

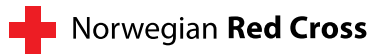
A photograph of a man sitting on a beach, wrapped in a red blanket. The blanket has a large white cross symbol on the back. The man is looking towards the right. The background shows a sandy beach and some rocks in the distance.

**DIGITAL IDENTITY:
ENABLING DIGNIFIED
ACCESS TO HUMANITARIAN
SERVICES IN MIGRATION**

JUNE 2021

ACKNOWLEDGEMENTS

Support for the production of this report from the following organizations is gratefully acknowledged:



This report was made possible by funding from the American Red Cross and Innovation Norway.

Thanks are also due to the author, Nadia Khoury, and all the interviewees for their contributions.

© International Federation of Red Cross and Red Crescent Societies, Geneva, 2021

Any part of this publication may be cited, copied, translated into other languages or adapted to meet local needs without prior permission from the International Federation of Red Cross and Red Crescent Societies, provided that the source is clearly stated.

Contact us:

Requests for commercial reproduction should be directed to the IFRC Secretariat:

Address: Chemin des Crêts 17, Petit-Saconnex, 1209 Geneva, Switzerland

Postal address: P.O. Box 303, 1211 Geneva 19, Switzerland

T +41 (0)22 730 42 22 | **F** +41 (0)22 730 42 00 | **E** secretariat@ifrc.org | **W** ifrc.org

*Cover photo: Canary Islands, 2006. No one knows how many migrants have died in the last ten years attempting to cross in small boats from Western Sahara, Mauritania and, most recently, Senegal to the Canary Islands. Spanish Red Cross assists those who succeed to reach the Canary Islands with emergency aid and clean and dry clothes.
Photo credit: Manuel Lérída/Spanish Red Cross*

CONTENTS

Executive Summary	3
1. Introduction	4
a. Background	5
b. Objectives of this report	6
c. Methodology	6
d. Terminology	7
2. Findings and Observations	8
a. Identity-related challenges to obtaining humanitarian services along migration routes	9
b. Defining digital identities in the context of migration	16
c. The promise of digital ID for migration	17
d. Risks and challenges	19
e. Ensuring inclusion for the most vulnerable migrants	25
3. Recommendations	30
4. Conclusion	35
5. Selected References	36
6. Appendices	39
Appendix I: Seven Key Questions Used In The Consultation	40
Appendix II: Literature Review	41
Appendix III: User Journeys	44
Appendix IV: User Personas	46
Appendix V: Initial Checklist Of Key Risks Or Issues	49

“

People take advantage when you are totally undocumented – you do not actually exist. If there is any disagreement, with your employer or with a traditional person, they can just kill you. Nothing will happen to them as you are just a body living there.

– Migrant in a European country.

”

*Edirne, Turkey, March 2020. Migrants seeking to protect themselves against the cold weather.
Photo credit: Erhan Idiz/Turkish Red Crescent*

EXECUTIVE SUMMARY

Digital identity systems are increasingly being used by humanitarian organizations attending to forcibly displaced migrants, though they may not always be recognised as such. With the aim of better understanding this trend, a global consultation with migration experts and key stakeholders in the humanitarian community explored the use cases, benefits and risks of digital identities, as well as the diversity of existing systems being used or under development.

The consultation and accompanying research identified several key findings. First, a broad range of humanitarian services are provided to vulnerable people on the move at each stage of their journeys, several of which are conditioned on a migrant sharing or proving their identity. This creates challenges in providing services to those who really need them, complicating access to humanitarian assistance. This finding also calls for reflection on the reasons for which identity data are collected and processed, and how this is balanced with the migrant's right to privacy and the overwhelming humanitarian objective of ensuring that the most vulnerable are assisted.

Second, there is no fully agreed definition of "digital identity" in the sector, creating an obstacle to a common vision and objectives on using the solution in migration activities. Nonetheless, there is a wide spectrum of digital identity solutions used in the context of migration, and potential for interoperable solutions. Third, providing a digital identity to vulnerable migrants to access services could be life-saving, as many do not have access to identity documents, and could empower migrants to better control their personal data. For humanitarian organizations, issuing digital identities could save time and funds, allowing them to focus more on the services being provided, facilitating access to services and, in avoiding constant collection of personal data, allow for a more dignified treatment of migrants. Yet, there are several risks and challenges to the use of digital identities, including data protection, privacy, investment, training and a lack of technical understanding of the solutions.

Finally, reflections are offered on the importance of ensuring an inclusive approach in developing and implementing a digital identity solution, recognising different individuals' varying levels of literacy (including digital literacy), access to information and access to digital means, and the impact of age and gender on these factors.

This report therefore recommends the following:

- Organizations should favour a long-term vision on digital identities, framed in guiding principles or a strategy to ensure internal and external accountability.
- Benefits and opportunities of digital identities, both for humanitarian organizations and migrants, must be fully explored and tested.
- Organizations seeking to use digital identities in their migration activities should follow a model of cooperation or consortia, identifying clear governance structures and incorporating relevant expertise in advisory and decision-making functions.
- Humanitarian organizations should advocate for greater engagement of migrants in developing digital identity solutions, as well as supporting national authorities to provide identity to the more than one billion people around the world who currently lack it.
- Building trust at all levels is crucial to the successful development and deployment of a digital identity solution in the migration scenario.
- Organizations should further advocate for data minimization in humanitarian action.
- The vulnerabilities of migrants should be carefully considered when piloting digital identity solutions.

1

Introduction



Vucjak, Bosnia and Herzegovina, August 2019. Migrants queue for food at Vucjak, a migrant reception site near the Croatian border where they were moved by local authorities. Photo credit: Victor Lacken/IFRC

a. Background

The International Federation of Red Cross and Red Crescent Societies (IFRC) is the secretariat, international coordinator and support provider for its 192 member National Red Cross and Red Crescent Societies, together forming the world's largest humanitarian network. Key missions of the IFRC are to save lives, protect livelihoods and strengthen recovery from disasters and crises around the world.

The IFRC's *Strategy 2030* focuses on five global challenges¹ to be addressed, one of which is "Migration and Identity". This seeks to ensure that all people who migrate and are displaced are safe, are treated humanely and with dignity, and have the support they need to thrive in inclusive societies. This will include expanding humanitarian support provided to migrants along their routes to ensure that their needs are addressed through essential services and protection irrespective of their legal status in both emergency and non-emergency contexts. The Migration and Identity challenge also recognises that migratory journeys are particularly difficult for stateless people and those who do not have identity documents.

At a global level, the UN Sustainable Development Goals (SDGs)² adopted in 2015 include Goal 16: "Promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels", and Target 16.9³ states, "By 2030, provide legal identity for all, including birth registration". The World Bank estimated in 2018 that just under one billion people worldwide lack an official proof of identity⁴, equivalent to roughly 13 per cent of the global population. The World Bank also identified 161 countries that have ID systems that use digital technologies, equivalent to 83 per cent of the countries in the world.

The Dignified Identities for Cash assistance project⁵ (DIGID) was launched in January 2019 under the governance of a consortium composed of the Norwegian Red Cross, Norwegian Refugee Council, Norwegian Church Aid, and Save the Children Norway. The IFRC, in partnership with the Norwegian Red Cross, has been leading the technical implementation of the DIGID project, which seeks to address the challenges of providing cash assistance to people who do not possess official identity documents. At the time of writing, the DIGID project is currently piloting a digital identity solution focussed on cash assistance in Kenya.

A second phase of DIGID is being launched in 2021 (DIGID2)⁶, focusing on the needs of vulnerable migrants to receive a wide range of essential services in a dignified manner, as displacement causes particular challenges related to identity. It was estimated by UNHCR that some 80 million people globally were forcibly displaced⁷ as of mid-2020, equivalent to 1 in every 100 people in the world, with approximately 40 per cent of those being minors of age. The project aims to investigate how different humanitarian actors can recognize the same set of digital credentials so that migrants may access more informed and better tailored essential services along their route, even in the absence of official identity documents.

1. <https://solferinoacademy.com/why-strategy-2030/s2030-the-five-global-challenges/>

2. <https://sdgs.un.org/goals/goal16>.

3. <https://indicators.report/targets/16-9/>

4. World Bank Identification for Development; still used as the current estimate: <https://id4d.worldbank.org/global-dataset/visualization>.

5. Dignified Identities for Cash Assistance (DIGID): <https://hiplatform.org/digid>

6. <https://www.innovasjon Norge.no/no/subsites/hipnorway/innovation-projects2/dignified-identities-in-cash-programming-ii-digid-ii/>

7. UNHCR Refugee Population Statistics Database: <https://www.unhcr.org/refugee-statistics/>

b. Objectives of this report

This document is the final report of a consultation and research commissioned by the IFRC with the support of the DIGID consortium. The primary objective of the report is to inform humanitarian organizations working with migrants of the opportunities and risks in the use of digital identities in providing services throughout the migrants' journeys. There is growing interest in this topic and this report aims to help humanitarian organizations better understand concepts and technologies related to digital identities in migration, as well as their value to the organization and people they attend to, so they can make informed decisions on exploring or investing in such solutions. This report is also intended to help the IFRC shape a position or strategy for using digital identity solutions particularly for vulnerable migrants.

Additionally, the findings in this report aims to guide the DIGID2 project team to assess, scope, plan and implement the project, as well as to provide some orientation for the subsequent user-centric consultation and design process to ensure appropriate engagement with affected communities.

c. Methodology

The methods used to complete this report were:

- (i) Literature review: Desk-based document review and non-exhaustive analysis of existing literature on the use of digital identities, with a particular focus on their use in providing humanitarian assistance to migrants and identifying potential case studies (see Appendix II).
- (ii) Development of user journeys and user personas, to highlight the services received along migration routes and where identification (ID) is used and becomes an issue. This also supports analysis of the pain points from a migrant's standpoint and potential motivations for having a digital ID.
- (iii) Expert interviews: Key informant interviews and focus group discussions were carried out through virtual meetings with a wide range of stakeholders. Seven key questions listed in Appendix I were used to prepare for the interviews.
- (iv) Migrant interviews: although consultation with migrants was beyond the scope of this study as it is planned for a follow-up consultation, informal conversations with migrants were facilitated by two National Societies, providing another perspective to complement the discussions with experts. It is recognized that this was a limited instance of end-user consultation and was not representative of the variety of forcibly displaced migrants or migration scenarios around the world.

The consultation was carried out remotely, between 1 February 2021 and 31 March 2021. In total, 80 individuals from 27 organizations, including 10 national humanitarian organizations and 10 humanitarian organizations with an international presence were consulted. Stakeholders interviewed included research institutions, donors, components of the International Red Cross and Red Crescent Movement (including the Global Migration Task Force), humanitarian partners, United Nations agencies, private sector service providers, and end users where possible, to integrate migrant voices. A broad range of informants were sought to cover the spectrum of contexts, global migration scenarios and humanitarian services provided, while efforts were made to seek views from headquarters and field implementers.

Interviews were conducted in English, French or Spanish, depending on the working language of the interviewees, using Microsoft Teams as the communications platform. Detailed written notes were taken as the interviews progressed. Participants were informed that the interviews would be treated as confidential and that all personally identifiable information would be anonymized. As such, the research findings do not identify specific individuals, organizations or locations, other than where those relate to the published literature review.

Despite the desire to do so, it was not possible to include local community-based organizations⁸ in the consultation due to time and access constraints, and it is recommended that they be included in future consultations.

d. Terminology

To ensure a common understanding with stakeholders, the following definitions were used where possible during the consultation:

- Digital identity: “a collection of electronically captured and stored identity attributes that uniquely describe a person within a given context and are used for electronic transactions”⁹.
- Self-sovereign identity: “a term used to describe the digital movement that recognizes an individual should own and control their identity without the intervening administrative authorities”¹⁰.
- Foundational identity: Provides a legal identity to a broad population as a public good without specifying a specific service. It allows individuals to prove who they are. Generates a legal identity that can be referenced by others. It is typically government-based and covers the whole population of a country (for example, a passport or a social security number).
- Functional identity¹¹: Enables a specific service (function) to authenticate participants. Every individual can have multiple functional identities (for example, a student ID or a voter number).
- Digital guardianship¹²: a digital guardian is a person or organization who administers identity data or wallets on behalf of a digital dependant, including sharing proof of the dependant's digital credentials where required for verification. Digital guardianship is the relationship between the digital guardian and the digital dependant.

8 While National Red Cross and Red Crescent Societies are organizations with a community presence, relying on their networks of branches and volunteers, they are nation-wide organizations. References to local community based organizations here are rather to organizations that do not have a national reach, and operate on a departmental, municipality or community basis, having their leadership bases built from the communities in which they operate.

9 International Committee of the Red Cross and Brussels Privacy Hub, [Handbook on Data Protection in humanitarian action](#), 2020, p. 207, referring to World Bank Group, GSMA and Secure Identity Alliance, Digital Identity: [Towards Shared Principles for Public and Private Sector Cooperation](#), World Bank Group, GSMA and Secure Identity Alliance, 2016, p. 11.

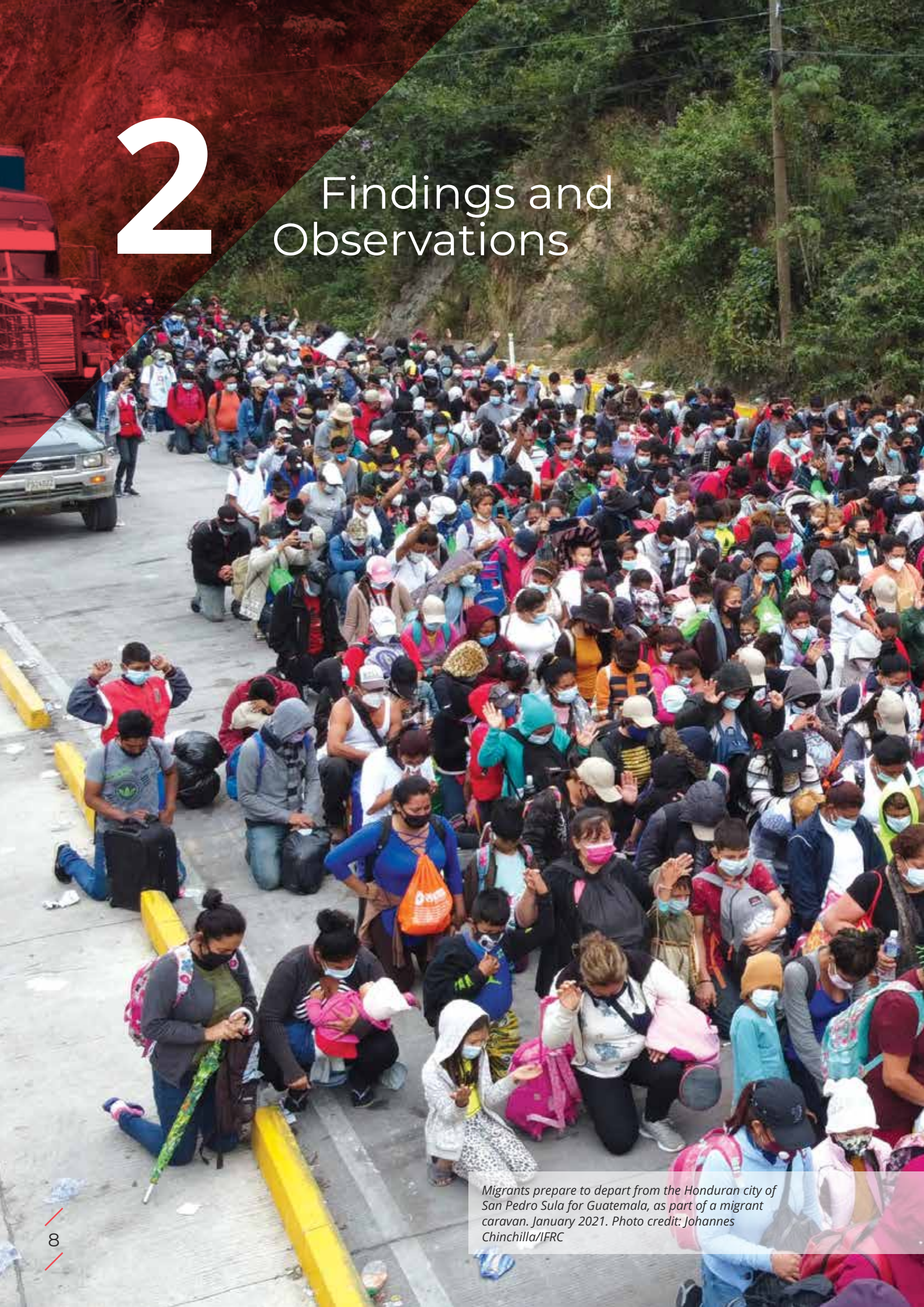
10 Sovrin: <https://sovrin.org/faq/what-is-self-sovereign-identity/>.

