DIGITAL IDENTITY
AN ANALYSIS FOR THE HUMANITARIAN SECTOR

MAY 2021

ACKNOWLEDGEMENTS

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

Norwegian Red Cross

NRC NORWEGIAN REFUGEE COUNCIL

NORWEGIAN CHURCH AID actalliance

Save the Children

Innovation Norway

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

The Oxford Centre for Development & Technology carried out the consultations and produced the report. The authors were Aiden Slavin, Franziska Putz and Dr Emre Eren Korkmaz.

OCTD Oxford Centre for Technology and Development

Thanks are also due to all the interviewees for their contributions.

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

Credit: Photo taken by Kenya Red Cross Society. From 121 project implemented by Kenya Red Cross Society, 510 an Initiative of the Netherlands Red Cross, and British Red Cross. Funded by GSMA.

CONTENTS

EXECUTIVE SUMMARY

The ability to prove one's identity is an increasingly important aspect of contemporary society. Indeed, the UN's Sustainable Development Goals include Target 16.9, "By 2030, provide legal identity for all, including birth registration." However, identification can represent a significant challenge to beneficiaries of humanitarian aid. Advances in technology hold much promise in the form of digital identification. But as humanitarian organizations start exploring such solutions, they must address several questions. These range from the technical – how to implement digital IDs in an increasingly complex ecosystem and apply such digital solutions in low-connectivity settings where many vulnerable groups reside – to the ethical – how to collect beneficiaries' data in a way that respects their privacy and gives them more agency over their own data – and how to ensure these solutions are sustainable.

This research report was commissioned by the International Federation of Red Cross and Red Crescent Societies with the support of the Dignified Identities in Cash Assistance (DIGID) project consortium and was delivered by the Oxford Centre for Technology and Development.

It lists seven key questions that humanitarian organizations should consider before investing in digital identification solutions. These questions in turn form the basis of a series of interviews with 24 experts with relevant knowledge and experience on digital identity. A set of three case studies complements and illustrates the conclusions drawn from the interviews.

This report starts with a brief analysis of how the private sector uses digital ID technologies before delving into the humanitarian sector use cases and needs to which such technologies could be applied. Achieving interoperability was noted as a critical requirement in realizing the key benefits of digital ID in the humanitarian sector. Such interoperability is twofold: digital ID solutions must be integrated with other data-driven technologies and data must be shared between different actors so a beneficiary's identity is recognized broadly instead of in siloed systems. Culture change in data governance and political will to achieve multi-stakeholder interoperability are important considerations on top of those concerning technical implementation.

There are barriers to implementation and adoption of digital ID solutions because many humanitarian organizations operate in environments that are not always digital-friendly in terms of access to connectivity, to devices such as mobile phones, and the literacy levels of end users. It is important to keep vulnerable communities in mind when designing such digital solutions and maintain a balanced view of their benefits for the organization and the beneficiaries themselves. In terms of deployment and maintenance of digital identification solutions, training and learning opportunities for beneficiaries must be integrated by vendors of the technology and organizations working with communities.

Digital identification systems can be costly to put in place and sustainable business models are necessary to ensure successful scale-up beyond piloting. Such costs can be exacerbated by their being perceived as "back-office" technology by donors. Therefore, organizations should make a clear case for their direct advantages for beneficiaries. Again, other sectors can serve as a model. For example, software as-a-service licensing can be more efficient in the long term than (series of) one-off development grants.

Overall, digital identification technologies do indeed show promise for extending humanitarian services to new beneficiaries and enhancing existing services to current beneficiaries, in addition to benefiting humanitarian organizations themselves. But their application requires careful planning and consideration to ensure their suitability and efficacy, taking into account local requirements and conditions.

INTRODUCTION

The United Nations' Sustainable Development Goals (SDGs), building on the successes of and lessons learned through the Millennium Development Goals, consist of 17 goals for the international community to achieve by 2030. Among these, Goal 16 "Peace, Justice and Strong Institutions" includes Target 16.9: "By 2030, provide legal identity for all, including birth registration." Target 16.9 has mobilized a broad coalition of public and private actors to work on bridging the gap that exists in the world when it comes to people's access to identification.

