Report: Initiating the co-development of IFRC's Digital ID strategy

June 2021

Authors: Emrys Schoemaker

with Paul Currion, Julia Zomignani Barboza, Lina Jasmontaite, Millie Womble And Boluwatife Ajibola

Introduction

This report was developed based on the contributions and inputs of Red Cross Red Crescent Movement participants that came together to initiate the co-development of the IFRC's Digital ID strategy. The report documents the steps taken in this initial phase and planning for next steps in this process. The body of the report contains the conclusions of a literature review, a summary of two workshops (22nd and 24th June 2021) exploring experiences related to Digital ID internal and external to the movement, and Recommendations for future action. The full literature review and workshop reports are included as Annexes.

The IFRC's Agenda for Renewal positions the IFRC secretariat for more effective global coordination and leadership to ensure the IFRC network addresses five global challenges, one of which is "Migration and Identity", and the areas for transformation reflected in the IFRC Strategy 2030. The "Migration and Identity" strategic priority will 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 the support to migrants along major migratory routes and cycles to ensure that their humanitarian needs are addressed through essential services and protection irrespective of their legal status, in both emergency and non-emergency contexts.

Additionally one of the flagship initiatives of the IFRC is to scale up Cash and Voucher Assistance (CVA) targeting 50% of humanitarian assistance delivered using CVA by 2025. Identity is a crucial element when providing cash assistance using Financial Service Providers (FSP) due to regulatory requirements such as "Know Your Customer" (KYC) making it mandatory to verify the identity of clients by providing an official ID; those with no such ID's are therefore made more vulnerable.

The IFRC's Digital Transformation Strategy also provides a broader context for this work. The Digital Transformation Strategy intends to develop and implement a standard for the digital delivery of humanitarian assistance in line with the IFRC's fundamental principles and by National Societies. The focus is on strengthening the delivery of humanitarian services, and therefore prioritises investments to improve the relevance, speed, quality, accessibility and resilience of humanitarian services, as well as increasing the sustainability of the IFRC's humanitarian mandate and with it, performance, technical, social, and resource accountabilities. A core enabler for the Digital Transformation Strategy is improving IFRC's capacity for interoperability and common data standards - while the Strategy does not mention Digital ID specifically, this goal highlights the importance of digital ID to achieving the Digital Transformation Strategy's objectives.

A number of initiatives within the movement further reflect the interest in digital identity:

- Dignified Identities in cash programming (DIGID) is led by the IFRC, who in partnership with the Norwegian Red Cross has been leading technical implementation. DIGID was funded by Innovation Norway in 2018 under the governance of a consortium of the Norwegian Red Cross, Norwegian Refugee Council, Norwegian Church Aid, and Save

the Children Norway. Innovation Norway has agreed to continue support to DIGID II, specifically addressing the needs of vulnerable migrants to receive essential services in a dignified manner, which will kick-off in January 2021.

- Through its Humanitech initiative the Australian Red Cross has been exploring the application of Digital ID to allow volunteers to manage their own training and development credentials within and between organizations, in order to facilitate mobility of volunteers and to improve due diligence regarding qualification. They have initiated the creation of the Trust Alliance to collaborate with humanitarian, academic and technology groups to research and develop an ethical and trustworthy digital identity ecosystem.
- The 121 Platform has been tested in the Netherlands by the 510 initiative of the Netherlands Red Cross, and is being piloted in partnership with the Kenya Red Cross, allowing targeted communities to self-register and get a digital credential to receive cash assistance.

The IFRC is planning a phased approach to develop a Digital ID strategy that will help guide the Federation's work, but also provide a model that National Societies will be able to build on for their own organizations. This report documents the first steps in bringing stakeholders together to support the development of this strategy.

Literature Review Conclusions

The full Literature Review is available as Annex A. It concludes by highlighting the advantages and disadvantages of Digital ID identified in the literature.

Advantages:

- **Giving beneficiaries more control over their data**: moving digital identities closer to self-sovereign identities may allow beneficiaries to have more access and control over their data including by deciding whom they want to share data with and which data they wish to share (Khoury 2021; *Kenya Digital ID Workshop Summary* 2019).
- **Facilitating access to services**: a digital identity could allow beneficiaries to easily present credentials to any organisation that requires them to provide a service.
- **Ensuring continuity**: a digital identity that allows the user to store data on previously received services, medical history or other crucial information can speed up and facilitate registration with multiple service providers, allowing them to provide tailored services and ensure continuity and complementarity (Khoury 2021).
- **Prevent survey fatigue**: being able to share registration information through a digital identity system allows beneficiaries to register with multiple organisations without having to repeatedly provide the same data. This can prevent traumatic experiences that re-living a difficult story may involve (Khoury 2021).
- **Increased efficiency for organisations**: as mentioned above, digital identities that can be shared between or accessed by multiple humanitarian organisations can facilitate registration and allow complementarity of services, which will consequently increase efficiency and the quality of the services provided (Khoury 2021). Furthermore, digital ID schemes can inform and facilitate data-driven decision-making processes to design and deliver programmes that address the needs of the populations they serve *(USAID* 2017).
- **Accountability and tracing of aid provided**: data about who has received services and assistance can help identify who may need additional outreach, which services are valued, and where services might be combined for greater efficiency (*Identity in a digital age: Infrastructure for inclusive development* 2017). It may be also used for accountability purposes in response to queries about programming efficiency.

Challenges, in turn, may include:

- **Lack of integration and interoperability**: often, humanitarian programmes (e.g. cash transfer programmes) will require beneficiary identification to be shared between aid and non-aid organisations. In practice, IFRC reports that interoperability can be challenging to achieve as it depends on a multitude of actors working in different fields, willing to work together and deploying the required technology to do so (Slavin, Putz & Korkmaz 2021). Furthermore, it requires organisations to set up agreements on data sharing, which may be an added challenge given different organisational policies and practices (*Kenya Digital ID Workshop Summary* 2019). Some have suggested that interoperability could be achieved if organisations agreed on standards concerning technical data formats and operational processes, legal agreements, and governance mechanisms (Schoemaker, Currion & Pon 2018).
- **Compliance with host governments policies and applicable legal frameworks**: government policies have proved to be “the single most significant determinant of formal refugee identity, both in terms of policy frameworks (e.g., the legal status of displaced

people) and political will (e.g., the type and amount of resources committed to their support)" (Schoemaker, Currion & Pon 2018).

- **Integration of humanitarian principles**: humanitarian organisations approach to Digital ID should be compliant with humanitarian principles (Zomignani Barboza, Jasmontaitė-Zaniewicz & Diver 2020; Goodman et al. 2020). Humanitarian organisations should conduct a holistic assessment of compliance with humanitarian principles.
- **Overcoming limited digital literacy**: Digital ID systems may require digital literacies that both beneficiaries and staff members of humanitarian organisations may not have - requiring long and costly trainings. Similarly, digital literacy and training campaigns may need to be offered to beneficiaries, who are not tech-savvy (Slavin, Putz & Korkmaz 2021).
- **Minimising risks associated with personal data processing**: "data protection and privacy considerations are critical in designing digital ID solutions particularly for the humanitarian sector where potentially sensitive data of the most vulnerable are at stake." (*Kenya Digital ID Workshop Summary* 2019, p. 3). Complex legal processing justification and onerous compliance requirements complicate humanitarian organisations capacity to minimise the risks of personal data processing. The IFRC's Policy on the Protection of Personal Data summarises many of these justification and requirements.
- **Establishing reliable and trustworthy partnerships**: when developing digital identity systems, humanitarian organisations may partner with governments, community-based organisations and the private sector (e.g. tech companies) to design and deploy the concerned solutions. Such partners, however, may have different goals and objectives in mind, which may conflict with the humanitarian objectives of the digital identity solution (Slavin, Putz & Korkmaz 2021) - complicating the ability of humanitarian actors to control all the processing activities involving beneficiaries' data (Kuner and Marelli 2020), and may even, in the case of some donors, require organisations to compromise their commitments to personal data protection (Slavin, Putz & Korkmaz 2021).
- **Ensuring continuous and stable access to connectivity**:. In some of the settings where humanitarian organisations work, however, connectivity may not always be available.
- **Ensuring trust and acceptability of digital identity solutions**: in some situations, beneficiaries of humanitarian assistance may not wish to be identified. For example, migrants may fear that personal information may fall into the hands of authorities in their countries of origin or reveal information such as their ethnicity, which could lead to discrimination (Khoury 2021).
- **Building on relevant experiences and lessons from the use of personal data in other sectors:** Goodman et al. (2020) suggest that humanitarian sector, when developing management information systems, should build on the learnings of personal data collection in other contexts concerning health, social, political, commercial, security, and military applications.

