Design Considerations of a Digital Identity Systems for Refugees

Sanjay Sarma, Philipp Schmidt
Massachusetts Institute of Technology (MIT)
June 6th, 2019

The MIT Office of Digital Learning and the MIT Media Lab have a keen interest and extensive experience in the design of digital identity/ credentialing systems as well as the use of technology to address challenges faced by refugee populations.

We are excited about the potential of recent developments in strong cryptography and decentralized computing systems such as distributed ledgers (including blockchains) for the design of new digital identity infrastructures. But we are also deeply concerned about the possible negative outcomes such systems might have in particular for vulnerable communities. There is no room for error when individuals rely on sociotechnical systems in order to access essential resources they need to survive, or rely on these systems to protect them from prosecution. Given the potential misuse and unintended negative consequences the burden should be high for new technology systems to demonstrate how they can meaningfully improve the situation of refugees.

In this short concept note we focus on three aspects of designing identity systems for refugees, which seem worth further exploration through the consultation process you outlined on the UNHCR website: (1) the importance of putting in place clear guidelines for the design process to ensure that the needs and interests of the target audience are centrally considered, (2) an emphasis on technology choices that offer the strongest opportunity to limit access to personal data, such as zero-knowledge proofs, and (3) the importance of investing in the human aspects of a technology-based identity solution.

Guidelines for the design process

In addition to carefully reviewing the advantages (or disadvantages) of specific technology choices, we recommend articulating a set of technical, policy and process requirements that guide the design, development, and deployment. These requirements themselves will be created through a multi-stakeholder approach and with input from refugees, but in order to provide a more concrete idea of the types of possible considerations we have in mind, please see a few example requirements below:
- Ensure that refugee input is considered in all stages of the design and development process.
- Articulate minimum requirements that can trigger automatic discontinuation if not met.
- Prepare fallback options to be able to quickly adjust for unintended consequences.
- Embed monitoring and oversight structures that can limit or shutdown the system.
- Enable quick interventions at the level of individual cases to address problems/ misuse.

- Provide high-level technical expertise to support UNHCR and other partners during the design process.
- Etc…

Technology systems that limit disclosure of personal data

Given the particularly sensitive nature of refugee identity data, we recommend exploring the use of cryptographic approaches that greatly limit access and disclosure of personal data. In particular zero-knowledge proof approaches allow two parties to reliable confirm the existence of specific facts (e.g. an individual has been registered as a refugee) without having to disclose any further information. By building up from technology foundations that place protection of the individual's data at the core, the probability of potential misuse or unintended consequences can be reduced.

The importance of the human aspects of a technology solution

While there is rightfully much interest in the potential of new technologies to solve some of the challenges around refugee identity, we recommend focusing at least the same amount of energy (and maybe more) on the human and organizational systems that need to be put in place to support the technology. All identity systems are socio-technical in nature and ensuring that the organizations interfacing with the system are well trained and prepared is paramount.

About the contributors

Sanjay Sarma is the Fred Fort Flowers and Daniel Fort Flowers Professor of Mechanical Engineering, and VP of Open Learning at the Massachusetts Institute of Technology. He is one of the architects of India's national identity system Aadhaar.

Philipp Schmidt is a research scientist at the MIT Media Lab. He designed the standards that are used by MIT to issue blockchain-anchored digital credentials to its graduates, and managed the Refugee Learning Accelerator that created technology-supported education programs for refugee learners in the Middle East.

We thank our colleague Jeff Dieffenbach for his helpful feedback on an earlier draft.