Funded by the Government of Canada
Financé par le gouvernement du Canada

Global Virtual Summit on Digital Identity for Refugees, Concluding Workshop: Summary Conclusions and Recommendations

Introduction

UNHCR, the UN Refugee Agency, with the support of Immigration, Refugees and Citizenship Canada (IRCC), has been undertaking a consultation project on digital identity for refugees and its role in enabling the implementation of the Global Compact on Refugees ("GCR"). As part of the consultations, 90 written submissions were received and three online events were held on 21, 24 and 29 May 2019, with a total of 24 speakers making presentations. Each online event was attended by around 100 participants. A workshop was held in Ottawa on 12 to 13 June 2019 at which 36 participants considered the themes raised throughout the consultation process in greater depth.

This document sets out a summary of the workshop's conclusions and recommendations. It does not represent the individual views of each participant or necessarily of UNHCR, but broadly reflects the understandings emerging from the discussions.

Preliminary observations

As digitalization increases in all sectors of life, refugees will increasingly require a digital identity if the GCR's goals are to be realized across the full spectrum of forced displacement. Registration and enrolment in a digital refugee registration system by UNHCR or the host State can facilitate access to basic assistance and protection and ensure the integrity of refugee protection systems particularly in the contexts of emergencies and mass influx.[1] An official or legally-recognized digital identity can help refugees to register a SIM card or open a bank or mobile money account in their own name, enabling the digital delivery of dignifying cash based interventions as well as longer-term economic inclusion.[2] Digital identity also contributes to solutions, with digitalization strengthening the integrity of resettlement processes and facilitating the processing of applications and integration.[3] As States and humanitarian actors increasingly digitalize their

[1] *Global Compact on Refugees ("GCR"), para 58*
[2] *GCR, para 100*
[3] *GCR, paras 90-96*

systems and processes, a recognized and trusted digital identity will become progressively more important for refugees to access essential services.

At the same time, some participants noted the risk that digital identity systems could also enable the implementation of discriminatory policies that can prevent refugees from accessing essential services. For example, refugees may be prevented from enrolling in the host State's foundational digital identity system, making it harder to establish their identity and preventing access to services. New protection risks were also highlighted, including the unauthorized access to refugees' personal data held in digital systems or the broad and unregulated collection, sharing and retention of personal data by humanitarian organizations. Likewise, the fear was expressed that digital identity systems have the potential to track, monitor or undertake the surveillance of refugees, jeopardizing the GCR's protection goals.[4]

Taking these considerations into account, the need to step back and ask whether digital identity is necessary to solve a particular problem or access a service, particularly life-saving humanitarian assistance, was emphasized alongside the importance of considering alternative models that prevent risks.[5] Similarly, to avoid the risks of exclusion and limitations on access, humanitarian systems could be designed in a way that do not make the use of a digital identification mandatory and allow alternative ways for refugees' identity to be authenticated or verified. Special care is required to ensure that new technologies, systems or approaches promote rather than undermine refugee protection.

1. Defining "digital identity"

The term digital identity is used with different meanings depending on the context. For example, digital identity can be the persona that an individual uses on the internet (e.g. a username in a chat forum), personal data in digital form (e.g. a Facebook profile), login details for websites (e.g. to access online banking) or proof of an individual's legal identity in digital format. In the context of the GCR, examples of a digital identity that enables protection, solutions and access to assistance include a refugee's digitally stored identity records in UNHCR's Population and Refugee Identity Management Ecosystem (PRIMES) or a refugee's legal identity in the host State in digital format.

[4] *GCR, paras 45, 58 and 82.*

[5] *See https://privacyinternational.org/advocacy/2994/privacy-international-participates-global-virtual-summit-digital-identity-refugees*

UNHCR should adopt definitions of key terms relating to digital identity, consistent with emerging international standards and the existing international legal and policy framework relating to refugees, including the GCR.

Potential definitions that were suggested included:

- **Digital identity:** a set of electronically captured and stored attributes and/or credentials that uniquely identify a person within a specific population.[6]
- **Trusted digital identity:** an electronic representation of a person, used exclusively by that same person to receive valued services and to carry out transactions with trust and confidence.[7]
- **Proof of legal identity:**[8] a credential, such as a birth certificate, identity card or digital identity credential that is recognized as proof of legal identity under national law and in accordance with emerging international norms and principles. In the case of refugees, Member States are primarily responsible for issuing proof of legal identity, including identity papers.[9] The issuance of proof of legal identity to refugees may also be administered by an internationally recognized and mandated authority.[10]
- **Trust framework:** a set of agreed upon definitions, principles, conformance criteria, assessment approach, standards and specifications.[11]