Workshop Summary

Staff of IFRC Secretariat and National Societies, with guest participants from organizations such as the ICRC and World Vision, participated in two workshops exploring the importance of digital Identity for the IFRC. The purpose of the workshops was to start the process of establishing a common vision, strategy and policies for digital identity. Full workshop reports are provided in Annex C; this summary outlines key themes that emerged from the two workshops.

Policy Matters
During the first workshop participants agreed that creating a common policy framework is essential for IFRC to establish a coherent approach to digital ID. Participants highlighted that this is complicated by the challenges around building an institutional framework for the use of digital technology; and that there is a push for more strategic conversations to promote data minimization and data protection by design, including with donors. Clear challenges to accomplishing these steps were identities by participants, including the core challenges of standards and governance. One IFRC participant asserted that *'tech is fast, humans are slow'*, which spoke to how standards and policy need to accommodate rapid change yet also maintain the core principles of the IFRC, while also being sensitive to the impact on politics and power.

IFRC Principles as a Guiding Lens
The second workshop explored how IFRC's seven Fundamental Principles could serve as the foundation for a possible vision of digital ID. In addition to the application of the principles to digital ID design, participants also discussed how a coherent approach to digital ID could serve wider institutional commitments. For example, participants discussed how digital ID could uphold the principle of independence by protecting National Societies' independence from state institutions, and the principle of universality by promoting interoperability. IFRC volunteers could use digital ID to avoid becoming dependent on a single organisation, allowing them volunteers to move across borders and between organizations; and affected communities themselves could achieve some independence from the IFRC itself, which some participants asserted is the overall goal of the organization.

IFRC as a 'humanitarian organization' or a 'data company'
There was widespread discussion of the potential for digital ID to a) protect the vulnerable from risks and b) enable IFRC to use data to strengthen operations; participants were challenged to discuss whether these two goals were compatible. Participants noted that the objectives of humanitarian and technology organisations were not necessarily aligned; data-driven technology providers must exploit data, while humanitarian organisations prioritise serving and protecting the most vulnerable. The ICRC handbook on data protection highlights the importance of data minimisation and the legitimate bases for using data, highlighting tension between data use and data protection.

Participants also discussed whether and how IFRC has the potential to be a 'neutral' identity provider within the wider humanitarian sector. IFRC was viewed as already being an identity *provider* given the capturing, storing and processing of individual data, while others suggested

that IFRC should be an identity *enabler*, providing the means for individuals to be their own provider. Participants highlighted that one way of mitigating risk was to limit IFRC's identity provision to a functional ID that limits the need for recipients' personal data. These discussions highlight the importance of IFRC deciding an approach to digital ID which, amongst other things, addresses the tensions between being a humanitarian organisation and a technology provider.

Data protection

Participants raised concerns that the IFRC, in pursuit of its digital ID vision, needs to maintain its commitment to 'keep beneficiaries at the centre' of how their data is collected, processed and managed securely. An IFRC participant highlighted the two data protection pillars of necessity and proportionality as critical lenses through which digital identity and data privacy can be assessed. Participants expressed concern about organisational capacity to manage data, particularly to prevent leaks, describing how humanitarian actors have limited understanding of risks around data protection, and how government restrictions around data access also limit humanitarian service delivery. Some countries adopt centralised identification systems, some of which are criteria to accessing state services, such as India's AAdhaar, Norway's National Identity Number or Kenya's Huduma Namba.

Participants discussed the use of blockchain technologies for resolving some ID related issues encountered by National Societies, including avoiding duplication of data collection and mitigating risks of centralised data storage. However they recognised that blockchain technologies have their own issues, such as identifying suitable use cases and meeting data processing requirements. Aid recipients may also have difficulty to understand the technology, challenging the humanitarian principle of 'informed consent' – as how can people consent to the use of their data if they don't understand how their data is processed and used?

Conclusion

The workshop discussion highlighted the rich experiences of IFRC staff, the diversity of positions, perspectives and needs around digital ID, and the potential for IFRC foundational principles to act as a shared framework for an organisation-wide approach to digital ID. This approach is more likely to be established on the basis of shared foundational principles and shared organisational norms than Federation-wide adoption of any single digital ID system or technology. IFRC's unique decentralised institutional structure, it's scale and its unique role mean the organisation has a unique opportunity to set an example for the humanitarian sector's approach to digital ID.

Workshop Conclusions

1. The workshops revealed both depth and breadth of experience, suggesting that the foundation exists for IFRC to develop a unique approach to Digital ID; however this experience is distributed and does not yet form a basis for collective action.
2. Rather than focusing on technological solutions, the IFRC needs to collectively understand better the specific problems that Digital ID might help to solve - and the associated challenges.

3. There was also an agreed need to take a problem-focused approach, particularly from the perspectives of beneficiary communities, and especially in order to avoid being distracted by new technologies that may be a good fit to those problems.
4. Participants recognised that it would be difficult to establish dedicated platforms that could work across the entire Federation for most of the thematic areas discussed in the workshop, due to the varying requirements and capacities of National Societies.
5. The workshops suggested that collectively IFRC could view Digital ID from the perspective of how to manage personal data, rather than how to build systems, moving attention away from specific platforms and towards shared principles.
6. The workshops further suggested that there is a higher chance of successfully addressing the challenge of Digital ID by taking an approach that is grounded in clear principles and organisational norms that could be adopted across the Federation.
7. Participants then suggested that framing digital ID as data management would enable it to be positioned more effectively within broader Federation initiatives, such as Strategy 2030, Digital Transformation strategy, and so on.
8. There are two challenges ahead: the first is to bring this varied and distributed experience together to form a coherent IFRC position; the second is to build the necessary consensus to adopt and promote that position across the Federation.

Workshop Recommendations

The two initial workshops were not designed to generate specific recommendations for the IFRC, but to scan the experience which currently exists within the movement and to generate a future-focused consensus around the need to develop a more coherent approach.

A clear vision for the future will require further collective work, but the workshops have established that there is wide engagement with the question of digital ID, which creates the potential for the IFRC to develop a distinct approach to digital ID which could

a. Ensure adherence to the Federation's Fundamental Principles
b. Enable better performance across the Federation and within National Societies
c. Contribute to more responsible digital ID practices across the humanitarian sector

We recommend that IFRC follow up the workshops with a phased approach based on achievable goals, framed within a clear vision for the future of digital ID in IFRC. This vision will need to be clearly positioned within IFRC's existing frameworks, e.g. Strategy 2030, and inform any future digital transformation initiatives.