11 Elements of the definition of foundational and functional identities were taken from International Committee of the Red Cross and Brussels Privacy Hub, [Handbook on Data Protection in humanitarian action](#), 2020, p. 207.

12 A definition for a digital guardian has been derived from the natural meaning of a guardian as a person or institution who is protecting another person and possibly their property. See Sovrin, [Whitepaper on Guardianship and Self-Sovereign Identity](#), December 2019.

2

Findings and Observations



Migrants prepare to depart from the Honduran city of San Pedro Sula for Guatemala, as part of a migrant caravan. January 2021. Photo credit: Johannes Chinchilla/IFRC

This section outlines the key findings and observations gathered from the consultation with migration experts and key stakeholders, including migrants.

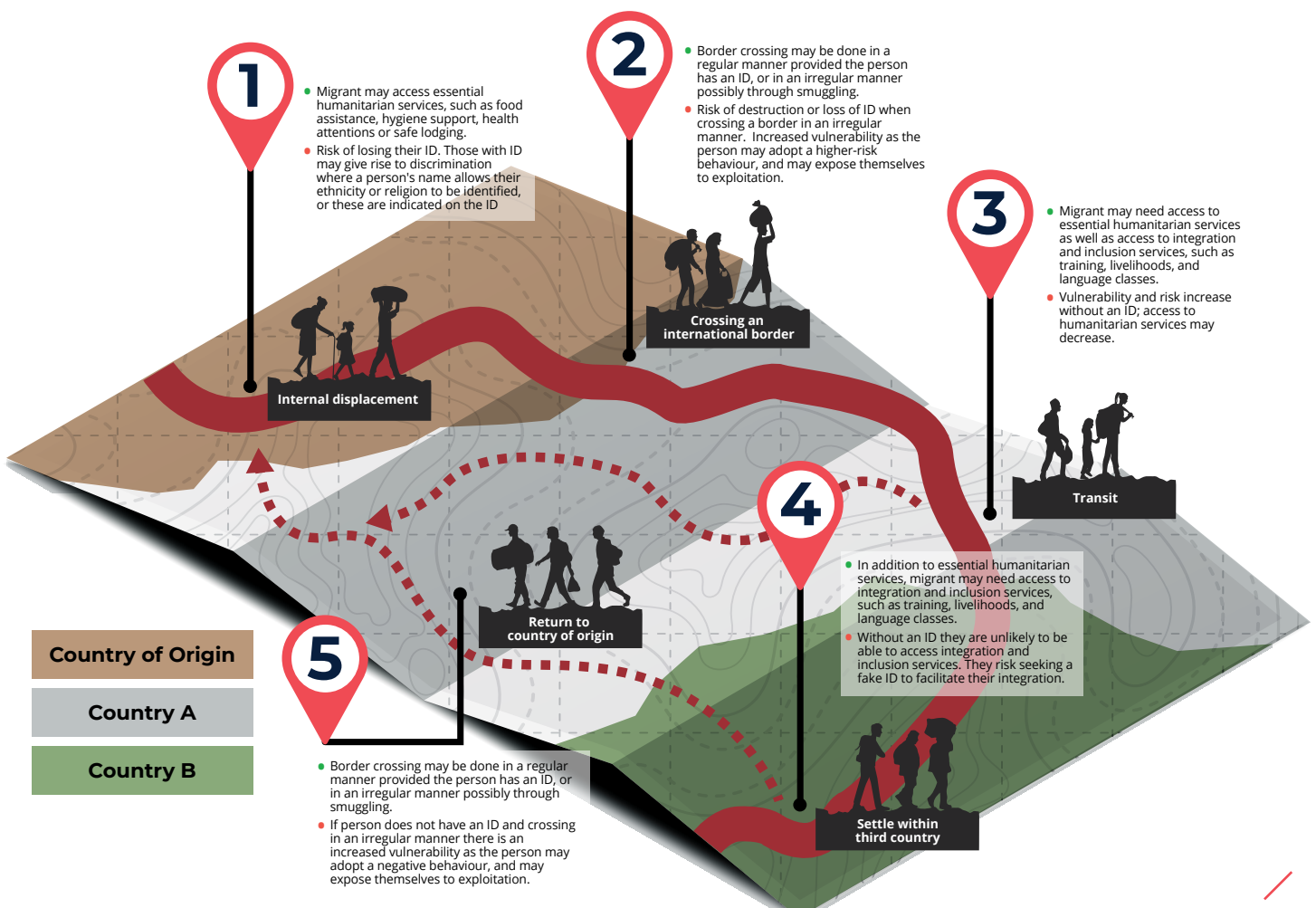
a. Identity-related challenges to obtaining humanitarian services along migration routes

All individuals have an identity, though not all individuals are able to prove their identity, and some may not wish their identity to be known. Yet, access to identity documents is intricately related to the ability to migrate and access to humanitarian services.

Based on the consultation, user journeys and migrant personas were developed to illustrate migrants' needs for identity in obtaining humanitarian services, and inform the eventual solution design, enabling a more user-centric approach (see Appendices III and IV for further details).

Two user journeys were designed to map the manner in which a migrant may migrate and access humanitarian assistance, and identify their interactions with identity, as well as the related risks or pain points. Figure 1 provides a simplified version of the first user journey, showing the migration path from the home country to a third country and the return to the home country. While migrating without identity documents is possible, it increases the risk to which the migrant is exposed as they seek to cross borders without formal identification and increases the vulnerability of the migrant as they find themselves in a country as an irregular migrant. Not having identification may also restrict the type of services which they may obtain along their journey, as identity tends to be requested (if not always needed) to obtain humanitarian assistance at different migratory stages.

Figure 1: Simplified user journey showing the migratory path and highlighting identity-related risks



Four user personas were also developed, incorporating migrant’s contexts, their personal profile, their vulnerabilities and complaints, their current motivations and core needs, and their perceived pain points related to identity issues. The four user personas are spread across different continents and represent people at different stages in their migration journey: an asylum seeker, a migrant in transit through a third country, a migrant returning to their country of origin and an internally displaced person. Figure 2 summarizes the four user personas.

Figure 2: Simplified version of four user personas, highlighting their needs and pain points relating to identity.

				
Persona/ Context	Internally displaced person following a natural disaster in Central Africa	Asylum seeker waiting for outcome of application in a European country	Unaccompanied minor transiting through informal border crossings in Latin America	Migrant returning to country of origin following a period of conflict, currently in transit country in East Asia
Identity issues	Never had an official ID	Lost official ID during journey; difficulty in receiving certain aid because unable to prove identity	Unaccompanied minor transiting through informal border crossings in Latin America	No clear view on how to access voluntary repatriation without an official ID from home country
Core Needs	Needs basic assistance for survival and healthcare for his unwell father	Needs basic assistance, need to pay debts and save funds to travel for better work opportunities	Needs basic assistance & contact with family members	Needs basic assistance including cash to facilitate his travel & contact with family in home country

*basic assistance includes food, water, shelter, and health services.

Despite the differences in their journeys, all user personas face identity-related challenges in accessing humanitarian services, these being more acute in the case of international migrants.

These issues are further explored below.

Humanitarian services provided to migrants and identity requirements

The consultation confirmed that a broad range of humanitarian services are provided to people on the move, at all different stages of their journeys, with many of those not requiring identity to be provided or registered. In the end-user consultation interviews, several migrants highlighted that they had not received any humanitarian services along their route, either because they had travelled with smugglers who kept them away from aid organizations, or because they were travelling with other single men and were therefore not considered to be a vulnerable target group.

Emergency services or what have been called “bulk services” can generally be provided without the need to share ID. These can include life-saving emergency health services, first aid, psychosocial support, emergency shelter, food or hygiene parcels, clothing, access to community soup kitchens or certain emergency protection services, safe water, access to showers and toilets, internet access, transport to certain facilities, post-exposure prophylaxis in case of abuse, counselling services or psychiatric support, safe spaces and family links restoration.

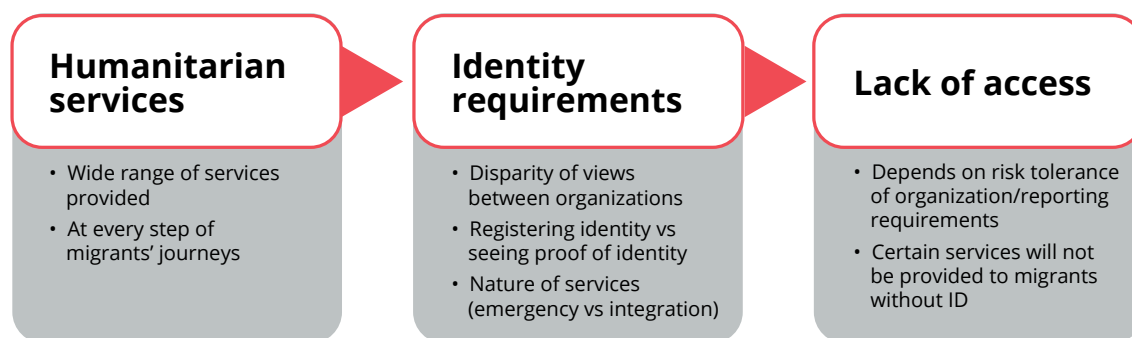
Access to certain services do usually require registration of the person, although verification of the person’s identity is not done, for example many health services, protection services (including protection from sexual and gender-based violence (SGBV)) or tracing services.

Services which are more orientated towards integration usually require provision of ID, including verification of the person's identity. These would include recurring cash transfers¹³, rental support livelihood activities, language and training courses, attending to former child soldiers, skills building, financial inclusion through microcredits, or access to legal assistance, for example for housing and land rights (lawyers will usually verify the migrant's identity rather than the referring organization).

In some cases, for cash transfers, an undocumented person can appoint a delegate who can represent them and act on their behalf to collect the assistance. When the person registers, they would need to be accompanied by their delegate, and the information on both persons is collected to physically authenticate them. At the time of obtaining the cash transfer, the delegate collects it using their own identity documentation, on behalf of the undocumented person. This solution tends to depend on the context and vulnerability of that person – they may be elderly or disabled, or a child-headed household. Alternatively, some financial service providers have accepted cards issued by a humanitarian organization, instead of formal identity, where these cards confirm the person's name and surname, and include a photograph or a signature.

These situations depend entirely on the country context, as certain national authorities may be more or less strict in terms of requiring migrants to register with the migration authorities, and in terms of monitoring compliance by humanitarian organizations. Figure 3 below illustrates the relationship between the availability of humanitarian services, identity requirements and access to humanitarian services.

Figure 3: Relationship between availability of humanitarian services, identity requirements and access to humanitarian services.



What data is collected?

The following elements of information are commonly asked of migrants when they receive services from humanitarian organizations. No key informant collects all of the elements below, and data collection is context specific. Yet each of these data is usually required by at least one of the organizations interviewed:

- name
- surname
- passport or ID number (or asylum registration number)
- date of birth
- age
- gender
- number of dependants
- marital status
- family demographics
- nationality
- ethnicity
- whether they have any disability
- legal status
- address
- contact telephone number
- e-mail address.

¹³ It is noted that although cash transfer is a modality which is used in emergencies as well as for stabilization and integration activities, electronic cash transfers are unlikely to be used in the context of people on the move, unless they are remaining settled for a number of weeks or months.

It was also noted that ample data is collected not just from migrants whom organizations serve, but also from meeting attendees. The documentation which includes this information serves as evidence that a given meeting did in fact take place for reporting purposes, and to support any expenditure such as refreshments for meeting participants.

One organization that provides a wide range of access to humanitarian services, including cash transfers, confirmed that they do not collect names or ID numbers of migrants, and rather information such as their gender and age to inform reports. Instead, they issue a card which provides a unique identifier to the person. Yet, some token-based systems that do not collect or verify name details leave open the potential that someone may register twice under a different name and be treated as if they were two different people. This also limits ID recovery when a person loses their identifier. Another organization explained that in sensitive contexts, they only collect the migrant's age within a range, gender, nationality and any specific vulnerabilities (such as a woman being pregnant or a child being unaccompanied), which allows them to report on key indicators. In some cases, a unique identifier is issued, not to be shared with the migrant, but rather to share with donors and to respond to partner/donor requirements. Organizations use this to ensure that there is no leakage of aid, or "double-dipping", and it is shared with donors as supporting documentation to financial reports.

A case management tool for SGBV events does not record names. Each person receives a survivor ID, which is created with numbers and letters based on some of the survivor's personal information. It could be based on the number of siblings they have, their mother's name and other such details. The code will always consist of the same stable questions so the survivor can recall their ID. The users are also informed that the survivor ID is used instead of their name, so their name is not kept in the database, a key factor to maintaining their privacy.

Certain organizations' processes do not allow for digital information to be collected from the field, thereby obliging implementers to create a double register: one paper-based register as the information is taken, and a second register as the information then needs to be digitized. This creates additional data protection risk since the information exists in two forms, both of which needs to be appropriately processed and stored.

Migrants unable to access services due to lack of identity

Out of the 16 organizations consulted and represented by field implementers, 10 of the organizations interviewed (equivalent to 62 per cent) said that they had been unable to offer services to a migrant due to their not having ID. However, all 16 organizations confirmed that they are able to provide emergency humanitarian services to a migrant without ID, due to the urgent nature of their needs. This demonstrates that migrants are unable to access certain services due to a lack of identification.