2. Establishing digital identity principles, standards and practical guidance in respect of asylum seekers and refugees

The identity challenges relating to refugees are in many ways unique. Many refugees do not possess any identity credentials when they arrive in a host State because their credentials may have been left behind, lost or destroyed during flight. Some refugees may have never been registered in the country of origin's legal identity system in the first place because they came from fragile or conflict affected areas or suffered from discrimination. At the same time, refugees require special protection which includes preventing the authorities of the country of origin being contacted to verify a refugee's identity, without consent and if there is any risk of

[6] *World Bank, Identity for Development, Practitioner's Guide, Draft for Consultation, June 2019*
[7] *Pan-Canadian Trust Framework, see https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16577*
[8] *See UN Legal Identity Expert Group/World Bank Operational Definition of Legal Identity*
[9] *1951 Convention on the Status of Refugees, Article 27*
[10] *1951 Convention on the Status of Refugees, Article 25*
[11] *See the Pan-Canadian Trust Framework: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16577*

harm.[12] For these reasons, host States are primarily responsible for providing refugees with a legal or foundational identity, supported by UNHCR where necessary.

Humanitarian contexts create additional complexity. Refugees are often issued with identity tokens by multiple humanitarian assistance providers to facilitate access to assistance and services. There is a risk that different providers develop multiple digital identity systems that are neither appropriately adapted to the context nor interoperable. Gaps in digital literacy may also prevent refugees from using or navigating these systems effectively.

UNHCR's Protection Mandate places the Agency in an ideal position to develop digital identity principles and standards for refugees, which enable the realization of the GCR's objectives. The "Good ID" design features of privacy, inclusion, transparency, accountability, personal value, user agency and security will provide useful reference points in developing and establishing such standards.[13] States, humanitarian organizations and the private sector also require practical guidance on how to implement such standards in the design and operation of digital identity systems that include refugees.

Given UNHCR's central role in the humanitarian ecosystem, the Agency could also convene a stakeholder group to support the development of digital identity standards and guidance for the humanitarian ecosystem as a whole.[14] It could also contribute in the longer term to the establishment of a trust framework for the humanitarian sector similar to the Pan-Canadian Trust Framework.[15]

Refugees will increasingly need to have access to a legally recognized identity to realize the GCR's key goals of allowing them to contribute more to their host communities and to facilitate their economic inclusion. Research by UNHCR and GSMA[16] indicates that non-conducive regulatory environments are one of the "hard stops" that prevent refugees' access to mobile connectivity and financial services, with ID-related regulatory requirements proving to be the most significant barriers. To promote access to services, financial and telecommunications sector regulators should issue guidance on what constitutes a reliable and independent source of identity for refugees and how risk-based approaches can be applied to prevent exclusion. At the same time, UNHCR could consider how its systems, policies and practice and the technical support provided to host States could be further aligned

[12] *See ICAO TRIP Guidance on Evidence of Identity (2018): https://www.icao.int/Security/FAL/TRIP/Documents/ICAO%20Guidance%20on%20Evidence%20of%20Identity.pdf*

[13] *See https://www.good-id.org/en/*

[14] *See http://docs.cariboudigital.net/identity/Identity-At-The-Margins-Identification-Systems-for-Refugees.pdf*

[15] *See https://canada-ca.github.io/PCTF-CCP/overview/pctf-overview.html*

[16] *GSMA is the Global Association of Mobile Network Operators, see https://www.gsma.com/*

with international digital identity technical standards to facilitate greater recognition of refugees' identity. For example, the Agency could consider how the capacity of PRIMES for identity authentication could be strengthened, alongside other integral elements of the digital identity lifecycle.[17]

As countries and regions move towards developing trust frameworks, identity considerations relating to refugees will need to be appropriately reflected. Where UNHCR's systems or processes interact with a State's trust framework, alignment will be required. UNHCR should look to explore these issues in a relevant use case, such as facilitating the integration of refugees selected for resettlement, and aim to avoid the emergence of new barriers.

3. Privacy and data protection

The GCR recognizes that the protection of refugees' privacy and personal data is necessary to achieve its goals.[18] Digital identity systems implemented by States, the private sector and humanitarian organizations require strong legal, regulatory and policy environments relating to privacy and data protection, accompanied by robust implementation mechanisms.