Every step in this process must be designed to establish and expand engagement, beginning from a core within the IFRC and expanding to include more stakeholders as it progresses. Establishing the core is important in order to prevent any changes in the goals and to mitigate any impact on the process through the inclusion of more stakeholders.

We recommend that this process begins with the following steps:

- Conduct a mapping exercise, initially based on workshop participation, to establish the core stakeholders that are essential for any work on Digital ID to move forward. The mapping should help to allocate resources (including time) to the exercise in order to make the most rapid progress.
- Establish a core vision statement for IFRC's approach to Digital ID, grounded in the IFRC Fundamental Principles. This vision should be based on stakeholder insight and support but also the insights and needs of disaster affected communities based on the experience of IFRC and others.
- Build a core of expertise based on the two previous exercises, recognising and promoting specific stakeholders within IFRC as resources for the entire movement, and linking those individuals through established IFRC methods (i.e. working group, knowledge network, or whatever is appropriate).
- Identify 3 specific issues or themes that have particular relevance for Digital ID within IFRC, and work with the core group to publish relevant internal documents and external publications in order to clearly position the development of Digital ID within wider IFRC and sectoral discussions.
- Frame these activities as a process of establishing organisational norms rather than technical standards.[1] It is easier to turn Fundamental Principles into norms rather than standards; and although norms take longer to establish and are more vague, they are often better at guiding organisational behaviour than standards.

[1] For example, instead of trying to make a commitment to open source software a requirement across the Federation, based on policy documents and enforcement mechanisms, promote the idea that open source software is a better fit with the fundamental principles, based on peer pressure (by providing examples of current projects within the movement that work on an open source basis).

Annexes

Annex A - Literature Review

LITERATURE REVIEW:
DIGITAL IDENTITY IN THE HUMANITARIAN SECTOR AND BEYOND

1. Introduction

"Being able to prove one's identity has increasingly become a prerequisite for accessing many services across the public and private sectors." (Slavin, Putz & Korkmaz 2021, p. 3) According to the Kenya Red Cross Society (KRCS), these may include voting, setting up a bank account, registering a business, purchasing land, enrolling in school, receiving social security benefits and even humanitarian assistance (KRCSa). However, there are still many who do not possess identity documents[1] and thus are unable to benefit from existing services. Different initiatives have tried to bridge this gap but, according to the Dignified Identities (DIGID) in cash programming project, identity management remains one of the biggest challenges, including for humanitarian action (DIGIT Consortium 2021).

While identification documents are often facilitated by paper credentials, initiatives to digitalise identification are increasing both in the public and private sectors. Some of the reasons behind these initiatives are the claimed benefits of digital identities, such as greater efficiency in processes and more focus on the provision of aid (and services) rather than on the registration of a person (Slavin, Putz & Korkmaz 2021). In practice, a digital identity (or digital ID) is essentially a form of electronic identification that provides unambiguous assurances as to the individual's identification. Depending on the function of such digital identity solutions, they may be considered foundational or functional. **Foundational identity** is one that aims to reliably prove someone's identity, thus granting them access to a wide range of services. Government issued foundational identities are the most authoritative form of identity (IFRC and KRCS 2019). **Functional identities**, in turn, are those that aim to provide its user access to one specific service (such as cash assistance). Most of the digital identity solutions that exist in the humanitarian sector are of the second kind. Some governments, however, have started programmes to digitalise foundational identities, as explained below

The COVID-19 pandemic accelerated the change toward digital solutions, as physical interactions were limited throughout a great part of the world to contain the spread of the virus. Indeed, the World Bank, which has been involved in digital identity initiatives since before COVID, extended their reach and funding of projects in this field during the pandemic (Cornish 2020). At the same time, with the evolution of the pandemic and the development of vaccines, new digital measures arose such as the so-called green certificate in the European Union (EU), which aims to provide a digital certificate containing a proof of vaccination, recent recovery from the virus or negative test to allow people to travel freely within European borders. Similarly, some States consider implementing immunity passports to allow access to events or specific places during the exit from lockdown phase. The EU debates over the Digital Green Certificate underlined some of the reoccurring issues in the digitalised ID solutions, such as accessibility, discrimination, information security, standardisation, safeguards for protection of personal data and interoperability. Indeed, Privacy International claimed that such type of solutions, especially immunity passports, have been questioned for their lack of scientific basis as well as possible violation of fundamental rights, especially when part of the population may not have access to vaccines or testing (Privacy International 2020). The organisation also pointed the risk of these digital identity initiatives being used beyond their initial purpose, without oversight (Privacy International 2020).

2. Digital ID and longer-term development: the digitalisation trend

As shown above, digitalisation initiatives concerning identification are no longer theoretical ideas but are starting to find their place in private and public projects. According to a report from the International Federation of Red Cross and Red Crescent Societies (IFRC), one of the goals of such initiatives is oftenlinked to the digitalisation of government services such as the transfer of social protection and other benefits (Slavin, Putz & Korkmaz 2021).

Digital ID solutions such as electronic ID-cards enabling the use of digital signatures and providing access to various e-services are widely used across the European Union (EU). These solutions (based on the eIDAS Regulation) are said to have created "the foundation for the development of an identity and trust services market in the EU, supporting the ever-increasing need for secure digital transactions" (European Commission 2021; 77). Recognising the limitations of the current approach to ensure cross-border and cross sector interoperability of trust services and building on emerging market trends such as Microsoft and Apple's work on different solutions that could result in a default standard for digital IDs, the European Commission's proposal on a European Digital Identity claims that it seeks to further the use of digital identities that shift the focus from the provision and use of rigid digital identities to the provision and reliance on specific attributes related to those identities (European Commission 2021; European Commission 2021a). According to the proposal, built as a digital wallet, these attribute-based digital IDs could potentially improve the efficiency of and trust on services provided across the EU, both in the private and the public sectors (European Commission 2021a). It could also allow EU citizens to minimise data sharing, especially in private platforms.

In Kenya, government authorities started an initiative – Huduma Namba[2] – to create a biometric registration system for all Kenyan and foreigners residing in Kenya, which would be linked to multiple services such as banking, education and healthcare (IFRC and KRCS 2019). Similarly, in Ukraine, the government launched a smartphone application in which users can obtain a digital version of their documents such as internal ID, passport, driver's license etc. as well as access multiple public services and use the app to update their residence or voting address or pay fines and fees (Kuzemska 2021). For the country's internally displaced population (IDPs), Kuzemska argues that the digitalisation of public services could assist in eliminating lengthy and repetitive in-person procedures, removing the need to travel to register for benefits, and ensuring greater transparency of State databases, potentially helping to fight corruption. However, she also notes that at the moment digitalisation of IDP registration still depends on IDPs obtaining a paper-based registration first as well as considering that most Ukrainian IDPs are elderly and thus less likely to have a high digital literacy, it is questioned whether those benefits could materialise (Kuzemska 2021). Furthermore, Privacy International has argued that these types of initiatives, especially those that require already having a physical document or the ones that only work on smartphones, may in practice lead to exclusion and not inclusion, as not everyone will have the required document in the first place or own the right type of phone to run the application (Privacy International 2020).

3. Wider trends on digital ID: technologies and design choices

As can be seen from the singularities of the different initiatives mentioned above, digital identity solutions may have different purposes and be designed in different ways. Similarly, digital identities are not linked to any specific technologies. They may be designed and deployed in different ways according to their objectives and the function they will serve for their users. For example, digital identity can take varied forms and the information related to them may be stored in a smartcard, be accessible via a bar code, be contained in a mobile phone or other portable device or be stored in the cloud (Clark et al. 2016). The systems used to build it may rely on biometrics to authenticate users or rely on previously registered devices such as personal mobile phones, and even rely on a blockchain for immutability and transparency (USAID 2017).