Provision of informed consent

Out of the 16 organizations consulted and represented by field implementers, 14 of the organizations interviewed (equivalent to 82 per cent) said that they ask migrants to sign a consent form to register the migrant's consent to share their data, or record consent electronically through a tick-box in a form after explanations are given. In the case of minors, their parents will be responsible, or a trustee can be appointed. Note that in some countries, the age of consent to use digital services may be as low as 13¹⁴. It may be the case that humanitarian organizations use a signed consent form to evidence informed consent for longer-term assistance, such as regular cash transfers or livelihoods, as opposed to one-off services such as the distribution of food aid or hygiene aid. In the case of the two organizations interviewed which do not use signed consent form, they confirmed that they do

14 Article 8(2) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (commonly known as the General Data Protection Regulation, or GDPR) provides that children may consent to the processing of their personal data as of 16 years of age for digital services, while member states are able to provide for a lower age for these purposes, provided this is not below 13 years of age. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>

explain to migrants how their data will be registered, used and stored, and that consent is implied when the migrants choose to proceed with the humanitarian assistance.

An organization which uses iris scans to provide a digital health file to refugees had to carry out quite an iterative process to obtain informed consent, ensuring that sophisticated technical language was sufficiently simplified so that it would be understandable. They shared that the informed consent process, which now includes visuals, would take approximately 15 to 20 minutes. Although this seeks to ensure that refugees understand the process properly, it could be viewed as overly time-consuming and imposing an important time commitment on refugees with urgent health needs.

“

We explain that the information is confidential, that the data will not be shared, and that the person can decide not to share the information. The image of the organization matters a lot – the majority of the migrants know us.

– Field implementer in a migration response from a humanitarian organization.

”

An added complexity when considering consent for digital ID is that the digital ID could exist forever and could be shared with an infinite number of entities. As such, it is particularly important that migrants understand how the data will be stored and used, and with whom it will be shared. Owing to concerns about the (mis)use of data, it is also crucial for migrants to be able to request that their personal data be deleted from an organization’s registers, at any time, and for organizations to respect those wishes, anonymising data where necessary to maintain a register.

“

I asked [the organization] to delete my information from the database, and it has not happened. I did not receive any reason about why they cannot delete it.

– Migrant in a European country.

”

Migrants’ understandings and concerns about identity.

The consultation highlighted that a majority of migrants understand that their identity can provide them with access to benefits or can cause them difficulties. Out of 16 organizations consulted and represented by field implementers, eight of the organizations interviewed (equivalent to 50 per cent) said that they had attended to migrants who had refused to share their identity with the humanitarian organization. In general, migrants who have fled due to political or social discrimination are particularly concerned about sharing their data and having the authorities of their home countries obtain them. Ethnicity, which can often be determined based on someone’s name, and the consequent threat of persecution, may also often be a reason for a migrant not to share their identity, especially in a conflict setting. A migrant’s country of origin may often affect their chances of a positive outcome for their asylum applications, depending on the country of application, so migrants may choose not to disclose their real country of origin. Finally, migrants in an irregular situation will be less likely to wish to share their information, due to fears that they may be identified and deported.

“

I felt no one cared for me because I did not have documents.

– Migrant in a European country.

”

Some people may provide an incorrect age, because they think they may get a better or worse service as a child. Being a minor can mean that the migrant will avoid detention as an adult, or that accommodation options will be opened to them due to their young age. In other contexts, being an

adult may result in obtaining documents (such as a deportation order) which allows them to continue their travel through a transit country, whereas being a minor will not allow them to access such documentation, and they might instead be placed in protective custody. Additionally, certain migrants may not know their age or their date of birth, if their cultural traditions rather link their birth to a season or a particular episode, or simply do not register their birth with anything more than a year.



In many countries..., the impact of age is class dependent... many minors have to go and work, regardless of their age. But in Europe, being a minor takes on a completely different meaning... Age can be a barrier that works exclusively or inclusively.

–Migration expert from a humanitarian organization.



Various informants also noted the difficulty faced in transcribing migrants' names, depending on the language of origin, leading to spelling mistakes or diverse ways of writing the same name. In some contexts, names do not easily transliterate to the working language of the registering organizations and can have diverse spellings when transliterated. As such, recording the person's name does not guarantee that the person can be readily identified in the future, where there is a risk of it being incorrectly transliterated.

Why is this data collected?

Migrants' personal data is usually collected for accountability purposes, whether required by their partners and donors or internal to the humanitarian organization (though this in turn may stem from donor or partner requirements, or financial accountability mechanisms). Organizations rightly wish to ensure that they are providing humanitarian assistance to the people who have been identified to receive it, based on vulnerability criteria, and a verification of the person's identity will need to be carried out when the humanitarian assistance is provided at a later date. Organizations also wish to ensure that they are avoiding end-user fraud. One key informant shared that their organization is providing a wide range of services, so they need to know what services each migrant has received in order to report on them and to prevent duplication of services. They framed it as required resource management, to ensure that the appropriate resources go to the appropriate need, and ultimately ensure that often limited resources be distributed properly. One organization explained that they collect migrants' addresses as their place of residence may determine whether the organization can attend to them or whether a different organization should be responsible (relating back to donor requirements).

Many informants noted that data collection standards for in-kind services, such as providing a food or hygiene kit, are usually a lot lower than for provision of cash transfers. It was highlighted that all but exceptional cases of cash transfers require identification information, even if the value of the cash transfer is lower than the cost of a hygiene kit. This is mostly due to requirements from financial service providers which are subject to financial regulations, and also due to organizations' internal requirements on providing cash to migrants. In the case of restoring family links and family reunification activities, which are typically carried out by National Red Cross and Red Crescent Societies, the type of data that is collected is entirely personal due to the nature of the service: personal details will usually be needed to reconnect two family members.

Finally, certain donors may require a high level of verification on people served by humanitarian organizations or impose on the humanitarian organization onerous contractual clauses regarding any loss or fraud of the humanitarian aid. Some key informants mentioned that certain donors require them to carry out checks on the people they attend, mostly due to counter-terrorism vetting. Humanitarian organizations therefore place more emphasis on verification of migrants' identities to ensure there is no duplication, rather than consider the impact from an operational perspective, although the real value of any end-user or downstream leakage may be a small fraction of the total donation¹⁵, and significantly less valuable than potential instances of fraud carried out upstream in

15 The Engine Room and Oxfam: "[Biometrics in the Humanitarian Sector](#)", March 2018.

the supply chain. Finally, as noted by a migration expert, registering an individual is unrelated to the quality or relevance of the service that they receive.

Additional questioning should take place on the need to collect migrants' personal data, its impact on the success of the activities, and the extent to which it is needed to measure that success (meeting indicators and reporting to the donor). There is an important balancing act to be carried out, weighing the risk of "double-dipping", and value for money for the donor, against an individual's right to privacy and the potential risks to that person should the confidential data be accessed. Figure 4 illustrates this balancing act.

“

Just registering the person does not show that we have given them a good service.

– Migration expert from a humanitarian organization.”

”

Figure 4: Competing considerations regarding data collection on migrants receiving humanitarian assistance.



Can migrants access this data?

Generally, migrants are not able to see the information regarding the services they have received. In some cases, they are able to call the organization's helpline to obtain the information or ask for a copy of the information they have filed. One organization shared that they are looking to set up an online platform for beneficiaries to access information about the services they are receiving. Many organizations mentioned that migrants never asked for the information, while one migrant emphasized that there is little awareness among the refugee population about the possibility of requesting that sort of information, hinting at the power imbalance between the attending organization and the migrant.

“

When I arrived in [Country X], I did not see any organisation providing any type of consent form to the refugees and asking them whether they can use their information... No one would ask what is being done with the information, we did not know about data privacy, data protection, confidentiality and no one told us what will be done with the information. People shared their concern about the lack of information... As refugees, they do not know their rights, whether they can have a copy of this information or not. They just know that they need to provide the information to obtain the service.

– Migrant in a European country.”

”

b. Defining digital identities in the context of migration



Identity is such a loaded word.

– Migration expert from a humanitarian organization.

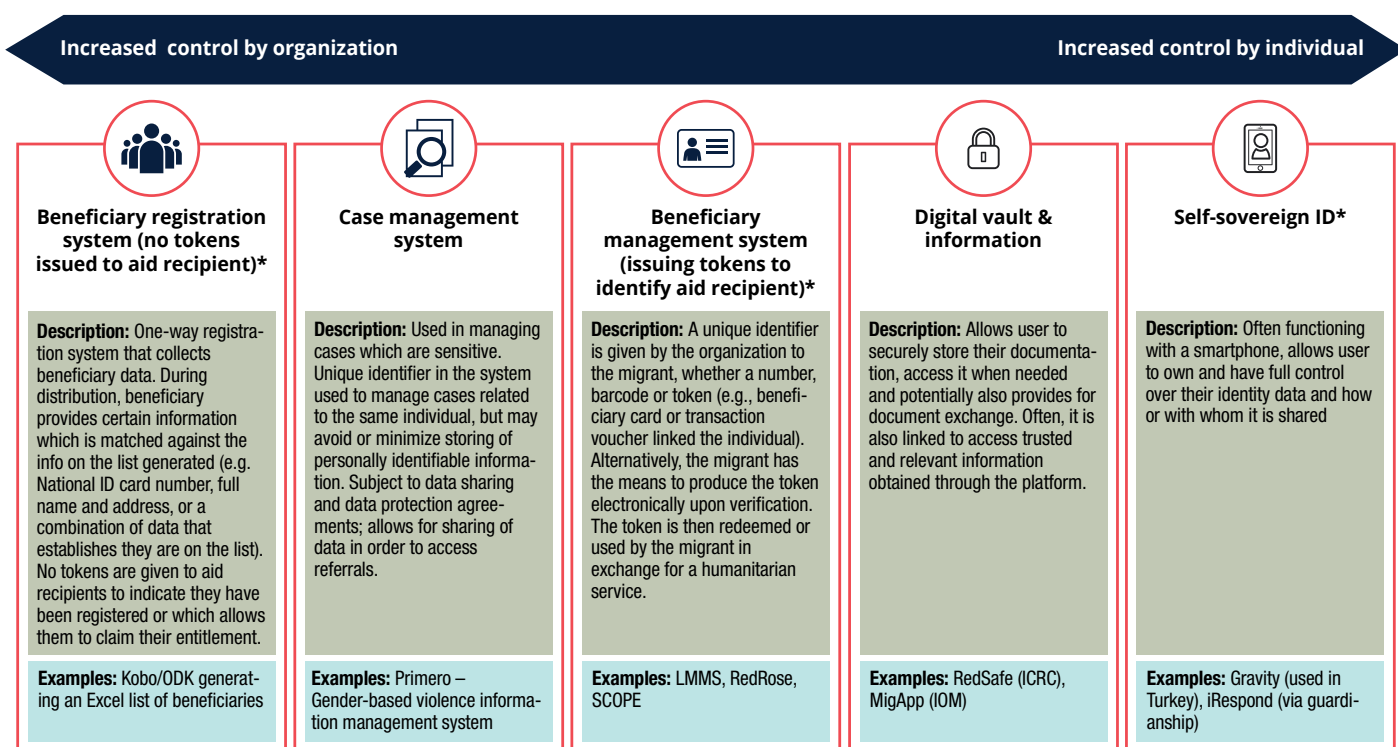


In the context of this consultation, a definition of digital identity was shared with each key informant and participant in focus group discussions, and the term was not the subject of debate in the sessions. Yet the term has different meanings to different people, depending on their exposure to the concept in practice. This creates further challenges to the

aim of interoperability, understood broadly as the capacity for communication and data exchange between solutions: it is harder to connect solutions when their definitions, let alone the objective they seek to achieve, are not aligned between key actors, and they may not be recognised or accepted as such.

The concept can also cause some confusion, as there are several digital identification solutions in the migration sector which vary in their functionality. Figure 5 illustrates an attempt to map out the different digital systems in which identity is used, as encountered in the consultation, as well as some of the key aspects of each type of solution.

Figure 5: Spectrum of digital systems in which identity is used, organised by degree of control by end-users.



*Use of biometrics may be possible with these systems

The spectrum ranges from a system offering greater control over data to the humanitarian organization, with less control to the end user, to a system that offers less control to the humanitarian organization and more control to the end user over their own data.

Digital identities and collection of data are interlinked (some form of data will always be required to create a digital identity) and the overall desire is to enable people to own and control their own data, which is assumed to increase their autonomy and dignity – whether they are people in need or not. Yet in practice, humanitarian organizations have predominantly developed systems that focus on their own need for data and have done so mostly in an independent and divided manner.

The consultation explored the possibility that existing systems could be used to provide the end user migrant with greater access to or control over their own information, moving closer to the self sovereign identity (SSI) end of the spectrum. Most data management systems can give a person access through a name and user profile and give restricted rights, meaning that it would be possible to provide migrants with some log-in details whereby they can access their files. In the case of survivors of gender-based violence or of other kinds of violence, this raises concerns that a partner or a community member may exert some duress on the survivor to access and read what is in the file, or in conflict situations, armed actors may force the migrant to access the information. In such scenarios, individuals could be exposed to retribution and potential harm. Limiting this access to being on-site with the humanitarian organization could mitigate this risk, though it would also limit the migrant's ability to access and use their information. Sensitive information could be ring fenced so that it is not accessed by the migrant directly, and they may not have any need for this information (for example, the circumstances of an attack). Greater digital access can also mean that access to the information becomes more difficult to control.

Various informants indicated that an SSI solution requires a high baseline of literacy and digital literacy as it requires a person to make calculated considerations. It is suggested to appoint a digital guardian to address the challenge of inclusivity, and this can be useful in certain contexts, albeit with certain risks which have been identified by the SSI industry. However, in the context of people on the move, this raises concerns about how digital guardianship will be applied when the person moves from country to country.

A first option would be to transfer guardianship from the original entity acting as a guardian to another humanitarian organization across the border, who would then attend to the migrant. Challenges would emerge if the original entity does not have a partner organization in the other country: a different organization would have different infrastructure, capacities, and perhaps no understanding of the digital SSI nor of the principle of guardianship. In addition, the migrant providing their consent to the original guardian would need to understand that in doing so, they would be projecting several layers of trust towards their possibly multiple unknown future guardians, which would certainly be a stretch.

A second option to address guardianship for people on the move is that the original guardian remains the migrant's guardian forever. That original guardian was responsible for obtaining consent in the first place, so should remain responsible to the migrant until they become digitally independent. Where a migrant is travelling across one or various borders, this again raises a challenge for practical application: how would this guardianship work when the guardian does not have a presence in other countries? How could the migrant contact their guardian so that their ID can be used to obtain a humanitarian service? There remain various unanswered questions regarding the application of SSI to migrants who are on the move, yet to be explored through implementation. While pilot projects in the migration context are ongoing, this led one interviewee to doubt that SSI could be of use for remote or last-mile populations.

c. The promise of digital ID for migration

An estimated 1 billion people in the world, some 13 per cent of the global population, do not have identity documents¹⁶. These are likely to be the most vulnerable populations, both as a result of not having identity documents, and also because their lack of documentation is due to underlying access or socio economic issues. Although the issuing of foundational identity should be the main priority, these are usually issued by nation states, and humanitarian organizations (with one exception)



I am fearful, with an SSI solution, that the solution is looking for a use case, rather than being developed for last mile populations.