UNHCR should develop specific guidance on how data protection and privacy principles should be realized by States, the private sector and humanitarian organizations when processing refugees' personal data and the principles that should be included in national legal and regulatory frameworks. This guidance should be built on the foundation of the Policy on the Protection of the Personal Data of Persons of Concern to UNHCR[19], other relevant international standards, including those contained in international human rights law.[20]

Providers of trusted digital identities for refugees, such as the host State or UNHCR, should aim to respect key data protection and privacy principles. For example, the principles of data minimization and purpose specification should be respected at the time of registration or enrolment and during processing. Digital identity systems should have the capacity for identity verification and authentication whilst minimizing the amount of personal data that is shared with

[17] *See, for example, UNHCR "Displaced and Disconnected" : https://www.unhcr.org/innovation/displaced-and-disconnected/*
[18] *GCR, paras 45, 58 and 82.*
[19] *See UNHCR Policy on the Protection of Personal Data of Persons of Concern: https://www.refworld.org/pdfid/55643c1d4.pdf*
[20] *E.g. Universal Declaration on Human Rights, Article 12 and the International Covenant on Civil and Political Rights Articles 17 and 26*

third parties. This can include the use of tokens and "zero-knowledge proofs".[21] Where consideration is being given to sharing refugees' personal data, particularly biometric data, this should be undertaken in a regulated environment with suitable safeguards in place. The appropriate use of Data Protection Impact Assessments to evaluate and inform risk prevention and management is particularly important when considering large scale or systematic sharing of refugees' personal data.

A culture of privacy and data protection should be encouraged and consistently strengthened in all bodies, including humanitarian organizations, that process refugees' personal data, with compliance and accountability mechanisms established. The sensitization of staff and filling the knowledge gaps are essential. Digital identity systems should be designed to include effective and accessible accountability and feedback mechanisms to address any issues that arise, including avoiding the risks of a single point of entry and failure.

Clear communications with refugees and asylum-seekers are necessary to ensure that they are informed of and can access their rights as "data subjects", including their right to access their own personal data, request correction and deletion of certain information, or object to certain forms of processing. Where consent is the legal or legitimate basis for the provision of personal data, including biometrics, it must be both freely given and informed. However, participants also noted the inescapable challenge of whether refugees were in a position to withhold consent in the context of registration to access humanitarian assistance. The need to find solutions to this issue consistent with humanitarian principles was emphasized by participants.[22]

4. UNHCR's role in registration and identity for asylum seekers and refugees in the context of the GCR

Consistent with the existing international legal framework and Sustainable Development Goal, Target 16.9,[23] the GCR envisages that host States will increasingly take greater responsibility for refugee registration and ensuring that they have a recognized legal identity. Where required UNHCR's supporting role in

[21] Tokens permit the service provider to authenticate the identity and register an individual in a database without providing personal data, such as the individual's unique identity number. A zero-knowledge proof allows one party to prove to another party that it knows a certain value (e.g. that the person is old enough to apply for a driving license) without providing additional information.

[22] Cf ICRC/Brussels Privacy Hub, Handbook on Data Protection in Humanitarian Action (2017), p. 45 at: https://shop.icrc.org/e-books/handbook-on-data-protection-in-humanitarian-action.html.

[23] Sustainable Development Goal Target 16.9 provides "by 2030 provide legal identity to all, including birth registration"

these areas will continue, particularly in emergency contexts of mass influx, in facilitating transitions, providing protection and assistance and enabling solutions. The Agency will also continue to offer technical and other support to host States, including the provision of appropriate digital and biometric technology for refugee registration and facilitating the inclusion of asylum-seekers and refugees in host States' civil registries and legal identity systems.[24]

As States increasingly develop digital identity systems, UNHCR must consider how PRIMES should evolve to work as part of the host State's digital ecosystem, for example, by interoperability with host States' digital identity systems where an appropriate enabling environment is in place. In this context, where no "one size will fit all", multiple technical solutions will be required within a standards-based framework. In some contexts, in order to meet the objectives of the GCR, UNHCR may be required to undertake the role of a provider of legal or foundational identity or a trusted digital identity provider, as part of the host State's digital identity ecosystem and regulatory environment.

5. The design and development of the humanitarian digital identity ecosystem

UNHCR, as a result of its Mandate, experience and digital systems that help to guarantee integrity in humanitarian assistance delivery, is also likely to remain as an important identity provider for asylum-seekers and refugees within the humanitarian ecosystem. Depending on the national legal framework of the host State, the identities provided in this context may be primarily functional in nature, facilitating access to protection, humanitarian assistance and solutions.