Some of these technologies have characteristics that have been presented as especially suited for digital identity solutions. For example, in spring 2021, Microsoft announced the public preview for Azure AD verifiable credentials, which, according to Microsoft, would allow organisations to empower users by

controlling credentials and managing access to their personal information. In this regard, Newman mentions that the Microsoft Authenticator app, along with two-factor verification, would provide decentralised verification and sharing of information concerning university transcripts, diplomas, and professional credentials (Newman 2021). Similarly, the decentralised and immutable characteristics of blockchain have been claimed by Jehl to offer the possibility to create immutable digital identity records that would provide greater security from attacks in comparison with centralised databases (which have one single point of failure) and that could be built in a user-centred and thus privacy friendly way (Jehl 2017). However, the Handbook on Data Protection in Humanitarian Action notes that there are multiple challenges to using blockchain in the humanitarian sector, including the fact that the immutability of these ledgers may be an obstacle to beneficiaries wishing to exercise their rights as data subjects as it may not be possible to modify or delete data from a blockchain (Kuner and Marelli 2020).

Apart from different technologies, different design choices can also influence the shape of a digital identity solution. These systems may be entirely controlled by the authority that issues the identification (such as a passport, which can only be issued by a specific authority and will always contain the same information) or grant more control to the user. The latter option (which is closer to what the EU and Microsoft initiatives above seek to achieve) usually takes the form of a digital wallet on a smartphone, which according to an IFRC report, allows the user to control which data are included (in the wallet) and with whom they are shared (Khoury 2021). This could give the user the option to, for example, share only the details strictly necessary to receive personalised aid (e.g. only showing that the person belongs to a pre-determined age group, such as children under 12, to receive a specific vaccine) without providing any other personal information (Kuner and Marelli 2020) such as their full name. In a workshop on digital ID in Kenya, it was mentioned that this would be possible because the user's digital wallet would store multiple credentials (e.g. name, birthdate, belonging to a specific minority group) and thus when requested, the user could only provide the required credential, and not all the information stored in his/her wallet (IFRC and KRCS 2019).

The actual control and ownership that these identity initiatives give to their users, however, has been questioned by Privacy International, who said that identity transactions often have a power asymmetry and thus the user who needs the services will feel like they have no choice but to provide whatever data is asked of them (Privacy International 2020).

4. Digital Identity in the Humanitarian Sector

Beneficiaries of humanitarian assistance are not always required to provide a proof of their identity to receive aid. According to an IFRC report, emergency health services, first aid, shelter, food assistance and family links restoration activities are often done without humanitarian organisations requiring the beneficiary to prove their identity through an official identity document such as a government issued identity card (Khoury 2021). The Handbook on Data Protection in Humanitarian Action says this is because in many cases humanitarian organisations only need to know that a person has a certain attribute that entitles them to participate in a specific humanitarian programme but do not need to know their identity to provide aid (Kuner and Marelli 2020). In these cases, beneficiaries may be asked to register and thus provide their names, but they do not need to provide a document as proof of their identity. This registration may provide them with a form of identification from the organisation, which they may present to access the services (e.g. when UNHCR grants asylum seekers or recognised refugees a card proving they are registered with the agency). This would work as a functional identification, as it allows them to access the specific services of the organisation.

Other services, however, may require a proof of identification. This is especially the case when they involve other partners such as financial institutions or governmental bodies, who may be bound by legal requirements that demand proof of identification to provide services. According to an IFRC report, these services may include, for example, cash transfers, obtaining microcredits, language and training courses, or legal assistance (Khoury 2021). In some cases, the functional identifications provided by aid organisations (as the UNHCR card mentioned above) have been accepted by service providers as a proof of identity (and thus, in practice,

can work as a foundational identity). However, that is not always the case. For example, it has been mentioned by humanitarian actors that migrants have tried using such types of identity to access other services and been denied (Khoury 2021). In practice, digital identity solutions in the humanitarian sector have often been linked to cash transfer programmes (Slavin, Putz & Korkmaz 2021).

Potentially, digital identities in the humanitarian sector could be used for multiple purposes, including to avoid duplication and provide tailored services (Goodman et al. 2020; Kuner and Marelli 2020; Slavin, Putz & Korkmaz 2021). For these goals to be achieved, in the ideal scenario, a humanitarian digital identity would be "interoperable" throughout the sector so that different humanitarian organisations could access the credentials linked to the digital identity (e.g. other humanitarian services the person has accessed), check the issuer of the concerned credentials (e.g. another humanitarian organisation), and extract only the data that is being shared by the owner of the digital identity (Slavin, Putz & Korkmaz 2021; Kuner and Marelli 2020). In this way, as noted by Khoury, members of affected communities could avoid having to register repeatedly (and potentially having to relive trauma as they recount their story), better preserving their dignity (Khoury 2021).

As this level of sophistication has not yet been achieved, the next paragraphs focus on the most common use case, that is, cash transfers. In these cases, humanitarian organisations may engage in efforts to ensure those without an identification document can access cash-assistance. Identification is usually required in these transactions so that financial institutions can comply with the so-called know your customer (KYC) requirements. During a workshop on digital ID in Kenya, multiple actors from the private and public sectors discussed how digital identities could help bridge this gap. The workshop noted that in some situations (referring specifically to the UNHCR cards mentioned above) NGOs could be seen as trust anchors and the identification cards created by them have been leveraged to enable access to services previously only accessible via legal ID. Whether these forms of identification are accepted, however, is context dependent and may be reliant on government approval (IFRC and KRCS 2019). Some guidance can be drawn from the experience of members of the Red Cross and Red CrescentMovement who were involved in such initiatives.

In Kenya, these initiatives include the 121 Consortium Direct Cash Aid and the Dignified Identities (DIGID) in cash programming project. The 121 Consortium, involving multiple partners, explored different aspects of digital identity when registering beneficiaries, including self-sovereign identity, which would shift control over data from the organisations to individual users. However, challenges related to connectivity, available infrastructure, software required, digital literacy and regulations led the consortium to discontinue that latter part of the project (Slavin, Putz & Korkmaz 2021). The DIGID project, in turn, aims to find a solution that would allow those with no recognised identification document to receive cash transfers. The solution would be in the form of a digital wallet, based on a user centred design, to also grant individuals more control over their data. It should be noted, however, that potential users interviewed in the context of the project mentioned that digital identity was a difficult concept to grasp and they would feel safer with a physical identity document due to its tangibility (KRCSa).[3]

5. Advantages and challenges of digital identity: a summary

Based on what has been exposed, it is possible to summarise the advantages and challenges of digital identity in the humanitarian sector as follows.

Advantages may include:

- **Giving beneficiaries more control over their data**: moving digital identities closer to self-sovereign identities may allow beneficiaries to have more access and control over their data including by deciding whom they want to share data with and which data they wish to share (Khoury 2021; IFRC and KRCS 2019).
- **Facilitating access to services**: a digital identity would allow beneficiaries to easily present credentials to any organisation that requires them to provide a service.
- **Ensuring continuity**: a digital identity that allows the user to store data on previously received services, medical history or other crucial information can speed up and facilitate registration with multiple service providers, allowing them provide tailored services and ensure continuity and complementarity (Khoury 2021).
- **Prevent survey fatigue**: being able to share registration information through a digital identity system allows beneficiaries to register with multiple organisations without having to repeatedly provide the same data. This can prevent traumatic experiences that re-living a difficult story may involve (Khoury 2021).
- **Increased efficiency for organisations**: as mentioned above, digital identities that can be shared between or accessed by multiple humanitarian organisations can facilitate registration and allow complementarity of services, which will consequently increase efficiency and the quality of the services provided (Khoury 2021). Furthermore, digital ID schemes can inform and facilitate data-driven decision-making processes to design and deliver programmes that address the needs of the populations they serve *(*USAID 2017).
- **Accountability and tracing of aid provided**: data about who has received services and assistance can help identify who may need additional outreach, which services are valued, and where services might be combined for greater efficiency (USAID 2017). It may be also used for accountability purposes in response to queries about programming efficiency.