- Digital identity expert from a humanitarian organization.



16 The World Bank, ID4D data: <https://id4d.worldbank.org/global-dataset>.

are not mandated to provide such IDs. Yet, to help bridge this gap, humanitarian organizations could issue functional identities limited to accessing services within the humanitarian sector. At a minimum, this would provide vulnerable migrants with a functional identity to access certain services and could be life-saving in those cases.

i. Benefits to end users

Although the reviewed literature does not focus much on the benefits of digital identity for end users, various positive aspects were highlighted during the consultation. For migrants, using a digital identity would facilitate their access to services in many ways, especially those that require some form of identity to be provided. Having a digital identity, which they could ideally manage and control, is assumed to support restoration of dignity. Depending on the solution, migrants may also be able to store and access documentation to obtain more sophisticated services, such as livelihood opportunities based on their digital credentials. A digital identity solution could help maintain privacy, particularly for those migrants who do not wish their journeys to be tracked. Finally, using digital ID would avoid the repetition of the registration process with different organizations operating along migrants' routes.

“

This is a protection issue of access to important documentation to open doors and obtain access to services.

– Country Director from a humanitarian organization.

”

“

A digital ID would be useful. I have a photocopy of all my medical documents and also have all my medical history on my mobile phone. It would be really helpful for a lot of people who would be scared to lose a document.

– Migrant in a European country.

”

“

A survivor [of SGBV] may find it easier that [the humanitarian organization] could share the confidential information with a service provider, without herself having to share all that traumatic information again.

– Sexual and Gender Based Violence (SGBV) expert from a humanitarian organization.

”

Beyond the time-saving aspect and practical easing of access to services, digital IDs could enable improved continuity of services, storage of crucial information and potentially tailored services should the end-user be more proactively able to use their data. This could lead to services that better meet needs.

Finally, in the case of people in need of protection, it was felt that such a process would spare them the potential trauma associated with registration processes, in which they may need to repeat a difficult story on several occasions.

ii. Benefits to humanitarian organizations

Digital identities offer many opportunities in the humanitarian field, since many organizations need the same data about beneficiaries. Beneficiary registration systems promote the cost benefits of their solutions, especially when used by a variety of humanitarian agencies¹⁷. A more fluid process to identify migrants being attended would be an important time saver for staff and volunteers, thereby allowing them to more promptly attend to the person in need and focus more on the quality of the service provision, rather than registering the person. Greater efficiency in processes would lead to improved timeliness in providing assistance, better services, more effectiveness in operations and, potentially, better resource management.

¹⁷ See for example World Vision's Last Mile Mobile Solutions (LMMS) reporting reductions in activity time and staff count: <https://www.wvi.org/disaster-management/last-mile-mobile-solution-lmms>. See also the Kenya Red Cross reporting time savings due to beneficiary identification through QR code scanning or biometrics, using the RedRose solution: <https://cash-hub.org/wp-content/uploads/sites/3/2020/10/Building-Back-Safer-Houses-ICHA-No-7.pdf>.

In particular, in an emergency situation, it would greatly facilitate the flow of access to services and allow greater complementarity of services in allowing a rapid identification of services already provided and supporting those in need with additional services. Finally, a sophisticated solution may avoid the need to constantly collect sometimes sensitive personal data, allowing for more dignified treatment of people in need.

To fully reap these benefits, close cooperation, scale, acceptance of solutions and/or interoperability between different solutions are needed. While organizations will likely continue to develop solutions best adapted to their own identified needs, a collaborative approach in development and scale-up, as well as a recognition of other solutions, will help to ensure that common systems can be used, or separate systems linked. One key informant suggested having a digital ID accepted within the International Red Cross and Red Crescent Movement, particularly where migrants may move across borders and receive assistance from different National Red Cross or Red Crescent Societies. This research has identified certain good examples of common systems, although the potential scale-up of those solutions beyond their organization-centred functions, or a specific sector, has yet to be explored.

d. Risks and challenges

While the use of digital identities could have valuable benefits for both humanitarian organizations and vulnerable people on the move, several risks and challenges were also identified in the consultation and research processes. These are outlined below.

i. Risks and challenges for end users

Informed consent

There is growing concern that informed consent is neither really consensual, nor properly informed, particularly in the case of digital identities, creating a risk of misunderstanding or lack of knowledge on behalf of the end user. When in need of humanitarian assistance, migrants' priorities are those needs, be they nutrition, hydration, shelter, protection or health, and they may thus provide as much information as is asked of them, their focus being on more urgent matters. They are likely not enthused by having to read and sign paperwork and in some cases having to self-register, prior to their needs being attended.

Migrants are also aware that there are also often repercussions for someone who does not provide their consent, and that they may be removed from a particular target group, thereafter not being able to receive the aid in question. As one migrant shared (quoted above), migrants just know that they need to share their data to receive a humanitarian service. Signing a consent form may therefore be less of a consensual matter, than one reflecting the imbalances between the attending organization and the migrant.

Consent may also not be fully informed when explanations are incomplete or when data are used and processed digitally; it is possible that migrants and the people attending them may not properly understand the practical implications of data processing, or indeed the risks to the data. There is a concern that migrants may not understand the potentially complex technology involved in the creation and use of a digital ID. For example, how would one explain what cloud storage is to a migrant with little previous exposure to technology and the internet? In addition, the technology, as well as the rules and regulations governing it, will continue to develop and evolve, such that the data could be used in ways that are not initially desirable or understood.

“

Collecting all this information before assisting a migrant is counter-intuitive to the humanitarian principles; asking for ID may mean that the most vulnerable would not be attended.

– Humanitarian expert, think-tank.

”

Certain organizations are favouring alternative legal bases, such as the public interest, the legitimate interest or the vital interest in delivering humanitarian assistance, understanding that informed consent may not work in an emergency context due to the dire need to obtain assistance. Vulnerable people under shock and with great needs may not be able to understand what is being asked of them, especially if it relates to new technology. Nonetheless, organizations should still provide the relevant information notices, and allow migrants to ask questions and object. Yet, in the case of digital IDs, it is even more likely that migrants, especially those who may not have a high level of technological literacy, will not fully understand and ultimately may not agree with such notices, creating an important risk for migrants.

Unauthorized access

One of the greatest risks for migrants in the use of a digital ID is the unauthorised access to the digital ID or all or part of a migrant's digital credentials. It has unfortunately become common for hackers to gain unauthorised access to digital identities of banks and service providers. ENISA, the European Union Agency for Cybersecurity, reported that between January 2019 and April 2020, there were 3,800 publicly disclosed cases of identity theft, in great part due to data breaches, with 4.1 billion records exposed¹⁸.

Similarly, digital IDs could be hacked or accessed remotely in an unauthorised manner. In the case of migrants, access to and use of their digital data could greatly affect their safety. First, geo-localized data may reveal migrants' journeys, which in some cases could deny them safe access and asylum in a particular country if it is determined that they should have sought asylum in a country they had reached previously. There is sufficient evidence about migration authorities requesting such data from migrants' phones to support or deny their asylum claims¹⁹. Second, this may have an impact on the migrants themselves and on individuals or organizations which have supported them along their routes.

“

In the context of growing criminalization of migration, it might be dangerous to have information about people's journeys.

– Operations manager from a humanitarian NGO.

”

Third, forcibly displaced migrants could potentially be at great risk should their countries of origin access their digital data, in situations in which migrants are fleeing discrimination or persecution. As national authorities gain increasing control of the digital sphere and may use this to restrict rights and civil liberties²⁰, the risk of access to migrants' data is real and concerning. This is particularly the case where humanitarian organizations are operating under shifting national laws and will need to comply with these, even if they require the sharing of confidential and sensitive data from those organizations or their service providers²¹.

Finally, there is an element of authentication and verification of a digital identity, accessed remotely by the intended end user, which could potentially place a migrant at risk of manipulation by another person, such that the end user's benefit will be given under duress to that third person. Whether with a digital ID or a physical ID, there is probably no solution that could prevent this human element, this person-to-person dynamic and the power of influence, short of the humanitarian agency ensuring that the humanitarian assistance is being consumed by the intended end user. While post-distribution mechanisms are put in place to evaluate this, where duress exists, monitoring will likely not reveal the alternative destination of the assistance.

18 ENISA, "Identity theft from January 2019 to April 2020: ENISA Threat Landscape, October 2020. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-identity-theft/at_download/fullReport

19 See note 31 from Mixed Migration Centre.

20 See Institute of Development Studies: "Digital Rights in Closing Civic Space: Lessons from Ten African Countries", 2021. <https://opendocs.ids.ac.uk/opendocs/handle/20.500.12413/15964>

21 See for example Financial Times: "Myanmar junta pushes punitive cyber security bill", 11 February 2021. <https://www.ft.com/content/7b02059f-d6b7-4b69-9612-80683b849424>.

Loss of digital ID

As with physical ID, there exists a risk that migrants may lose access to their own digital identity. This will depend to a large extent on the components of the digital ID and to what degree it can be traced back to the user, as well as the security measures that are put in place.

In contrast to a physical ID, a digital ID (or its components) can be copied for safekeeping (though duplicating these elements increases the risk of unauthorised access). One key informant shared that their end users favoured the idea of using a QR code as their digital ID access, as it could be saved in their devices' memory or in their e-mail accounts as a back-up, accessible from different devices. A digital ID could also incorporate some of the retrieval procedures that are usually applied when a user forgets their username or password to access a platform. This could require a migrant to answer a straightforward personal question that is easy for them to remember, and difficult for others to know, thereby easing the process of retrieval. However, this would require the digital ID to be linked to the individual, and for the data to be stored on a platform, raising other privacy and control issues. Should the digital ID be completely decoupled from the individual (as in the case of organizations that do not link a digital ID number to a particular individual), then the ID would be difficult to retrieve in case of loss.

Confusion with foundational ID

The term "digital identity" can cause confusion, whether on the part of migrants, humanitarian workers or national authorities.

Key informants highlighted the need for digital ID solutions to be developed in the context of "do no harm" and particularly without providing false expectations to migrants who may have never possessed a foundational ID. One organization shared that some years ago, an NGO had provided some form of documentation to migrants, who mistook it for official acceptance of their asylum claims. Besides being detrimental to the morale of migrants, as well as highly confusing, such misunderstandings could cause conflicting communications with authorities and put migrants at risk where they are irregularly remaining within a country.

Another key informant highlighted that giving migrants their digital ID card had a huge impact on them. Although the card clearly indicated, in English and the native language of the migrants, that the card was for a limited medical purpose, and this limited purpose had also been explained orally during the registration process, the organization received reports from state hospitals that migrants were seeking services there on the basis of that digital ID card. The key informant indicated that although the limited purpose of the card was well understood, migrants had no other ID with which to seek services, and tried to use their digital ID for that reason.

Humanitarian workers may also misunderstand the concept of a digital ID in their contexts, confusing it with foundational ID, especially in the case of migrants who have no other form of ID, rather than linking the digital ID to a particular humanitarian function.

Finally, regarding national or local authorities, organizations have shared concern about how their digital IDs could be perceived as some form of informal registration of migrants that would go against the state's policy and approach to migrants. One organization decided that it was safer not to provide any kind of paper documentation to migrants to avoid confusion from the state. Other organizations shared that they had to carry out careful outreach with the national and local authorities to explain their digital solution in advance of its implementation and ensure that relevant staff would be appropriately briefed in cascade. In one case, it was referred to as a "digital profile", so that it would not be confused with foundational ID. Linking the digital ID to



In the context of growing criminalization of migration, it might be dangerous to have information about people's journeys.

- Operations manager from a humanitarian NGO.



humanitarian services that were already provided by the agency, and known to authorities, was useful to highlight that the digital ID was a component of the same service, and only an alternative manner to access the service.

ii. Risks and challenges for humanitarian organizations

Compliance with data protection (and potentially cross-border) regulations

As mentioned above, digital IDs will continue to develop from a technological perspective, as will the rules and regulations around their use and the associated data. A humanitarian organization, which may not have data protection or technology specialists, may not fully understand all the components of a digital ID, nor the future framework that may emerge to regulate it. This may expose an organization to regulatory risks, in addition to not being able to provide data security guarantees to a vulnerable migrant. Even where an organization may have strong data protection policies, there may be challenges in the practical implementation of those policies in the field.



A fundamental challenge is the level of capacity and understanding at the different levels of the organization – people do not know how to measure risk. So there is a disconnect between policies and practical implementation in terms of access to information.

– Migration expert from an international NGO.



There are some good examples of data protection agreements and information sharing protocols²² between various humanitarian organizations, based on cooperatively developed legal templates, and working successfully across a common cause and objectives. Key informants shared that these tended to be the result of a lengthy process when several organizations are involved, requiring contextual adaptations to be made to the agreements given the particular humanitarian scenarios. Yet, through the consultation it was not possible to identify instances in which these data sharing agreements had been deployed and functioned in cross-border contexts (although one worldwide data transfer form is being finalised between a network's members, for subsequent adaptation to each country's data protection laws). Cross-border data sharing may lead

to additional risks for the organization, particularly if it is not established across the border, and may be unfamiliar with the relevant legal framework.

National authorities' requests for data (in exceptional circumstances or not)

As mentioned above, national authorities are increasingly able to access confidential information, even when end users and humanitarian organizations believe the information to be safe. This may be due to a lack of understanding about the relevant data protection laws in a particular country or by underestimating a state's ability to subpoena an organization's confidential data about the migrants whom they serve. Alternatively, security-related issues may mean certain local authorities will requisition the information. Such access to sensitive data would constitute a key risk for humanitarian organizations in terms of internal compliance issues and potentially placing at risk the vulnerable people whom they serve. This could usually be mitigated through carrying out a data protection impact assessment prior to starting operations.

There are different vulnerable groups in terms of surveillance, and forcibly displaced migrants may be of particular interest for the authorities in their country of origin. Cognizant of this, one key informant explained that their standard policies and training include provisions for staff to regularly delete

²² For example, the Data Protection and Information Sharing Protocol Template from the Alliance for Child Protection in Humanitarian Action: <https://alliancecpha.org/en/child-protection-online-library/data-protection-and-information-sharing-protocol-dpisp-guidance-and>

sensitive emails and destroy hardware such as laptops and disks storing information, in the case of a hostile takeover by armed forces, serving to mitigate the risk.

High levels of investment and the search for sustainability

Initiating a digital ID solution, at a time when it is still considered an emerging technology, carries some financial risk in terms of the investment required (both of cost and time) and the potential non sustainability of the solution. Programmatic donors will likely not have a specific line item for these systems when funding a humanitarian activity, as the funding will be linked to the objectives and results of the project, rather than the solutions such as digital ID which may support the achievement of those objectives. One key informant queried the relevance of a digital ID solution, suggesting that it would be most important to focus on the protection of migrants, rather than developing a digital ID and improving the manner in which migrants may access services.

