve as the backbone of a longer academic and policy work that may emerge over the course of this UNHCR summit process.