Challenges, in turn, may include:

- **Lack of integration and interoperability**: often, humanitarian programmes (e.g. cash transfer programmes) will require beneficiary identification to be shared between aid and non-aid organisations (e.g. humanitarian organisation, financial institution, mobile connectivity provider), which will require a digital identification scheme to be interoperable between all those needing to access it. This is even more true if humanitarian organisations seek to create foundational digital identities, which should be accessible to a vast range of service providers. The Handbook on Data Protection in Humanitarian Action notes, however, that "very few Humanitarian Organizations have the mandate – and therefore the legitimate basis – to develop and deploy foundational systems of this type." (Kuner and Marelli 2020, p. 213). In practice, an IFRC report mentions that interoperability can be challenging to achieve as it depends on a multitude of actors working in different fields, willing to work together and deploying the required technology to do so (Slavin, Putz & Korkmaz 2021). Furthermore, it requires organisations to set up agreements on data sharing, which may be an added challenge as their programmes may have different donor requirements or they may follow strict organisational policies and also may not be willing to trust all the data gathered by others, as data collection models can differ between organisations (IFRC and KRCS 2019). To counter some of these challenges, it has been suggested that interoperability could be achieved if organisations agreed on standards concerning technical data formats (e.g. the use of XML or JSON) and operational processes, legal agreements, and governance mechanisms (Schoemaker, Currion & Pon 2018).
- **Compliance with host governments policies and applicable legal frameworks**: government policies have proved to be "the single most significant determinant of formal refugee identity, both in terms of policy frameworks (e.g., the legal status of displaced people) and political will (e.g., the type and amount of resources committed to their support)" (Schoemaker, Currion & Pon 2018). Government policies shape the way in which, if at all, State-based identity systems interact with the humanitarian response, be it for refugees or other beneficiaries. For example, in Uganda the government has mandated health centres in refugee camps to adhere to the same data management practices as government-run health clinics (Schoemaker, Currion & Pon 2018).
- **Integration of humanitarian principles**: due to the humanitarian sector's mission to carry out assistance, relief and protection operations in an impartial manner that does not cause harm to beneficiaries, it has been claimed to be essential that the humanitarian principles are also complied with (Zomignani Barboza, Jasmontaitė-Zaniewicz & Diver 2020; Goodman et al. 2020). The authors defending this idea argue that before deciding on the use of a certain solution, humanitarian organisations, in addition to compliance with legal requirements, should conduct a holistic assessment of compliance with humanitarian principles, such as humanity, impartiality, independence and 'do no harm'.
- **Overcoming limited digital literacy**: a shift into digital identities may require both beneficiaries and staff members of humanitarian organisations to start using specific technological solutions they are not familiar with. For staff members, implementing digital identity solutions may require long and costly trainings. Similarly, digital literacy and training campaigns may need to be offered to beneficiaries, who are not tech-savvy (Slavin, Putz & Korkmaz 2021). It is, however, debated whether governments or NGOs should be in charge of beneficiary education concerning the use of digital identity.

- **Minimising risks associated with personal data processing**: "data protection and privacy considerations are critical in designing digital ID solutions particularly for the humanitarian sector where potentially sensitive data of the most vulnerable are at stake." (IFRC and KRCS 2019, p. 3) A particular challenge in this regard, as mentioned in the Handbook on Data Protection in Humanitarian Action, is the legal basis to process beneficiaries' personal data in a digital identity solution. While some services such as urgent medical care may be based on the vital interest of the data subject – in this case, the beneficiary – other services may rely on consent, which, as mentioned above, may not always be freely given since beneficiaries may feel compelled to give access to their data, as otherwise they will not be able to obtain the desired services (Kuner and Marelli 2020). Instead, organisations providing humanitarian assistance may rely on public interest or other legal ground as the legal basis for a programme that provides foundational identity credentials (Kuner and Marelli 2020). It is also important to note that complex data protection legislations, such as the General Data Protection Regulation EU/679 (GDPR), which is being recognised as the gold standard for data protection (Zomignani Barboza, Jasmontaitė-Zaniewicz & Diver 2020) can impose numerous requirements (e.g. data protection impact assessments and personal data breach notifications) for the processing of personal data by humanitarian organisations operating in the European Economic Area (EEA). The influence of these legal text in the humanitarian sector can be illustrated by the IFRC's Policy on the Protection of Personal Data, which reflects many GDPR provisions.
- **Establishing reliable and trustworthy partnerships**: when developing digital identity systems, humanitarian organisations may partner with governments, community-based organisations and the private sector (e.g. tech companies) to design and deploy the concerned solutions. Such partners, however, may have different goals and objectives in mind, which may conflict with the humanitarian objectives of the digital identity solution (Slavin, Putz & Korkmaz 2021). In this regard, the Handbook on Data Protection in Humanitarian Action notes that when working with partners, humanitarian actors will not be able to control all the processing activities involving beneficiaries' data and thus may not be able to prevent, for example, partners using beneficiaries' data for advertising or other non-humanitarian purposes (Kuner and Marelli 2020). It has also been noted that, in some cases, donor funding may require organisations to compromise their commitments to personal data protection (Slavin, Putz & Korkmaz 2021). Furthermore, "[O]rganizations may also be unwilling to engage with some private-sector partners because of the reputational risk that doing so can carry." (Kuner and Marelli 2020, p. 269).
- **Ensuring continuous and stable access to connectivity**: digital identities often require internet connection to function properly and thus require their users to be constantly connected. In some of the settings where humanitarian organisations work, however, connectivity may not always be available. For example, after natural disasters, such as floods or earthquakes, when connectivity infrastructure may have been damaged.
- **Ensuring trust and acceptability of digital identity solutions**: in some situations, beneficiaries of humanitarian assistance may not wish to be identified. For example, migrants may fear that by providing identification information to humanitarian organisation, this information may fall into the hands of authorities in their countries of origin, leading to persecution of their family members or of themselves upon return. Similarly, beneficiaries may fear that their identity will reveal information such as their ethnicity, which could lead to discrimination (Khoury 2021).

- **Building on relevant experiences and lessons from the use of personal data in other sectors:** Goodman et al. (2020) suggest that humanitarian sector, when developing management information systems, should build on the learnings of personal data collection in other contexts concerning health, social, political, commercial, security, and military applications. It is suggested that by doing so, humanitarian organisations could potentially avoid further exclusion, marginalisation and political polarisation (Goodman et al. 2020).