In addition to initial investment, organizations would need to ensure that the solution can be sufficiently financially sustainable, or that there is guaranteed funding to pursue its use over several years, to mitigate this financial risk.

Field staff may not be appropriately trained or interested

As noted above regarding compliance with data protection regulations, an organization's data protection policies may not be implemented in practice. In part, this may be due to national and field staff receiving insufficient training or not applying relevant processes. This in turn also exposes the organization to regulatory risk, with a variety of implications for the organization depending on its country of operation, as well as for the migrants themselves should there be a data breach.

In the move to a digital ID, key informants also highlighted the risk of buy-in or acceptance from the organizations' own field implementers. One noted that field implementers are weary of new solutions being introduced and may have limited interest in using any new system. Another key informant felt that resistance is particularly strong when staff are asked to use a digital system, due to a lack of perceived benefit to them.

This resistance can be overcome once a benefit to their work is demonstrated, though in the former instance, it may be a challenge for the organization to ensure buy-in from their exhausted field staff, especially if there have been various iterations of data registration systems. This in turn translates to an important operational risk for the organization as to the viability of a tool when its field implementers are unwilling to use it.

“

Refugees should be protected and we should look at this from the lens of how to protect them rather than how to give them services.

– Migration expert from a humanitarian donor.”

“

The majority of the technical solutions that are suggested are about moving from the analog world to the digital world. Some people do not understand the need to move to a computer database. This will create some resistance.

– Technology expert from a humanitarian organization.”

“

The nurses and the doctors and the people being asked to implement these new registration systems – they are just burnt out... They know who their populations are – they just need a pen and paper.

– Expert from a digital ID service provider.”

Reliance on scaling up and data sharing with other institutions

Scaling up a solution can be challenging, both within an organization and outside of it, bringing with it risks to successful implementation. One key informant highlighted the importance of developing a tool which can meet the information needs of all the organization's projects, given that their various donors require different types of information about the migrants whom they serve. Without the tool being aligned to the different information requirements, there is a risk that the tool will not meet with buy-in internally within the organization, resulting in weak and inconsistent deployment.

Other organizations consulted raised concerns about sharing sensitive data with other humanitarian organizations. One mentioned that if they did share the data with another humanitarian organization, this would give room for the state authorities to argue that the data could be shared with them too. Another organization highlighted the challenges in using a single, uniform system, given that different organizations have different mandates and consequently different ways of assisting migrants and protecting their data.

“

A key issue being examined is digital ID technical standards, to have a broad acceptance network. Those relying on the identity need to know what those standards are and whether they can trust it, and how different tools can interoperate.

– Digital identity expert from a humanitarian organization.

”

These risks regarding scale-up could be mitigated by ensuring that standards on digital IDs, data protection and data sharing are uniform, thereby building acceptance from the network required to use the solution at scale.

Lack of understanding of innovative technology and of different types of identity

By virtue of digital identities being innovative, developing them for use in the context of migration exposes humanitarian organization to risks related to the practical usability of the solution. Ultimately, the solution may not function as desired, and may face internal resistance.

“

Whilst there is appetite to test, there is some anxiety once we go beyond a pilot; it is a nascent technology, there is uncertainty about the user experience.

– Innovations expert from a humanitarian organization.

”

A new technology will also bring with it a lack of understanding from within the humanitarian organization, which, by its nature, will have expertise in other matters. In particular, humanitarian organizations may enter into an operational relationship with a technology provider, having substantially less understanding of the technology than the service providers. This could expose the organization to risks in not taking into account certain functions of the digital ID, or, as detailed below, that the technology could develop in unforeseen ways. One key informant shared concerns about the longevity of digital data, and the resulting responsibility of the humanitarian organization in ensuring that the data is available and maintained safely.

“

The tricky piece that we are trying to work out is: who holds on to this information and ensures that the information is available forever? Or until when?

– Country Director from a humanitarian organization.

”

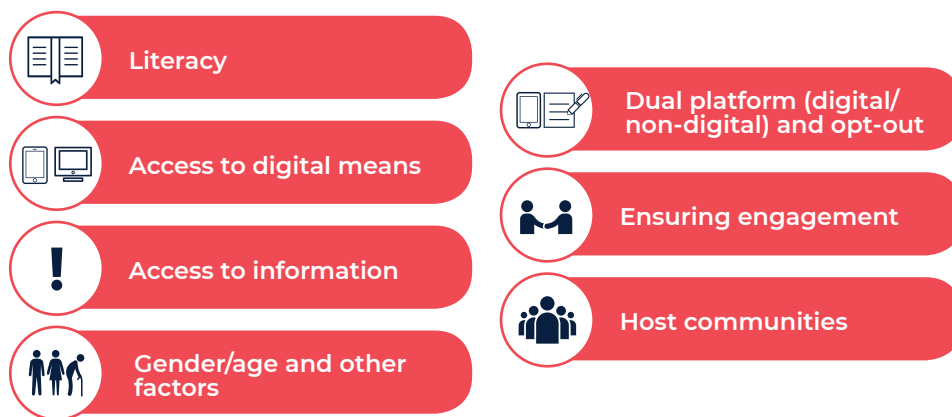
As mentioned above, there is also a lack of alignment on the meaning of functional and foundational identity. For example, the proposed definition for foundational identity at the start of this report mentions that it is a legal identity. However, a birth certificate is widely considered to be foundational

identity, yet it is not a document a person uses to legally prove their identity (it is usually not issued with a photograph, nor does it make mention of identifying features). Instead, it is used to support the issuance of identity documents.

It is also likely that functional ID will be linked to foundational ID in some manner, even if the digital functional ID does not include personally identifiable information (PII). For example, paper based personal information (such as that included in medical histories or training records) will likely be digitized and included within the digital ID to ensure that a migrant's legacy information is retained with their new digital ID. One key informant highlighted that the legacy documents containing the migrant's PII could be suitably encrypted and kept secure in a locked digital wallet while maintain interoperability between the two forms of ID.

e. Ensuring inclusion for the most vulnerable migrants

Figure 6: Key elements to be considered to ensure inclusion in developing a digital identity.



In developing a digital solution for migrants, it is crucial to remain sensitive to local contexts and concerns as these relate to identity (especially where there may be ethnic tension) as well as to the use of technology and the types of facilities which are known to that community and used by them. The inclusivity of a solution will also be key to ensuring its acceptance and adoption by different communities, especially as perceptions of exclusion could create divisions within the migrant community in a particular scenario, with the associated safety risks. Figure 6 sets out the key elements to be considered to ensure inclusion in developing a digital identity.

Literacy

For a digital solution to be inclusive, it would need to be adapted to migrants who have varying levels of alphabetical and technological literacy, and therefore may not be able to access a digital solution which relies on interaction with text and technology. Literacy levels depend strongly on migrants' age ranges, their level of education and their place of origin.

“
Learn, adapt and trial in a way that avoids risk of exclusion and be open about the risks that flow from that.
 – Technology expert from a humanitarian organization.”

One interviewee shared that an estimated 90 per cent of the migrants to whom they attend are illiterate and faced challenges in communicating with them as they were not able to rely on sending SMS or publishing signs or infographics. Equally, those migrants were not able to interact with their digital IDs, relying instead on the humanitarian organization to guide them on its use.

The COVID-19 pandemic has required humanitarian services to be adapted and has accelerated a move to digital means due to the desire to reduce the risk of transmission through physical contact. This has led various organizations to have to innovate and to orient their staff, as well as the vulnerable people whom they serve, towards the use of new technological tools. Some organizations have had to carry out eligibility confirmation or authentication remotely. In terms of digital literacy, it was generally felt that migrants up to 35 years of age could be considered eager to learn how to use new technology.

Regarding the use of digital technologies by elderly people or those not used to them, additional support from humanitarian organizations was found to be required for humanitarian assistance to be accessible. Some provided physical outreach teams who supported beneficiaries with registration processes. One interviewee shared that in the context of livelihood activities, their organization provided one-to-one support for migrants and developed a tutorial to explain to them how they could access a personal email, create an account, and use a weblink to access a course on business management.

Another key informant shared their organization's experience of supporting migrants in seeking work through a digital platform. Migrants were trained on digital literacy and additional skillsets that enabled them to set up an online profile on the platform. The humanitarian organization also provided several computer workshops so that migrants could learn to edit their profiles and work with various pieces of software. Migrants were then paid for their services through an electronic transfer. Once they had some success in earning through the digital platform, the organization supported them further in providing them with laptops to facilitate their work.

Similar support and one-to-one attention could be provided to migrants in the use of a digital identity to ensure that, where they may not have the technological skills, they may be able to develop these with support from the humanitarian agency. Peer to peer support from within migrant communities is also promoted, as certain members of the community are likely to be more technologically literate than others and can provide support to their fellow migrants.

In the event of migrants who are unable to read and/or write, a digital identity solution could incorporate the use of feature phones with pre-recorded messages providing options for steps to be taken and requiring a number to be pressed to select a given option. A solution including such functionality would also be inclusive for an elderly population more accustomed to listening to radios than to using digital screens.

Access to digital means

A digital ID solution will also require migrants to have access to digital means for it to be inclusive.

Certain sophisticated solutions, such as digital IDs based on biometrics, will require higher end smartphones to function.

Access to smartphones varies by migration contexts. In the journey between the Middle East and Europe, smartphones are widely owned and used, whereas in the Horn of Africa, they are less readily available or are often stolen or sold²³. Additionally, in several contexts, smartphones are shared between families or communities, so there is no guarantee of privacy. Many key informants emphasised that means of communications are usually highly valued by migrants, who will seek to prioritise these when they have savings.

Given that migrants' access to digital means is highly variable, an inclusive solution will need to be adapted to those who do not have access to the technology. It would ideally incorporate accessible elements of hardware, such as fixed-site tablets, computers or mobiles and mobile kiosks, at locations that migrants could reach.

23 Mixed Migration Centre, "Hype or hope? Evidence on use of smartphones & social media in mixed migration", 23 January 2019. <https://mixedmigration.org/articles/hype-or-hope-new-evidence-on-the-use-of-smartphones-and-social-media-in-mixed-migration/>

To cater to migrants who have access to hardware without connectivity, an option may be to bulk purchase SIM cards and provide these to migrants (usually a SIM card would be registered to a person, requiring ID and potentially excluding undocumented migrants). Alternative solutions include providing free connectivity vouchers or data packages and negotiating reserve charges with telecoms operators. Though this would lead to high costs and would unlikely be sustainable over the long term, such solutions have been used by some of the organizations consulted, to ensure that digital solutions could be used by migrants.

There may be constraints in terms of accessibility of the relevant telephone or internet network. As such, the solution would need to work partially offline, with a capacity to update any data once a connection is reached. It was also suggested that last-mile connectivity activities could take place in parallel with activities to increase digital literacy and access to digital means, while questioning whether digital IDs would be appropriate for last-mile communities, given the lack of infrastructure and hardware.

Finally, ensuring an inclusive approach also requires being open-minded about the different abilities and access of migrants relating to technology, such that capacities and skills not be underestimated, but rather promoted and engaged through the digital solution.

Access to information

Access to information needs to be guaranteed to ensure that any digital ID solution is consulted, co-designed and ultimately used by migrant communities. It goes without saying that if migrants are not aware of a particular digital solution, they are not going to engage with it or use it. Improved access to information is crucial so that migrants can access trusted information and act upon it²⁴.

Though access to services and information may also depend largely on the level of immersion of a migrant in a given context, many key informants reported that migrants were consistently seeking information, learning from observation and building on their lived experiences of crossing borders and adapting to new contexts.

Modern communications tools (social media, digital campaigns, printed press and signs, videos) are important in reaching migrants who are open to receiving information, or who are actively searching for it. Yet communications may be challenging where migrants speak a different language to the official language of a particular country, or where migrants may not be literate, impacting their ability to understanding written communications. In such circumstances, organizations seek oral communication routes, disseminating messages and information through staff and volunteers (particularly looking to do so in the languages used by migrants), through community meetings or through loudspeakers attached to vehicles driving through areas known to be frequented by migrants.

Organizations also seek to leverage existing community interactions and networks, recognising that trusted sources of information for migrants tend to be their family, friends, fellow migrants or diaspora. Promoting sharing of accurate information between communities can also be much more engaging than where that information is shared by a humanitarian organization.



We often work in contexts where internet is not prevalent, but should not underestimate people's abilities and access to technology.

– Technology expert from a humanitarian organization.



24 In a regional evaluation of information and communications needs of migrants from Venezuela, results indicated that one in two people felt informed, and that their prime sources of information are Facebook, WhatsApp, speaking to people and using the internet and television, with 57% of surveyed persons using the internet every day. See R4V, IFRC, UNHCR: Regional Information and communications needs assessment: Understanding the information and communication needs of refugees and migrants in the Venezuela Situation, November 2019. <https://data2.unhcr.org/en/documents/details/73683>

Gender and age

Gender and age were identified as two key factors that could affect a migrant's ability to access trusted information and digital means, as community norms and culture, or power imbalances within communities and families, could limit these. Other elements that may give rise to discrimination within a community, such as disability, sexual orientation, ethnicity or religion, may similarly lead to a person's lack of access to information or to a digital solution.



There may be issues when one person receives a message for the whole family; they may not be physically close to their family or may not be honest in terms of sharing the information with the family or the rest of the community.

– Operations expert from a humanitarian organization.



Particularly when it comes to gender, a digital solution should seek to address the existing gender identity divide²⁵, as well as the gender digital divide²⁶, recognising that women have greater needs for identity and have lesser access to digital means. A solution should therefore incorporate the flexibilities required so that women and girls may enhance their digital knowledge and skills, potentially with tailored training to ensure that they are properly empowered.

Regarding age, some of the digital challenges faced by more elderly members of the population are outlined above. Different age perspectives should therefore be built into the digital solution, to ensure that it remains accessible and inclusive for the young and for the elderly.

Dual platform and opt-out

Several key informants emphasized the need to have a dual platform, which would provide a digital option as well as a non digital option. Another suggestion would be to have a mix between a virtual and physical interaction, such that a migrant needing technology support would be able to access the required hardware and advisory support to be able to use the digital technology.



A single system has a greater risk of excluding the vulnerable population.

– Migration expert from a humanitarian organization.



Real alternatives to a digital solution should be provided, allowing migrants to make informed choices about the platform they prefer to use. Ultimately, a migrant's access to humanitarian assistance should not be conditioned upon use of a digital identity, and migrants must be free to state they do not wish to use a particular solution. Accordingly, any digital solution will need to allow for migrants to opt out of using it, and an alternative (or alternatives) provided to those migrants, along with explanations about the differences between both systems.

25 World Bank Identification for Development estimates that one in two women in low income countries do not have an ID: <https://id4d.worldbank.org/global-dataset/visualization>.

26 GSMA: "The digital lives of refugees: How displaced populations use mobile phones and what gets in the way", 2019; Overseas Development Institute, Humanitarian Policy Group: "The humanitarian 'digital divide'", November 2019.