"People-centered approaches" are particularly important in the design and development of digital identity systems for refugees, with consultations with refugee communities an essential ingredient. Digital identity systems for refugees should have an increased emphasis on user control and choice. They should be able to provide refugees with greater control over the personal information that is shared with third parties in each circumstance or "use-case". "Edge cases" amongst the refugee population could be the focus of design to avoid the risks of exclusion and to promote equal access to digital identity. These approaches may require additional research, including on how to appropriately include and

[24] *GCR paras 58 and 82*

accommodate the full range of age, gender, disability, and diversity amongst refugee populations in digital identity systems[25].

Good practice indicates that a set of technical, policy and process requirements that guide the design, development, and deployment of new platforms should be established at the start of any design process. They should include safeguards established to manage risk, including minimum requirements that can automatically trigger discontinuation. Given the vulnerability of refugees, to adhere to the principle of "do no harm", design should also prepare to "fail well" to avoid putting refugees at risk.

6. Implications of new technologies and approaches

The GCR reflects the opportunities that new technologies and approaches can provide for refugees, for example, through online education and livelihood opportunities.[26] UNHCR's approach places an emphasis on using established technologies and is cautious about the use of emerging technologies to mitigate potential risks. Echoing the GCR, the protection and security of refugees' personal data are priorities. However, it was recognized that this approach would not necessarily be followed by all entities which offer or provide services to refugees.

The establishment of a multi-stakeholder technology ethics board could screen technologies to give guidance on the use of emerging technologies for refugees using the experience of the technology sector, such as large scale platform providers.[27] It was also recognized that refugees required information about platforms or services which used certain technologies and the risks that could arise. A "quality mark" system or model based on both technical and protection standards, could help to address these issues, learning from existing models.[28] The need to be aware of and evaluate developments in emerging technologies such as biometric facial recognition and its applications and blockchain/distributed ledger technology were highlighted.

It was noted that digital identities will be necessary for refugees to take advantage of the opportunities offered by new technologies, such as online education or work. However, platforms will need to be designed in ways which are appropriate to

[25] *GCR, paras 13 and 58*
[26] *GCR, paras 69 and 71*
[27] *See https://www.unhcr.org/idecosystem/wp-content/uploads/sites/69/2019/06/CIGI_Global-Compact-on-Refugees-and-Digital-Identity_Technology-Ethics-Boards-Final-Submission.pdf*
[28] *See https://medium.com/id2020/id2020-launches-technical-certification-mark-e6743d3f70fd*

refugees' needs. Low-tech solutions may be more appropriate to many of the environments in which refugees reside. Efforts would also have to be made to ensure that all refugees were sufficiently data literate to prevent practical barriers to access arising from the use of new technology.

"Vendor lock-in" was identified as a risk that should be managed, particularly by UNHCR and the public sector, including in relation to the control of personal data processed by proprietary systems. Open source, standards-based models for digital identity systems that placed an emphasis on interoperability were identified as one way to address these issues.

Workshop Participants*

Daniel Bachenheimer, Accenture Security

Sara Baker, The Engine Room

Othalia Doe-Bruce, InnovFin Consulting Inc., Canada

Amos Doornbos, World Vision International

Tom Fisher, Privacy International

Moses Karanja, Omidyar Network

Meredith Kravitz, ID2020

Jonathan Marskell, ID4D, The World Bank

Aaron K. Martin, Tilburg Law School, Tilburg University, The Netherlands

Elif Mendos Kuşkonmaz, University of Portsmouth, United Kingdom

Balázs Némethi, Taqanu

Sabaa Notta, Columbia School of International and Public Affairs, Columbia University

Johanna Reynolds, York University, Toronto, Canada

Emrys Shoemaker, Caribou Digital

Yiannis Theodorou, GSMA

For UNHCR: Alexander Beck, Jean-Nicolas Beuze, Clève Brethneve Massamba, Michael Casasola, Claudine Nduwimana, Nicholas Oakeshott, Salam Shahin, Dimitris Thanos, Sara Tholozan

For the Government of Canada:
Paula Betuzzi (Global Affairs Canada)
Brad Adams-Barrie, André Belzile, Emmanuelle Deault-Bonin, Jean-Marc Gionet, Chris Gregory, David Léger St-Cyr, David Luchuk, Edwina O'Shea, Michelle Richardson, Karen Tso, Fraser Valentine (Immigration, Refugees and Citizenship Canada)
Tim Bouma, Manas Mehta (Treasury Board Secretariat)

* Institutional affiliation given for identification purposes only

UNHCR and Immigration, Refugees and Citizenship Canada were very grateful for the contributions received in the project, particularly those who made presentations at the online events.