Bibliography

- (Clark et al. 2016) Clark, J, Dahana, M, Desaia, V, Iencob, M, Labriollec, S, Pellestorc, J P, Reidb, K & Varuhakic, Y 2016, *Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation*, GSMA, World Bank Group and Security Identity Alliance, Washington, viewed 21 June 2021, < https://documents1.worldbank.org/curated/en/600821469220400272/pdf/107201-WP-PUBLIC-WB-GSMA-SIADigitalIdentity-WEB.pdf>.
- (Cornish 2020) Cornish, L 2020, 'Digital IDs during COVID-19: How is the debate changing?' *Devex*, 10 November, viewed on 21 June 2021, < https://www.devex.com/news/digital-ids-during-covid-19-how-is-the-debate-changing-98481>.
- · (DIGIT Consortium 2021) *Dignified ID's: Invitation to a Dialogue (summary)* 2021, DIGIT consortium, viewed on 21 June 2021, <https://static1.squarespace.com/static/5b75620445776e4b290c0d96/t/5c6a857fa4222f337826e6e5/1550484865704/Executive+Summary+%282%29.pdf>.
- (European Commission 2021), European Commission 2021, *Staff Working Document on the evaluation of Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS) {COM(2021) 290 final} - {SEC(2021) 229 final}*, Publications Office of the European Union, viewed 21 June 2021 <https://op.europa.eu/en/publication-detail/-/publication/00dfddeb-c449-11eb-a925-01aa75ed71a1/language-en/format-PDF/source-212313796?cookies=disabled>.
- (European Commission 2021a) European Commission 2021, *Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity {SEC(2021) 228 final} - {SWD(2021) 124 final} - {SWD(2021) 125 final}*, EUR-Lex, viewed 21 June 2021, <https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:52021PC0281&cookies=disabled >.
- (Goodman et al. 2020) Goodman, R, Shoemaker, E, Messenger, C, Steller, R 2020, *Review and analysis of identification and recurrent crises, External briefing note*, UK aid, London, viewed 21 June 2021, <https://www.dai.com/uploads/bsic-MIS-2020.pdf>.
- (IFRC and KRCS 2020) *DIGID Project - User Consultation Report* 2020, IFRC and KRCS, viewed 21 June 2021, <https://static1.squarespace.com/static/5b75620445776e4b290c0d96/t/603d14c5775eed6fbde2883b/1614615753940/%5BFinal%5D+DIGID+Kenya+User+Consultation+Report.pdf>.

- (IFRC and KRCS 2019) *Kenya Digital Id Workshop Summary* 2019, International Federation of Red Cross and Red Crescent Societies (IFRC) and Kenya Red Cross Society (KRCS), viewed on 21June 2021, < https://www.adelaide.edu.au/writingcentre/sites/default/files/docs/harvard-referencing-guide.pdf> .
- (Jehl 2017) Jehl, L E 2017, 'Blockchain – The Future of Digital Identity?' *Bloomberg Law*, viewed 21 June 2021, <https://bakerlaw.com/webfiles/Privacy/2017/Articles/12-13-2017-Jehl-BNA-Blockchain.pdf>.
- (Khoury 2021) Khoury, N 2021, *Digital Identity: Enabling Dignified Access to Humanitarian Services in Migration*. International Federation of Red Cross and Red Crescent Societies, Geneva, viewed 21 June 2021, <https://preparecenter.org/wp-content/uploads/2021/06/Digital-Identity-Enabling-dignified-access-to-humanitarian-services-in-Migration-Final.pdf>.
- (KRCSa) *Consulting communities for digital identities for humanitarian cash assistance,* Kenya Red Cross Society, viewed on 21 June 2021, <https://www.redcross.or.ke/index.php?option=com_content&view=article&id=%27372%27>.
- (Kuner and Marelli 2020) Kuner, C and Marelli, M (eds) 2020, *Handbook on Data Protection in Humanitarian Action*, 2nd edn, International Committee of the Red Cross, Geneva, viewed 21 June 2021, <https://shop.icrc.org/download/ebook?sku=4305.01/002-ebook>.
- (Kuzemska 2021) Kuzemska, L 2021, 'How useful is 'State in Smartphone' for the IDPs in Ukraine?', blog post, RLI Blog on Refugee Law and Forced Migration, May 10, viewed 21 June 2021 <https://rli.blogs.sas.ac.uk/2021/05/10/how-useful-is-state-in-smartphone-for-the-idps-in-ukraine/ >.
- (Newman 2021) Newman, L 2021,' Microsoft's Dream of Decentralized IDs Enters the Real World: The company will launch a public preview of its identification platform this spring—and has already tested it at the UK's National Health Service.' *Wired,* 2 March, viewed 21 June 2021 <https://www.wired.com/story/microsoft-decentralized-id-blockchain/>.
- (Privacy International 2020) *The looming disaster of immunity passports and digital identity* 2020, Privacy International, viewed 21 June 2021, <https://privacyinternational.org/long-read/4074/looming-disaster-immunity-passports-and-digital-identity>.
- (Schoemaker, Currion & Pon 2018) Schoemaker, E, Currion, P, Pon, B 2018, *Digital Identity at the Margins*, Caribou Digital, Farnham, viewed 21 June 2021, < https://www.cariboudigital.net/wp-content/uploads/2020/03/Identity-At-The-Margins-Identification-Systems-for-Refugees.pdf>.
- (Slavin, Putz & Korkmaz 2021) Slavin, A, Putz, F & Korkmaz, E E 2021, *Digital Identity: An Analysis For The Humanitarian Sector*, International Federation of Red Cross and Red Crescent Societies, Geneva, viewed 21 June 2021, <https://preparecenter.org/wp-content/uploads/2021/05/Digital-Identity–An-Analysis-for-the-Humanitarian-Sector-Final.pdf>.
- (USAID 2017). *Identity in a Digital Age: Infrastructure for Inclusive Development* 2017, USAID, viewed 21 June 2021, < https://www.usaid.gov/sites/default/files/documents/15396/IDENTITY_IN_A_DIGITAL_AGE.pdf>.

- (Zomignani Barboza, Jasmontaitė-Zaniewicz & Diver 2020) Zomignani Barboza, J, Jasmontaitė-Zaniewicz, L & Diver, L 2020, 'Aid and AI: The Challenge of Reconciling Humanitarian Principles and Data Protection', in M Friedewald, M Önen, E Lievens, S Krenn, & S Fricker (eds.) *Privacy and Identity Management. Data for Better Living: AI and Privacy. Privacy and Identity 2019. IFIP Advances in Information and Communication Technology, vol 57,* Springer, Cham, pp. 161-176.

---

[1] According to the World Bank ID4D data, about 1 billion people in the world do not have identity documents: https://id4d.worldbank.org/global-dataset.
[2] See more on: https://www.hudumanamba.go.ke
[3] See more on DIGID and the user consultation process in the project in (IFRC and KRCS 2020).

Annex B - Workshop 1 Report

Introduction to the Workshop

IFRC representatives emphasising the importance of Digital Identity for the organisation, highlighting that those without official identity are often at more risk of being marginalized and vulnerable. The IFRC commitment to the people it serves means a collaborative "people first" approach to digital identity is critical. The stated purpose of the workshop was to build on the work that IFRC National Societies (such as Red Cross Kenya) are already doing in this area and take the first steps towards IFRC's common vision, strategy and policy for digital identity.

Presentations (link to video recording of the presentations)

Digital Identity as beneficiary management: Amos Doornbos introduced World Vision's journey to their approach to digital identification, highlighting functional identity as a beneficiary

management tool, and introduced two challenge questions for the IFRC. First, are you interested in being a humanitarian organization or a data company? Second, what does 'keep the beneficiaries at the centre' mean with how we treat data? These questions serve as a starting point for additional questions regarding how organizations manage, collect, and keep data, and how these questions should shape the discussion on how humanitarian organizations manage beneficiaries' data and how beneficiary's privacy can be best maintained.

Digital Identity as service provision - cash: Paul Currion introduced digital identity as a tool to support service provision, specifically cash, highlighting it as a key driver of digital identification in the humanitarian and development sector. Know Your Customer / Anti-Money Laundering (KYC/AML) requirements require financial service providers to verify the identity of clients, and since humanitarian actors usually work through these providers, this shapes how they approach digital identity. Increased use of cash transfers, as well as increasing financial inclusion generally, have therefore increased pressure on the sector to adopt similar digital identification. While this was less of an issue previously, it is now crucial for humanitarian organizations to become more aware of the impact of financial regulations on their work.