Ensuring engagement

Ensuring that a digital solution can be inclusive will also require that not only migrants, but also local level community and social organizations, are constructively engaged in the process.

To engage migrants, it was recommended that a solution should be perceived as “fun” as well as useful, so that it could be seen as interactive in the same way as social media and video games are, as opposed to being “a worthy cause only”. Means of engagement through active participation can include working with community leaders, setting up community working groups, ensuring co-design sessions, and ensuring that feedback is integrated into the product and processes, including through complaints mechanisms.

What will drive migrants to participate in a digital ID system or not may be intrinsically linked to their reasons for migrating, the associated risks, and their means of migration, recalling that resorting to the services of smugglers can be common in certain migration scenarios. Those who have fled due to a threat of immediate harm to themselves or their families are probably less willing to have their personal information collected and registered during their migration journeys. Those who have fled to seek a more secure environment with a focus on their future potential may be more willing to seek means to integrate into the education system or the workforce and accordingly be more open to participate in a digital ID system.

Including local community-based organizations is essential, as certain migrants will be attended by them rather than by national and international organizations, due to their sometimes-remote locations and higher level of local knowledge and reach. Beyond framing digital ID initiatives within the scope of the localization debate²⁷, it is also important to evaluate the ability of local organizations to engage with digital solutions for those solutions to have the sufficient scale and scope.

Host communities

Several key informants emphasized the importance of involving host communities, as well as migrants, in the use of digital IDs. Recognizing that humanitarian organizations are guided by people’s vulnerability, rather than their profile as migrants, they attend similarly to people on the move and host communities when in need, in line with the humanitarian principle of impartiality. As such, the application of digital IDs should be done equally between migrants and host communities. This would also be key to countering xenophobic sentiment and potential violence based on perceived views that migrants access more resources than host communities.

27 The Grand Bargain, Workstream 2 on more support and funding tools for local and national responders (localization) <https://interagencystandingcommittee.org/more-support-and-funding-tools-for-local-and-national-responders>; Workstream 2 website: <https://gblocalisation.ifrc.org/grand-bargain-localisation-workstream-2/>.

3

Recommendations



*Children displaced from Rakhine State in Myanmar, living in Cox's Bazar, Bangladesh. April 2017
Photo credit: Mirva Helenius/IFRC*

1

Favour a long-term vision on digital identities, framed in guiding principles or a strategy to ensure internal and external accountability.

Organizations seeking to expand their work on digital identities should ensure that they adopt and publish a long-term vision on the matter, ideally framed within guiding principles or a strategy. This transparent approach will help to ensure that internal and external accountability is clearly understood by all stakeholders and will seek to guide ongoing developments. This should include definitions, principles, standards, sustainability strategies and risk mitigation actions (such as field level data protection training).

In addition, safeguards should be put in place in terms of the level of control a migrant may have over their data, to evaluate whether too much onus may be placed on an individual and whether the organization itself will eventually be able to attend to the person's needs.



If we give a person the full control, we need to ensure that we have the capacity of dealing with the consequences of giving the person full control, in terms of providing services.

- Operations expert from a humanitarian organization.



2

Further exploring and testing opportunities for humanitarian organizations and migrants.

Digital identities seem to offer many opportunities for organizations working in the humanitarian field. These include more efficient use of time and money, an improved focus on the quality and effectiveness of assistance and more efficient service provision. There is a potential for wide impact and reach and, ultimately, digital identities could better safeguard communities. For migrants, using a digital identity would support their privacy, strengthen their dignity and facilitate their access to services. It would be essential to explore and test these assumptions, particularly with field staff and migrants to verify that the concept and eventual solution will in fact work for them.

The consultation process triggered various expressions of interest from humanitarian organizations eager to participate in and explore the opportunities for themselves and for migrants. The wide interest in the Global Virtual Summit on Digital Identity for Refugees²⁸, led by UNHCR in May 2019, demonstrates the interest from the global humanitarian community in exploring the issues around digital identities specific to refugees. As forcibly displaced migrants include a range of profiles and situations, it is expected that interest in exploring digital identities in this context will only increase.

28 See: <https://www.unhcr.org/idecosystem>

3

Follow a model of cooperation or consortia, identifying clear governance structures and incorporating relevant expertise in advisory and decision-making functions.

Organizations wishing to use digital identities in their migration activities should seek to ensure a cooperative approach from the outset, considering work in consortia to pool resources and seek common objectives. This common mindset could be leveraged to promote exchanges and shared learning, to identify shared challenges needing to be resolved and to minimise redundant systems. In addition, in exploring the application of digital identity to migration activities, it is crucial that structures include organizations that have substantial migration activities and expertise. It would also be key to encourage partners to reflect on their potential engagement with such a solution, including with donors. Such collaboration can be stimulated through private exchanges, public talks and conferences and more pro active involvement as mentioned above, whether as observers to the process, sharing their time and resources on selected aspects of the pilot, or having a guiding or advisory role.

For example, the DIGID Advisory Group was established with a specific outcome in mind, which was to resolve the difficulties in making humanitarian cash transfers to end users who do not have identity documents. As the DIGID2 projects moves away from the focus on cash transfers and seeks to prioritise migrants as a target group, it is recommended to include additional members in the DIGID Advisory Group and the DIGID Steering Group, with expertise in substantial migration activities and, ideally, reflecting the diverse migration scenarios and levels of organizational capacity in the field.

Implementing a digital ID system to be used by several organizations and, in due course, a growing number of organizations, will require clarity in terms of the system's governance framework. Not making it agency-specific may mean that organizations and staff will feel more comfortable using it, as it would reflect an inter-agency process.

Several key questions would need to be explored and resolved in establishing a governance framework for a digital identity system:

- Who has oversight?
- Who has accountability?
- Who owns the digital ID system?
- Who owns the data within the digital ID system?
- Which organizations are part of the coordinating committee?
- Which organization leads configuration and training?
- What is the coordination mechanism?
- How can interoperability issues be resolved?
- How are new organizations vetted to issue credentials?
- What standards govern the way in which credentials are created?

4

Leverage advocacy and leadership roles from humanitarian organizations.

Humanitarian agencies working with migrants should leverage their experience and expertise to advocate for the required adaptations for digital identity solutions to be properly inclusive, with greater user control.

Recognising that many of the vulnerable migrants whom they serve often do not have access to identity documents, humanitarian organizations could carry out greater advocacy towards governments for equitable access to foundational identity, for the more than one billion people around the world who currently lack it. They could also ensure national authorities' buy in for functional ID solutions and seek to expand as much as possible the scope of the functions and services that can be accessed with this ID, subject to appropriate data protection and data sharing mechanisms.

5

Build trust at all levels.

Building trust at all levels will be crucial to the successful development and deployment of the solution. Trust will need to be established:

- (i) Internally within the organizations making up the DIGID consortium – to demonstrate internally that the solution is desirable and that it can work at scale.
- (ii) With the migrants being served – so that they can feel comfortable in developing and using the solution, and trust the technology to keep their personal data safe and confidential (if any is collected).
- (iii) With the national authorities – to ensure that the digital identity is not understood as a back-door solution to providing foundational ID to people on the move, ideally linking the digital ID to services that are already being provided.
- (iv) With other humanitarian organizations – to build consensus between those organizations, to be able to accept and use their credentials when verifying digital ID and ultimately to ensure that the solution works at scale with a large number of humanitarian organizations.

With regard to the final point on building scale and inclusion of other organizations, the pilot should ensure testing of interoperability and the use of a solution in accessing a variety of services, reducing fragmentation and to address one of the more challenging aspects of digital IDs from the outset. The pilot should also explore the ways in which different digital ID systems could be interconnected, given the diversity of systems already in existence, and which will surely continue to be developed.

“

Trust is central to interoperability – Technology expert from a humanitarian organization.

”

“

There cannot be one identity to rule them all. There cannot be one proprietary. There is no way there will be a single vendor for this. I believe there will be a network of networks... There will be information exchange hubs. There will be no solution to the siloes other than connecting them... like using different airlines.

– Expert from a digital ID service provider.

”

6

Carry out internal and external advocacy about data collection and data minimization (privacy versus the risk of fraud).

As highlighted above, a wealth of personal information of unclear operational use is collected throughout registration and monitoring processes when attending to migrants in need. In some cases, asking too much information of migrants erodes trust with a humanitarian institution, creating a perceived linkage with migration authorities who ask for the same information. Migrants who have had a demanding journey, encounters with armed forces and smugglers, and who ultimately do not want their journeys to be traced, may be unwilling to be in touch with a humanitarian institution, like any other institution, and may be less willing to share their personal information, rather preferring “to stay invisible to continue on his way”, as shared by a migrant in a European country.

Minimizing the collection of such personal data would be a key component to incorporate within a digital ID solution, alongside clarifying donor and partner expectations before moving forward, in terms of contexts, risks, access to identity details, and the vulnerable condition of the migrants being attended. Arguably, when the risks to privacy and safety are being weighed up against the potential downstream leakage of aid, a humanitarian organization should seek to support the person in need, in line with the humanitarian principles. Most donors may err on the side of avoiding the quantifiable loss, rather than some harm to a person’s rights, which can be hard to quantify, and will want to know that their goods were distributed as promised. As such, it will be key to engage with donors to seek their contributions and find a solution that balances these concerns.

“

From a donor verification point of view, we need to ensure that the person selected is the same person who receives the assistance. There are ways to do that without visualizing data.

– Migration expert from a humanitarian donor.

”

Internal advocacy will also be required, to examine the relevance and proportionality of internal rules, policies and procedures relating to the collection of beneficiary data in humanitarian operations. Finally, relating to an earlier recommendation on leadership and advocacy, the DIGID consortium could seek to streamline data collection, access, usage, sharing, retention and deletion practices across the DIGID consortium in the first instance, and then more broadly with other organizations (which will likely be a significant challenge due to the wide differences in practices).

7

Carefully consider the vulnerabilities of migrants which may render their profile unsuitable for a digital ID pilot.

A vulnerability and stability (or resilience) evaluation should be carried out to determine the preferred migrant profile for the pilot, as certain migrants may be in too unstable a situation to participate. This should take into account the stage of their journey they are at, as well as their geographic location. This vulnerability evaluation should also take host communities into account, where their vulnerabilities mirror those of migrants.


4

Conclusion

The use of digital identities by humanitarian organizations in migration activities is a growing area of interest, providing considerable potential for greater collaboration around shared challenges. Findings from the consultation explore the uses of digital identities, as well as the associated benefits and risks, with a strong focus on the need for an inclusive and engaged approach to ensure a user-centred vision. Recommendations to organizations are both internal facing, towards their own processes and visions, as well as external facing, proposing to draw on their expertise and positioning to advocate for identity for the most vulnerable. These recommendations also seek to incorporate an end-user perspective, to be further tested in end-user consultations as the DIGID2 pilot progresses.

5

Selected References

A photograph showing a group of migrants on a rescue vessel in the Mediterranean Sea. The migrants are crowded together, some wearing orange life jackets. The background is a blue wall with some peeling paint. The overall scene is one of a rescue operation.

October 2016. Migrants brought to safety on rescue vessels in the Mediterranean Sea. Photo credit: Mathieu Willcocks/MOAS.eu

Bogle, A. "Biometric data is increasingly popular in aid work, but critics say it puts refugees at risk", ABC Science, 20 June 2019. <https://www.abc.net.au/news/science/2019-06-21/biometric-data-is-being-collected-from-refugees-asylum-seekers/11209274>

Caribou Digital, "Identity at the Margins: refugee identity and data management", 2018. <https://assets.publishing.service.gov.uk/media/5cecedd6ed915d2475aca8c5/Identity-At-The-Margins-Identification-Systems-for-Refugees.pdf>

Cheesman, M. "Self-Sovereignty for Refugees? The Contested Horizons of Digital Identity, Geopolitics, October 2020. <https://doi.org/10.1080/14650045.2020.1823836>

Data & Society, "Digital Identity in the Migration and Refugee Context: Italy Case Study", 2019. https://datasociety.net/wp-content/uploads/2019/04/DataSociety_DigitalIdentity.pdf

Dreir, H. "Trust and Consequences: how confidential therapy notes were used against a teenage asylum-seeker", The Washington Post, 15 February 2020, <https://www.washingtonpost.com/graphics/2020/national/immigration-therapy-reports-ice/>

GSMA: "The digital lives of refugees: How displaced populations use mobile phones and what gets in the way", 2019. <https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/07/The-Digital-Lives-of-Refugees.pdf>

Korkmaz, E. "Blockchain for refugees: great hopes, deep concerns", 24 January 2018. <https://www.geh.ox.ac.uk/blog/blockchain-refugees-great-hopes-deep-concerns>

International Committee of the Red Cross (ICRC), Policy on the Processing of Biometric Data by the ICRC, 2019. https://www.icrc.org/en/download/file/106620/icrc_biometrics_policy_adopted_29_august_2019_.pdf

International Committee of the Red Cross (ICRC) and Brussels Privacy Hub, "Handbook on Data Protection in Humanitarian Action", second edition, May 2020. <https://www.icrc.org/en/data-protection-humanitarian-action-handbook>

International Committee of the Red Cross (ICRC) and Privacy International, "The humanitarian metadata problem: "Doing no harm" in the digital era", October 2018. <https://www.privacyinternational.org/sites/default/files/2018-12/The%20Humanitarian%20Metadata%20Problem%20-%20Doing%20No%20Harm%20in%20the%20Digital%20Era.pdf>

International Federation of Red Cross and Red Crescent Societies, Humanitarian Service Point Toolkit, October 2020.