Digital Identity and risk - data protection: Vincent Graf from ICRC highlighted the two data protection pillars of *necessity* and *proportionality* as critical lenses through which to assess digital identity, and their implications for issues such as privacy. Necessity refers to the reason for data collection (is it necessary to collect to solve the problem the digital identification system is addressing?) and leads towards an approach that minimises data collection; proportionality is the balance between the intended aim with the means to meet that aim. Importantly, while ICRC have one of the most conservative and risk-averse approaches to biometrics, he emphasised that he believed biometrics were here to stay, and the challenge is to mitigate rather than solve the risks involved.

Breakout Room Discussions

To facilitate shared understanding of digital identification participants shared stories of digital identity that they had experienced or heard in their work and personal life, and to explore implications of these experiences for the work of IFRC on Digital ID.

Digital ID for both beneficiaries and IFRC: Participants described digital ID as an opportunity as well as a challenge for migrants and refugees, but that in either case it required a lot of work to inform them about what digital identity would mean for them. In the past migrants have expressed concern about ID solutions offered, including protesting their implementation, with concerns including the impact on their livelihoods. Digital ID was thought to have potential to address the challenge of aid worker sexual exploitation and abuse, in the form of a list of those who have breached the codes of aid practice, although it was acknowledged this was a sensitive legal and ethical area.

Data protection and the role of private companies: Participants expressed concern about organizational capacity to manage data, particularly to prevent leaks, and described humanitarian actors as having limited understanding of risks around data protection. Services

such as cloud storage distance humanitarian actors from data management leading to an under-estimation of such risks. Participants echoed the need for privacy-by-design in the humanitarian sector, noting the tension between humanitarian vs commercial imperatives in companies working with data, who might rely on using or selling data for tracking. Although the objectives of tech companies and humanitarian actors do not need to be completely aligned, there should be provisions for and measures to manage risk in such partnerships. The need for partnership will likely only grow as large tech companies possess the scale needed to respond to increased demand, with capacities that humanitarian actors do not have. Digital ID must also be understood in context. Cultural elements shape the deployment of digital identity - such as mobilization against national ID in Britain, and social attitudes in Belgium towards their National Identity System - with particular concern around how different records are consolidated (driving license, insurance, medical records, and national ID card – the sharing of digital medical prescriptions with pharmacists, for instance) and its wider implications for data protection and privacy.

Centralized data management: Centralised identification systems, such as Norway's National Identity Number (NIN) serves as an authenticator to make it easier to access a range of state services; however delays in receiving the number illustrate how a single point of entry can cause wider access issues, including challenges in the provision of Covid-19 vaccinations. This single point of failure leading to challenges in accessing services was also described in other countries, such as the Netherlands; one participant shared her experience with a humanitarian cash program managed by the Turkish government, where restrictions over data access limited humanitarian service delivery. Centralised data management is often justified in order to address duplication and fraud, yet in Greece a centralised Red Cross identity card failed to eliminate beneficiary double counting. During an emergency period in Cox's Bazar, the Red Cross' decision to register the whole population in the catchment area created problems a few months later since it was difficult to maintain and update such a large amount of data with limited resources. Anonymous services have also created tension between donor reporting and M&E requirements. Importantly, there was a shared sense that within the humanitarian sector, IFRC could have the potential to be a good 'neutral' identity provider.

Blockchain technologies: blockchain technologies were described as having helped reduce some of the issues encountered by the Kenyan Red Cross - specifically, it was described by participants as resolving repeated manual data collection that had driven consultation fatigue and the alienation of some beneficiary groups. Blockchain also introduces challenges: in contrast to traditional data collection and management approaches, beneficiaries struggle to understand the use and endpoints of data collected. This complicates the humanitarian principle of 'informed consent' - as how can people consent to the use of their data in ways they do not understand? Alternatives to blockchain that were flagged in discussion included the *Solid Server* and *API protocols*.

Final Discussion

The final discussion contained three guiding questions:

1. **What issues are there with digital identity?** Workshop participants highlighted a multitude of issues that were common across discussions, with particular emphasis on standards and governance. An IFRC participant stated “tech is fast, humans are slow”, and standards and policy need to accommodate rapid change yet maintain core IFRC principles, and be sensitive to impact of power and politics.
2. **Whose issues are they?** The discussion highlighted key stakeholders: key stakeholders: organisational staff, volunteers, andand beneficiaries, each with different concerns, each with different concerns. For organizational management, a core issue was the importance of improving staff and volunteer interaction;interaction; or beneficiaries, there were practical challenges of lack of connectivity and lack of digital skills.
3. **What should be IFRC’s first steps**? The first common theme was the importance of creating a common policy framework. There has been a lot of research on technology and potential use cases, but less on building an institutional framework on how to use the technology. A second theme was to push strategic conversations with donors that will allow the IFRC the space to implement strategies, such as data protection by design and data minimization. A third theme was the importance of identifying people who can translate between humanitarian practitioners and technology experts. Finally, one participant confessed that in the past they’d started with some exciting ‘shiny’ technologies, and looked for problems to solve, only to fail in their application; instead, they argued that it was important to understand and define the problems that needed to be solved, including and especially from the perspectives of beneficiary communities, and to explore possible solutions from that shared understanding.

Workshop 1 Mural Notes - Breakout Group

Workshop 1 Mural Notes - What & Whose Issues, IFRC priorities

Annex C - Workshop 2 Report

Introduction

The workshop began with representatives from IFRC identifying the importance of digital ID. They specifically highlighted how the technology has the potential to enable beneficiaries' access to services in the management of IFRC staff and volunteers. They stated the objectives for the workshop, which focused on identifying what good digital ID manifests as and a common vision around digital ID.

Session 1

This first session broke the participants into groups that focused on four different IFRC's areas: migration, health, cash, and staff and volunteer management. The groups grappled with the future of digital ID through creating stories of how certain IFRC users will utilize digital ID in the future.

Digital ID and its Role in IFRC

All four of the groups examined what digital ID would mean for the role the IFRC plays with their staff, volunteers, and beneficiaries. The participants underlined that digital ID could aid the mission and values of the IFRC in ways such as enabling vulnerable beneficiaries to bypass medical insurance requirements and receive valuable services.

They also highlighted challenges to achieving 'good' digital ID by posing questions such as, 'does the recipient (beneficiary) have enough information about how digital ID works?' Another question revolved around if the beneficiary receives information from IFRC NS staff, how do NS staff learn about the IFRC HQ's overall policy? How are they taught to communicate the digital ID IFRC vision to an aid recipient or beneficiary? These challenges must be at the center of the conversation about IFRC's future use of digital ID.

Additionally, a particular group that was focused on staff and volunteer management highlighted that IFRC HQ's overall role is to create the shared protocols that are necessary for the NS to use, but the NS should be kept at the forefront of creating the digital ID software itself. The IFRC HQ should be focused on producing lessons, documentation, and standards in order to create common protocols across all national societies. This group underlined that the roles of IFRC HQ and IFRC NS should have the same overall goals when it comes to digital ID, but different roles to how digital ID will be executed.

Security concerns with Digital ID

The participants grappled with security concerns with digital ID and possible solutions to those security concerns. The security concerns around digital ID included how data protection systemscan be an enormous feat, which would signal that IFRC should begin creating a data protection system soon. The group focused on health underlined that private companies could

create data security concerns, so the IFRC should be hesitant about sharing health data and genetic information with the organizations. They underlined that the IFRC should view itself as the protector of their beneficiaries' genetic information. Additionally, the participants stated that solutions to the glaring security concerns could be an IFRC card with no identifying features, which would only include a type of number signaling the beneficiaries' identities.

Digital ID Aiding Movement Possibilities

The groups within this session underlined the possibilities that digital ID could offer for IFRC. One of these possibilities was with the IFRC's many volunteers. The participants believed that digital ID could be a tool for the volunteers to obtain their necessary credentials to work as a volunteer. This would allow the IFRC staff to clarify that the volunteer has the needed skills to complete the job quicker. These credentials could permit the volunteer to move seamlessly around different organizations. Additionally, the digital ID credentials for volunteers would give the volunteers and staff the option to go to events without disclosing and duplicating their information endlessly, which would improve the IFRC overall.

Session 2:

In this session, participants debated 'challenge questions', some of which were drawn from discussions at the first workshop. As opposed to resolving the questions, participants broadly articulated some of the issues, as well as their wider implications.

IFRC as a neutral identity provider: While some participants admit IFRC as being an identity provider given its ongoing practices involving the capturing, storing and processing of beneficiaries' data; others argue that it should not be a provider as people should be their own provider. Participants highlighted that it is important, for humanitarian purposes, to have a functional ID that limits the credential requirements for recipients. The Australian Red Cross, for example, offers ID storage for people in bushfire-prone areas, e.g., passport scans which can be retrieved when necessary, but its access remains restricted to the Australian RC. Interestingly, rising demands for official recognition from commercial tech providers including Apple, opens another opportunity for IFRC to decide on what it wants to be and where it stands on the digital ID landscape.

IFRC as a software company: Some participants invite IFRC to own its position as a software company already. Although this seems to be ambitious to others. An interesting linkage of IFRC's work to services rendered by airlines mirrors the need for IFRC to grant recipients the opportunity to choose the services that they want. This stems from IFRC assuming its position as a service provider. It needs to demonstrate its beneficiary management by providing assistance and a sense of inclusion to national societies. In other words, it should champion national society-led approaches. Further, some participants recognize the consultative roles IFRC could play in its interaction with multiple stakeholders. IFRC can provide needed advice on offered digital ID solutions; it could serve as a broker between countries, given the unequal nature of identities across regions in the world; it can as well help steer consistency in the provision of digital ID services, as this can be difficult to be achieved with multiple players on the

field. Also, either as a software company or not, IFRC should prepare its staff and volunteers for the future of digital ID. They should be provided with adequate literacy, such that 5 years from now actors within the system are well informed to respond to simple and complex issues raised.

Biometrics are here to stay: The participants believe that the evolving realities of biometrics mean that the IFRC should take either a 'passive' (harm minimisation) or 'active' (regulation advocacy) approach to biometrics. Participants contend that both approaches are intermediated as 'harm minimisation' cannot be divorced from the establishment of strict regulations about biometrics. Notably, alternatives to identity capturing exist across IFRC's societies. For example, IFRC Geneva has embraced other means aside from fingerprints as it creates exclusions for those without quality fingerprints. Palm printing scanning was also found to be more reliable, token-based and constant overtime. The work of IFRC and its national societies with partners raise concerns about the retainment of biometrics in the Digital ID landscape. This stems from tendencies for differentiated use of technologies based on conflicting principles. Also, the autonomy enjoyed by national societies grants IFRC less privileges for advocacy. Participants raise a few questions regarding the uptake of biometrics. Is policy enough (as policy can be easily broken)? Does IFRC possess the capability as a movement to manage biometrics? What is the purpose for the use of biometrics? What provisions are there for identity theft and data leakage? The quest for accuracy in the biometrics industry should not be given up for security. Hence, IFRC's priority should also be to advocate for the security side of things. For example, it should offer humanitarian, ethical and impartial alternatives for the management of people's genetic information.

At the centre of IFRC's digital ID - principles or beneficiary preferences: kThe participants in this group had a similar perspective that the IFRC should strive to manage its expectations for the organization and the beneficiaries. It is highly crucial for clear boundaries to be defined, as it might be difficult for IFRC to offer every type of identity. Nonetheless, beneficiary cultures need to be in harmony with said principles. Intersecting beneficiary preferences and the IFRC principles will on one hand facilitate the understanding of what works and does not for beneficiaries. On the other hand, the seeming transactionary relationship between IFRC and the beneficiaries would be founded on mutual and informed consent, integrity and trust.

Implications of IFRC values and principles for Digital Identity

IFRC's seven principles were unique lenses through which the future of the organisation's Digital ID project could be envisioned.

Humanity: The right of an individual to the ownership of their data is fundamental. Also, IFRC should be customer-service oriented and should serve beneficiaries based on their needs.

Impartiality: People should be protected against any form of politicization. Services should be rendered without political preference and interference. This can be further demonstrated by protecting the data of beneficiaries from being used for political purposes. Digital identity systems can be designed in ways that would make data sharing impossible. As such, even government pressures and politicking would not be able to get such data out.

Neutrality: It is important to make Digital ID services available to all irrespective of their identities and based on their needs. In addition, neutrality would be better displayed when data is moved away from the organization towards the beneficiaries themselves. A neutral Digital ID will also reduce or eliminate IFRC's cross-border restrictions.

Independence: The participants highlighted three overall possible influences of digital ID to this principle: NS, beneficiary, and volunteer independence. Digital ID could enable independence from the state, which are usually political institutions, where NS is working. Additionally, the beneficiaries could become more independent from the IFRC. Finally, the volunteers within IFRC would be able to use digital ID to become more independent of specific IFRC organizations and move around to different organizations easier.

Voluntary Service: Digital ID could be given to the volunteers. Also, IFRC could use this technology to search for solutions within the organization and call on people's overall notion of voluntary service.

Unity: The participants highlighted that the IFRC could be able to act with unity across all the societies through digital ID, because the technology would be able to identify people more effectively and promote inclusion.

Universality: The IFRC, which is a service industry that focuses on beneficiaries' needs, could utilize interoperability and widely recognized solutions in order to meet the principle of universality.

Conclusion

The workshop concluded with a quick word from representatives from the IFRC, who highlighted the importance of the workshops and discussions, and that action will be taken soon to move the IFRC closer to a digital ID solution.

Workshop 2 Mural Notes - User Story

Workshop 2 Mural Notes - IFRC Challenge Questions

Workshop 2 Mural Notes - IFRC Principles & ID

Annex D - Inception Report

The below table outlines the high-level timeline, proposed activities, and effort estimates to help achieve an outline of a vision for digital identity for the IFRC, and steps required to progress it.

Methods include the conduct of a literature review (see Annex A) based on an agreed list of literature documents. The first workshop was based on the principle of knowledge exchange, including the sharing of external experience as well as internal IFRC experience. See the workshop writeup (Annex B) for full details. The second workshop was based on the principles of building a future vision for Digital ID for IFRC, and included both futures exercises as well as aligning insights on digital ID to the IFRC core principles (see Annex C for full details).

		Tues	Weds	Thurs	Tues	Weds	Thurs	Tues	Weds	Thurs	Tues	Weds	Thurs	Tues	Weds	Thurs	Tues	Weds	Thurs	Tues	Weds	Thurs	Tues	Weds
	LoE	8	9	10	11	**12**	**13**	14	15	16	17	18	**19**	**20**	21	22	23	24	25	**26**	**27**	28	29	30
Workplan:																								
Literature Review	10																							
Workshop 1:																								
Design workshop process	3																							
Workshop	0.5																							
Writeup	1																							
Workshop 2:																								
Design workshop process	2																							
Workshop	0.5																							
Writeup	1																							
Recommendations																								
	2																							
Total days	20																							