Meaker, M., "Europe Is Using Smartphone Data as a Weapon to Deport Refugees," Wired UK, 2 July 2018. <https://www.wired.co.uk/article/europe-immigration-refugees-smartphone-metadata-deportations>

Overseas Development Institute, Humanitarian Policy Group: "The humanitarian 'digital divide'", November 2019. https://odi.org/documents/6109/The_humanitarian_digital_divide

R4V, IFRC, UNHCR: Regional Information and communications needs assessment: Understanding the information and communication needs of refugees and migrants in the Venezuela Situation, November 2019. <https://data2.unhcr.org/en/documents/details/73683>

Raczkowski, C. and Reed, D. "2020 – How SSI went mainstream", published 12 January 2021. <https://sovrin.org/2020-how-ssi-went-mainstream/>

Solomon, B. "Digital IDs are more dangerous than you think: Opinion: Digital identification systems are meant to aid the marginalized. Actually, they're ripe for abuse." Wired, 28 September 2019. <https://www.wired.com/story/digital-ids-are-more-dangerous-than-you-think/>

Sovrin, "Whitepaper on guardianship in self-sovereign identity", December 2019. <https://sovrin.org/on-guardianship-in-self-sovereign-identity/>

Thakur, S. "Results from the field: Improving livelihood prospects for refugees through decentralized identity in Gaziantep, Turkey", Medium, 14 January 2021. <https://medium.com/gravity-earth/results-from-the-field-improving-livelihood-prospects-for-displaced-persons-through-digital-5786587308f8>

The Engine Room: "Understanding the lived effects of digital ID: A multi-country report", 2020. https://digitalid.theengineroom.org/assets/pdfs/200123_FINAL_TER_Digital_ID_Report+Annexes_English_Interactive.pdf

The Engine Room and Oxfam: "Biometrics in the Humanitarian Sector", March 2018. <https://www.theengineroom.org/wp-content/uploads/2018/03/Engine-Room-Oxfam-Biometrics-Review.pdf>

USAID, "How to: Create digital ID for inclusive development – A companion to identity in a digital age: infrastructure for inclusive development", July 2019. https://www.usaid.gov/sites/default/files/documents/15396/DID_Layout_v9_Interactive.pdf.pdf

USAID, "Digital Ecosystem Country Assessment (DECA): Colombia", July 2020. https://www.usaid.gov/sites/default/files/documents/DECA_Report_COLOMBIA_EXTERNAL_15OCT20.pdf

UNHCR Strategy on Digital Identity and Inclusion, February 2018: https://www.unhcr.org/blogs/wp-content/uploads/sites/48/2018/03/2018-02-Digital-Identity_02.pdf

UNHCR: "Ethiopia rolls out new biometric system to enhance registration of refugees", 1 December 2017. <https://www.unhcr.org/blogs/ethiopia-rolls-new-biometric-system-enhance-registration-refugees/>

UNHCR briefing note: "Joint Bangladesh/UNHCR verification of Rohingya refugees gets underway", 6 July 2018. <https://www.unhcr.org/en-us/news/briefing/2018/7/5b3f2794ae/joint-bangladeshunhcr-verification-rohingya-refugees-gets-underway.html>

UNHCR, "How digital identity can enable the Global Compact on Refugees", December 2019: <https://www.unhcr.org/blogs/how-digital-identity-can-enable-the-global-compact-on-refugees/>

UNHCR, "Connecting With Confidence: Managing Digital Risks to Refugee Connectivity", March 2021. <https://www.unhcr.org/innovation/wp-content/uploads/2021/03/CWC-Managing-Digital-Risks-To-Refugee-Connectivity-Report.pdf>

Yoti digital identity toolkit. <https://www.yoti.com/resources/digital-identity-toolkit/>

Young, L. and Jurko, I. 2020, "Future of Vulnerability: Humanity in the Digital Age", Humanitech, Australian Red Cross. <https://apo.org.au/sites/default/files/resource-files/2021-02/apo-nid311045.pdf>

6

Appendices



*Ethiopia, North Gondar. Women in Debarik IDP camp, having fled fighting in Tigray. February 2021.
Photo credit: Rita Nyaga/IFRC*

APPENDIX I: SEVEN KEY QUESTIONS USED IN THE CONSULTATION

The seven questions guiding the consultation with migration experts and key stakeholders were the following:

- i. What are common services (e.g. cash) provided to vulnerable migrants, what are the identity related requirements, issues/challenges in receiving such services that are related to identity? At what points along a migration route(s) are these services provided?
- ii. What are the needs and concerns of vulnerable migrants regarding identity? What is the understanding of migrants regarding identity and its uses?
- iii. How to ensure inclusion of vulnerable migrants particularly those with minimum levels of literacy and low access to digital means (e.g. phones and internet)? What are the conditions or contexts for vulnerable migrants to manage their own identity information and sharing such data? Any risks of exclusion for those with low digital means and those who may not want to be identified?
- iv. What are the systems or solutions used or being developed by humanitarian organizations to manage services to vulnerable migrations and how do they tackle identities? How is the data used or shared by those organizations?
- v. How to ensure compliance with data protection regulations, or other national or local government rules (including rules imposed by FSPs), especially cross-border, or to what extent data will be caught by applicable data protection regulations?
- vi. What are the major risks to vulnerable migrants when digital ID technology is employed? How does this differ from the use of physical ID? Do organizations take actions to ensure risk to migrants is minimized beyond simply following regulations?
- vii. How can foundational digital ID's issued by government or other organizations with mandate towards migrants/refugees in providing services to migrants be linked to functional digital ID's issued by humanitarian organizations? What are the obstacles to the adoption and acceptability of functional digital identities issued by humanitarian organizations? What are possible pathways (including advocacy) to address these?

APPENDIX II: LITERATURE REVIEW

The non-exhaustive literature review below, limited due to time constraints, focuses on existing resources on digital identities in the migration context, along with associated risks and opportunities, although some more general literature on digital identities has also been included for greater context. The literature reviewed originates from the technology industry, in terms of highlighting theoretical or tested innovations (because significant opportunities for digital identities are being created in the private sector), from humanitarian organizations and human rights organizations outlining elements of practical implementation and risks, and from policy and research institutions investigating benefits and concerns. For a list of selected references used in the literature review, see the Selected References section.

Toolkits and guides

Several toolkits and guides²⁹ on digital identity exist, guiding users on the use cases of digital identity, how to create them, key factors to consider when implementing them, data protection considerations and how digital identity systems could be managed.

Risks to privacy as a major concern

Much of the recent literature highlights the risks to privacy in confidential data collection and use of mobile technology by migrants, noting that data anonymization is a particular challenge, as the removal of personally identifiable information does not prevent the use of other information, such as metadata (data about the data, while not being the content of the data), being used to identify a specific individual³⁰.

In the case of people on the move, access to and use of metadata about location, date and time may be of particular concern. Certain countries have laws allowing immigration officials to extract data from asylum seekers' phones in relation to their asylum claims³¹, leading certain migrants to fear mobile phone surveillance, despite mobile phones often facilitating their journeys and their contacts with loved ones. Other reports cite immigration agencies using confidential therapy notes to support deportation requests of teenagers³². In the light of increased surveillance through the use of technology and complex laws requiring personal data to be shared, there is concern that digital identities may pose one of the gravest risks to human rights through technology³³.

Additional concerns and challenges on digital identities for migrants

Concerns about migrant consent and the lack of migrant agency, privacy and engagement have been highlighted³⁴, along with the importance of greater interoperability between humanitarian organizations, recognising that this remains one of the key challenges. One report argues that digital identity technologies will not provide easy solutions in the context of migration, instead introducing a new layer of bureaucratic biases, discrimination or power imbalances³⁵. Recommendations include

29 Yoti digital identity toolkit, January 2020; International Committee of the Red Cross (ICRC) and Brussels Privacy Hub, "Handbook on Data Protection in Humanitarian Action", second edition, May 2020; USAID, "How to: Create digital ID for inclusive development – A companion to identity in a digital age: infrastructure for inclusive development", July 2019.

30 International Committee of the Red Cross (ICRC) and Privacy International, "The humanitarian metadata problem: "Doing no harm" in the digital era", October 2018.

31 Meaker, M., "Europe Is Using Smartphone Data as a Weapon to Deport Refugees," Wired UK, 2 July 2018.

32 Dreir, H. "Trust and Consequences: how confidential therapy notes were used against a teenage asylum-seeker", The Washington Post, 15 February 2020.

33 Solomon, B. "Digital IDs are more dangerous than you think: Opinion: Digital identification systems are meant to aid the marginalized. Actually, they're ripe for abuse." Wired, 28 September 2019.

34 Caribou Digital, "Identity at the Margins: refugee identity and data management", 2018.

35 Data & Society, "Digital Identity in the Migration and Refugee Context: Italy Case Study", 2019.

donor alignment and support for greater privacy and data management, the integration of data accountability in interactions with affected populations, the establishment of a multi stakeholder working group on interoperability as well as a standards body, and better training and internal capacity-building on data protection and data responsibility.

The promise of digital identities for migrants should also be weighed up against the socio-economic and structural contexts of the countries in which they are migrating. Given that the majority of refugees are based in the global South, a refugee with a digital identity may not automatically be empowered or able to overcome poverty in a context of high unemployment rates and harsh working conditions³⁶. As the literature reviewed tends to weigh more heavily towards the risk elements, this serves as a reminder of caution required in developing such systems.

Focus on specific migrant crises

Some of the literature focuses on particular migrant crises, including Rohingya refugees in Bangladesh³⁷ and refugee camps in Ethiopia³⁸ and the deployments of digital identities in both contexts with the aim of empowering refugees and affording them increased access to services such as aid, child protection, education, and to preserve individual identity. Those scenarios have also raised challenges³⁹ around the risk of surveillance and control over those populations, lack of community engagement, lack of informed consent, potential exclusion (also through barriers to registration and use), decrease of data privacy, lack of trust, and power imbalances between the migrant and the entity collecting data, all of which can lead to negative perceptions from the target population and resistance to the solution.

Types of migrants

Though much of the literature refers to the number of people globally who do not have identity documentation, as well as Sustainable Development Goal 16.9, it is of note that the limited case studies on migrants and digital identity focus on refugees or asylum seekers, being settled migrants. At this stage, it was not possible to find any examples in the literature of digital ID for people still on the move. More generally, there are not many examples of operational uses of digital identity with migrants. This is indicative of the challenges in attending to people on the move through a digital identity, especially since they are pursuing a journey and possibly will not be interested in participating in a pilot project or training session on digital identities.

Little user engagement

Although one study does focus on the importance of communicating with communities in developing digital connectivity solutions generally⁴⁰, and the need to engage with communities is clearly recognised, the literature review did not identify a case study or in-depth exploration of user-centric design in the development of digital identities.

Increased use of biometrics in attending migrants

Over the past two years, there has been continuous growth in publications on the use of biometrics technology in migration work, considering both its risks and efficiencies⁴¹, as the use of biometric data⁴² to register and de-duplicate migrants receiving assistance increases across humanitarian

36 Korkmaz, E. "Blockchain for refugees: great hopes, deep concerns", 24 January 2018.

37 UNHCR briefing note: "Joint Bangladesh/UNHCR verification of Rohingya refugees gets underway", 6 July 2018.

38 UNHCR: "Ethiopia rolls out new biometric system to enhance registration of refugees", 1 December 2017.

39 The Engine Room: "Understanding the lived effects of digital ID: A multi-country report", 2020.

40 UNHCR, "Connecting With Confidence: Managing Digital Risks to Refugee Connectivity", March 2021.

41 Bogle, A. "Biometric data is increasingly popular in aid work, but critics say it puts refugees at risk", ABC Science, 20 June 2019.

42 Defined by ICRC as "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person", Policy on the Processing of Biometric Data by the ICRC, 2019.

operations⁴³. Some United Nations agencies, such as the United Nations High Commissioner for Refugees and the World Food Programme, are making increasing use of biometrics to enable migrants to receive cash assistance through eye scanners⁴⁴, and the International Committee of the Red Cross (ICRC) has published its policy on processing biometric data in limited use cases.

Increased exploration of the potential of self-sovereign identity

There is increasing examination of the potential use of self-sovereign identity (SSI) for migrants. This has brought to light three challenges to its “emancipatory potential”: it is a form of technology that is not neutral towards its users; refugees’ capacities may not be sufficient; concerns exist over data governance⁴⁵. Some positive case studies on the use of SSI were also identified in the literature review, including the pilot project implemented by Gravity as part of the Sustainable Development Goals Impact Accelerator⁴⁶. The project in Gaziantep, Turkey, ran from July to December 2020, from the first phase of partner engagement and requirement gathering, to the final implementation phase. The pilot enabled displaced persons to create identity based digital wallets to store certified training certificates and share those certificates with potential employers among a pool of seven enterprises. This solution provided an important benefit to settled migrants in being able to store and manage their educational and professional credentials to seek improved livelihood opportunities.

As part of its next steps, it is understood that Gravity will be improving its solution, incorporating participants’ feedback and evaluating their suggestions for additional features. Gravity has also recruited additional staff to review the user interface and continue engaging with local partners and share their desire to collaborate further with other organizations. It would be of particular interest to follow the development of the solution as the pool of potential employers increases, as well as the number of users and duration of the pilot project.

43 For example, UNHCR’s Biometrics Identity Management System: <https://www.unhcr.org/protection/basic/550c304c9/biometric-identity-management-system.html>

44 For example, see here for further information on UNHCR’s use of IrisGuard: <https://www.unhcr.org/registration-guidance/chapter3/registration-tools/>

45 Cheesman, M. “Self-Sovereignty for Refugees? The Contested Horizons of Digital Identity, Geopolitics, October 2020.

46 Thakur, S. “Results from the field: Improving livelihood prospects for refugees through decentralized identity in Gaziantep, Turkey”, Medium, 14 January 2021.

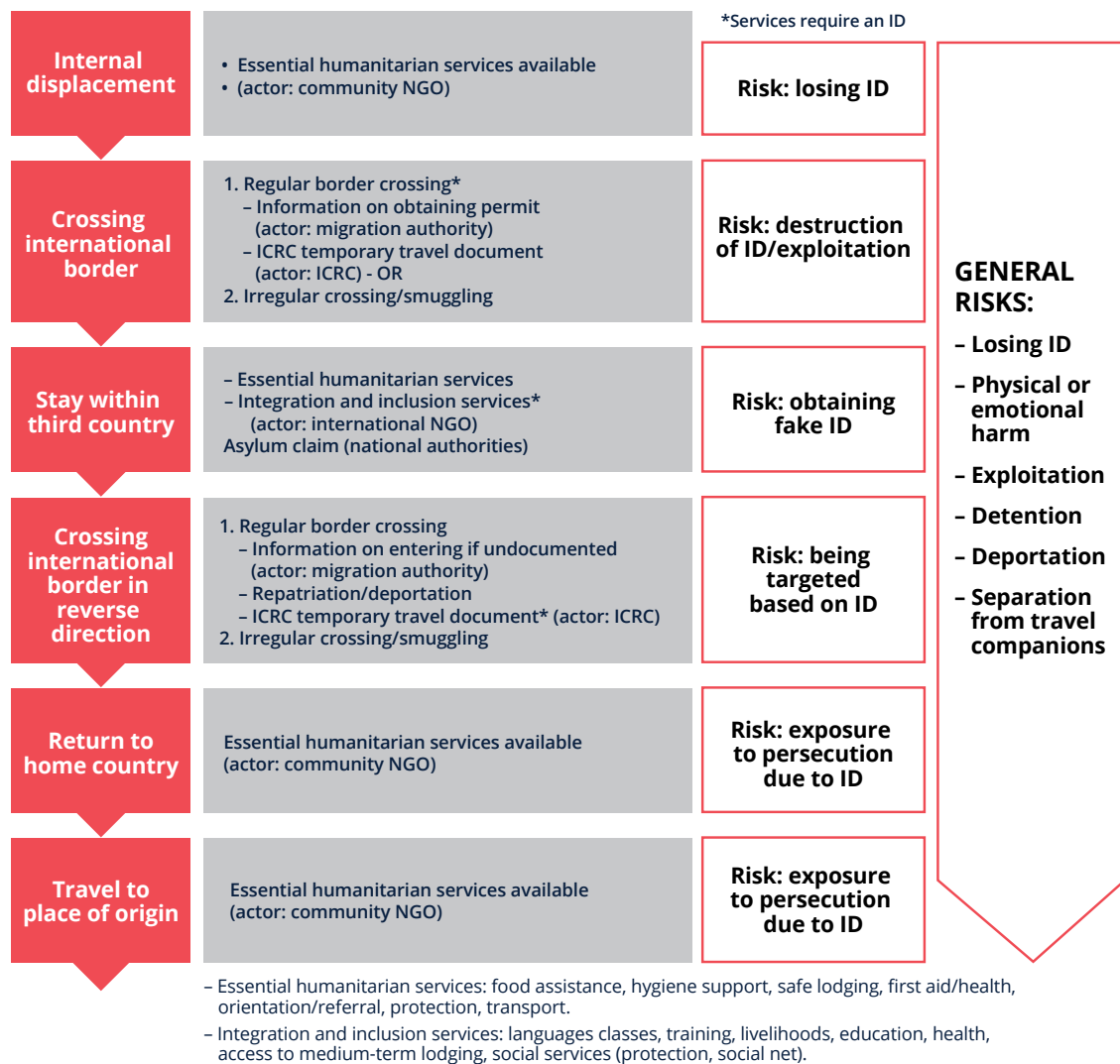
APPENDIX III: USER JOURNEYS

Two user journeys have been designed to map how a migrant may access humanitarian assistance and to identify their interactions with identity, as well as the related risks in doing so. These journeys, developed from discussions with stakeholders, are intended to inform the eventual solution design, enabling a more user-centric approach.

1. Migrant user journey 1: travelling across borders and returning

The first high-level user journey outlines the key steps taken by a migrant during their journey, incorporating multiple scenarios of internal displacement, border crossing, temporary settlement in a third country, and return to their place of origin. At each stage, the journey identifies the types of humanitarian services possible, the actor that might be providing them and the potential risks faced by the migrant related to identity.

User journey – Migrant returnee scenario



2. Migrant user journey 2: receiving health assistance at a humanitarian service point

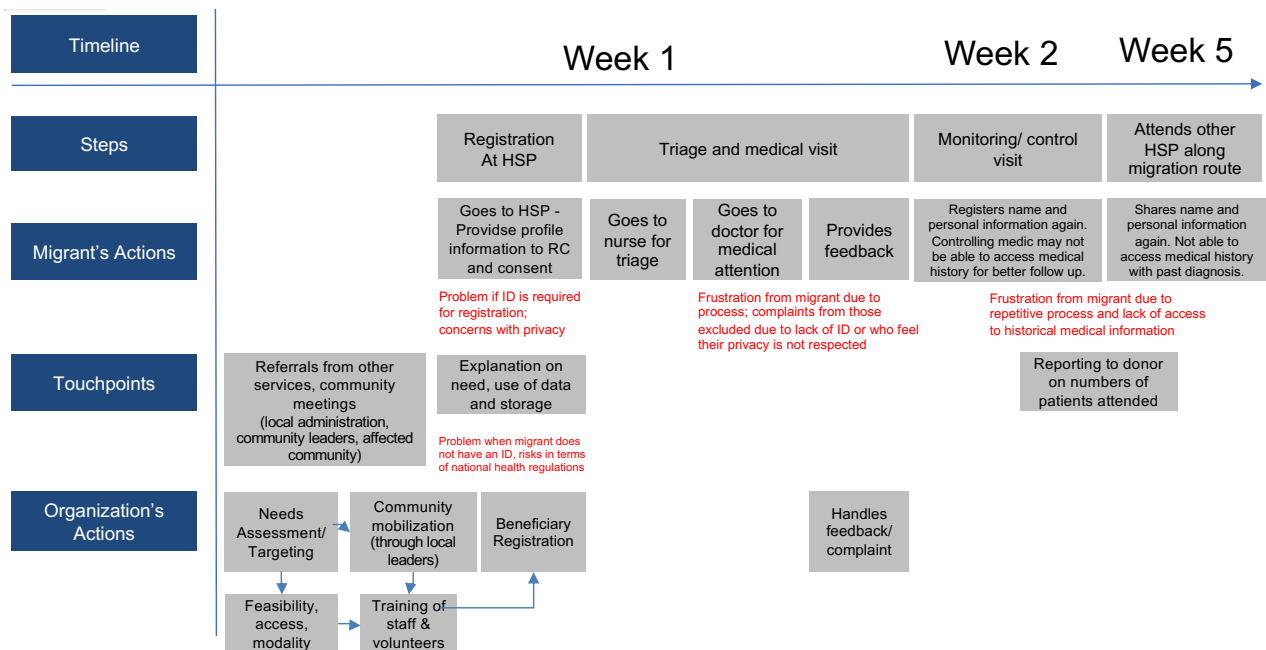
This second user journey outlines the key steps often taken by a migrant in accessing a health service at a humanitarian service point (HSP) against a general timeline, setting out the key steps of the humanitarian service provision, the actions taken by the migrant, particular touchpoints and pain points when the migrant receives the services, and the parallel actions taken by the humanitarian organization in providing the service.

Challenges with Identity – health assistance



Persona: Alpha

Scenario: Provision of health assistance to migrant at a humanitarian service point (HSP).



APPENDIX IV: USER PERSONAS

Four user personas were also developed to inform the design process, based on migrant profiles and experiences shared during the consultation process. The user personas incorporate migrants' contexts, their personal profiles, their vulnerabilities and complaints, their current motivations and core needs, and their pain points related to identification. These migrant user personas are intended to serve as a reference point to test the development of the eventual solution as it progresses, and ensure that it addresses the needs of users.

The four user personas are spread across four continents, and represent people at different stages in their migration journey:

- i. An asylum-seeker waiting for the outcome of their application in a European country
- ii. A migrant transiting through Latin American country, crossing through informal border points
- iii. A migrant returning to their country of origin in East Asia following a period of conflict, currently in a transit country
- iv. An internally displaced person following a natural disaster, within a Central African country.

This allows for a reflection on the evolution of their pain points and needs along their journey depending on where they are in their migration route, and also their different needs for identification.

Migrant persona 1



Alpha: From Middle East

Context: Asylum-seeker waiting for outcome of application in European country

General Profile		Additional Information		Motivations	Pain Points
Age	32	Vulnerabilities	Woman travelling without her husband exposed to security/SGBV threats; no regular source of income; unable to contact her husband regularly; caring for two young children	<ul style="list-style-type: none"> Seeking refugee status in order to be able to access the work market in her profession and earn livelihood Wish to travel to third country to reunite with husband 	<ul style="list-style-type: none"> Lost official ID during journey Difficulty in receiving certain aid because unable to prove identity
Has official ID	No				
Gender	Female	Past Assistance received and from whom	Clothing (received from private individuals), housing assistance (from community shelter), Restoring Family Links (from the National Society), medical assistance (NGO)	<p>Core Needs</p> <ul style="list-style-type: none"> Pay for basic needs & healthcare Need to save money to pay debt owed to family member Save funds to travel and access better work opportunities 	<p>Technology challenges:</p> <ul style="list-style-type: none"> No access to hardware as had to sell mobile phone during journey Connectivity issues in temporary camp Lack of security to possess mobile phone
Marital Status	Married				
Family Size	2	Feedback/Complaints	Lack of access to information, not aware of availability of regular support from humanitarian NGOs, does not often receive aid		
Education	Tertiary education				
Location	Capital city	Level of technological ability	Medium		
Host government	Stretched administrative capacity				
		Mobility	Independent		

Migrant persona 2



Beta: From Latin America

Context: Migrant transiting through Latin American country, crossing through informal border points

General Profile		Additional Information		Motivations	Pain Points
Age	17	Vulnerabilities	Unaccompanied minor exposed to dangers on the road; often joins groups of migrants for security; walking to destination; uncertain as to route; does not want his age to be known so he is not sent to national protection authorities.	<ul style="list-style-type: none"> Insecurity in home country Desire to finalize secondary education and access tertiary education Join his eldest sister in destination country 	<ul style="list-style-type: none"> Receives mostly in-kind and not able to access cash assistance due to age (would have appreciated cash so that he could pay for shelter and transport). Does not trust that humanitarian agencies will not share data with national authorities
Has official ID	Yes – national ID card				
Gender	Male	Past Assistance received and by whom	Food aid, hygiene kit and first aid (National Society), shelter (NGO), protective space (NGO), phone charge and internet access (National Society)	Core Needs <ul style="list-style-type: none"> Basic needs: food, access to hygiene, clothes and shoes Contact his sister through social media or telephone 	<ul style="list-style-type: none"> Technology challenges: <ul style="list-style-type: none"> Mobile: No connectivity on the road, phone battery getting poor, limited access to electricity/difficulty charging.
Marital Status	Single				
Family Size	1	Feedback/Complaints	Not comfortable sharing his identity with NGOs; does not understand why they register so much personal information.		
Education	Secondary	Level of technological ability	Owens a second-hand smartphone. Comfortable with technology.		
Location	Small border town	Mobility	Independent		
Host government	Administrative capacity is high and attending migrant administrative needs;				

Migrant persona 3



Gamma: From East Asian country

Context: Migrant returning to their country of origin following a period of conflict, currently in transit country

General Profile		Additional Information		Motivations	Pain Points
Age	35	Vulnerabilities	His ID has been stolen during his journey, so he is not able to return to his country of origin in a regular manner; as an irregular migrant, he is at risk of sanctions by the host authorities, including deportation. He has not been paid his earnings from his informal work (labour exploitation); has no savings nor contact with his family.	<ul style="list-style-type: none"> Be safely back in his home Return to his family in country of origin Seeking financial and social integration following a long period out of his country 	<ul style="list-style-type: none"> Has no clear view on how to access voluntary repatriation without ID Technology challenges Illiterate and able to use a basic phone
Has official ID	No				
Gender	Male	Past Assistance received and from whom	Food aid, shelter, water (provided by NGO).	Core Needs <ul style="list-style-type: none"> Basic needs: Food, access to hygiene, clothes and shoes Cash to facilitate return Contact with his family 	
Marital Status	Married				
Family Size	6	Feedback/Complaints	Not able to identify an org to provide humanitarian assistance; no access to information on potential support.		
Education	None	Level of technological ability	Can use a basic feature phone.		
Location	Urban	Mobility	Independent		
Host government	Little administrative capacity				

Migrant persona 4



Sigma: From Central African country

Context: Internally displaced person following a natural disaster, within a Central African country

General Profile		Additional Information		Motivations	Pain Points
Age	23	Vulnerabilities	Living in an IDP camp with his family. The camp is in a rural border area, no clear access to humanitarian support; speaks local dialect and has a poor knowledge of official country language	<ul style="list-style-type: none"> Return home and tend to his flock Enrol children in primary school 	<ul style="list-style-type: none"> Unable to communicate easily with national NGOs due to language barrier; does not understand when they ask him to sign documents Unable to access or use hardware or internet Originates from a border area and as a pastoralist, he regularly moves across traditional lands; has no documental proof to show he is a national of that country, rather than the neighbouring one, in order to claim ID
Has official ID	No				
Gender	Male	Past Assistance received and from whom	Anti malarial medicines, basic food aid on a very intermittent basis (NGO).	Core Needs <ul style="list-style-type: none"> Basic survival needs in short term Need to access healthcare for unwell father 	
Marital Status	Married				
Family Size	4	Feedback/Complaints	Not able to identify an NGO or national authority to provide consistent humanitarian assistance.		
Education	Primary				
Location	Rural	Level of technology ability	None		
Host government	Overwhelmed by the response to the natural disaster and seeking to attend to several thousand IDPs in rural areas				
		Mobility	Independent		

APPENDIX V: INITIAL CHECKLIST OF KEY RISKS OR ISSUES

Below are some key risks or issues to be determined prior to proceeding with project implementation.

a. Internal ecosystem

- Availability of financial and human resources (time and expertise)
- Ensure sustainability in medium to long term:
 - o political buy-in,
 - o resources,
 - o change management and training needs,
 - o strategy and plan in terms of transition to digital identity solution, including clear definition of digital identity and governance structure
- Risk appetite of implementing organizations

b. Identification of population and context

- Map clear needs of and benefits to the target population, with understanding of users' perspectives.
- Evaluate stability and resilience of the target population.
- Map humanitarian organizations involved in migration response.
- Map humanitarian services available (including duration and frequency of implementation).
- Develop parallel alternative platform for those who wish to opt out.
- Map telephone connectivity and internet coverage (digital ecosystem).
- Survey average literacy and technological literacy, as well as access to digital means, identifying consequent training, hardware and human resources needs.
- Develop clear community engagement strategy to ensure appropriate inclusion.
- Confirm applicable regulatory context and identify risks through a data protection impact assessment (DPIA).

c. Advocacy:

- Ensure buy-in and appetite from involvement with variety of humanitarian organizations involved in response (enable recognition and sectoral interoperability) and potentially other service providers (for example, health or education, to enable cross sector interoperability).
- Ensure frequent communications with national and local authorities with clear understanding of organization's humanitarian mandate/auxiliary role in the case of a National Red Cross or Red Crescent Society, ensuring host government non-objection.



Pendular migrants using informal crossing point to walk from Colombia to Venezuela, April 2019. Photo credit: Nadia Khoury, IFRC

THE FUNDAMENTAL PRINCIPLES OF THE INTERNATIONAL RED CROSS AND RED CRESCENT MOVEMENT

Humanity

The International Red Cross and Red Crescent Movement, born of a desire to bring assistance without discrimination to the wounded on the battlefield, endeavours, in its international and national capacity, to prevent and alleviate human suffering wherever it may be found. Its purpose is to protect life and health and to ensure respect for the human being. It promotes mutual understanding, friendship, cooperation and lasting peace amongst all peoples.

Impartiality

It makes no discrimination as to nationality, race, religious beliefs, class or political opinions. It endeavours to relieve the suffering of individuals, being guided solely by their needs, and to give priority to the most urgent cases of distress.

Neutrality

In order to enjoy the confidence of all, the Movement may not take sides in hostilities or engage at any time in controversies of a political, racial, religious or ideological nature.

Independence

The Movement is independent. The National Societies, while auxiliaries in the humanitarian services of their governments and subject to the laws of their respective countries, must always maintain their autonomy so that they may be able at all times to act in accordance with the principles of the Movement.

Voluntary service

It is a voluntary relief movement not prompted in any manner by desire for gain.

Unity

There can be only one Red Cross or Red Crescent Society in any one country. It must be open to all. It must carry on its humanitarian work throughout its territory.

Universality

The International Red Cross and Red Crescent Movement, in which all societies have equal status and share equal responsibilities and duties in helping each other, is worldwide.



The International Federation of Red Cross and Red Crescent Societies (IFRC) is the world's largest humanitarian network, with 192 National Red Cross and Red Crescent Societies and around 14 million volunteers. Our volunteers are present in communities before, during and after a crisis or disaster. We work in the most hard to reach and complex settings in the world, saving lives and promoting human dignity. We support communities to become stronger and more resilient places where people can live safe and healthy lives, and have opportunities to thrive.

Follow us:

www.ifrc.org | twitter.com/ifrc | facebook.com/ifrc | instagram.com/ifrc | youtube.com/user/ifrc | tiktok.com/@ifrc