Being able to prove one's identity has increasingly become a prerequisite for accessing many services across the public and private sectors. While the process of identification has been traditionally facilitated by paper credentials, identification processes are increasingly reliant on digital technologies [1]. It is now more important than ever for humanitarian and development agencies to examine the benefits and drawbacks of digital identification technologies. Today, organizations including telecommunications providers, financial institutions, governments and other organizations are beginning to undertake new digitalization efforts to adapt to new developments in the identity and access management and decentralized identification sectors [2].

A digital identification (ID) system is not a single technology, but a suite of a technologies that, when taken together, facilitate the identification process. A digital identity solution is a technology suite capable of supporting identification processes [3]. Digital ID is still defined differently by various stakeholders. A digital ID can be a digital copy of an identity document, a set of attributes representing an individual in a transaction or a metasystem of digital identifiers that, when taken together, can uniquely identify an individual [4].

A variety of private sector organizations are leading investment in digital identification systems and their underlying technologies. In addition to marquee corporations such as Microsoft and Mastercard investing resources in digital identity systems, several digital identification and access management companies have begun to dominate the market [5] [6]. Okta, for example, recorded a revenue in 2020 of 586 million US dollars [7]. Notably, many of these private sector implementations of digital ID technologies are still in a pilot phase. As a client of several of these organizations, the humanitarian sector both benefits from and informs the development of technology in the private sector. Both the public and private sectors are exploring digital ID technologies. That said, the private sector is advancing much faster than the humanitarian sector and, as noted below, humanitarian sector organizations may benefit from innovations coming out in the private sector.

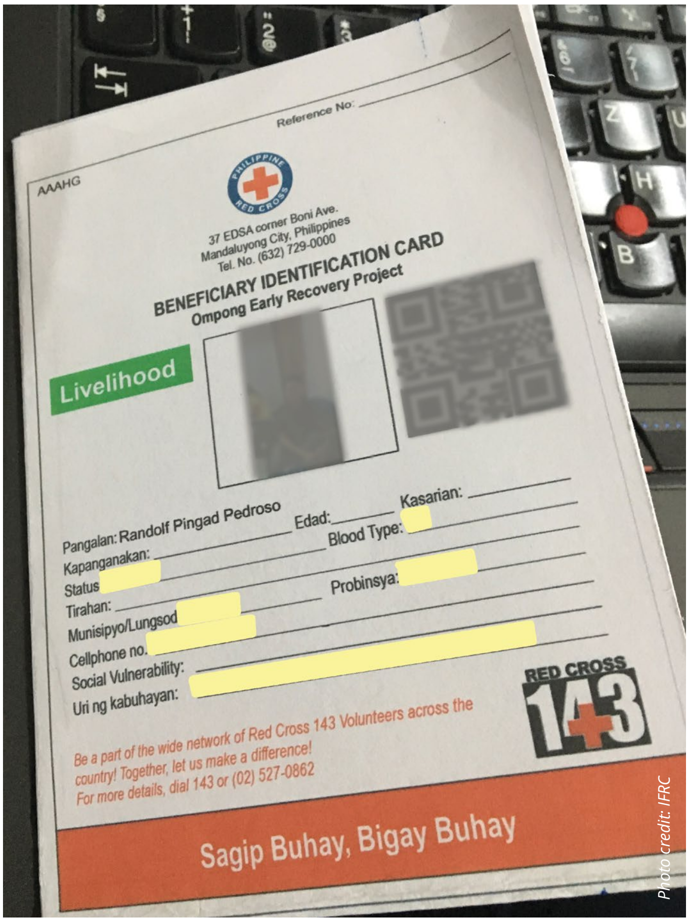
The private sector sees the potential for digital ID to unlock economic value for firms, governments, employees, consumers and taxpayers. A key demographic value that private sector organizations are seeking to access through digital identification technologies is the more than 1.7 billion people worldwide who are currently financially excluded from the traditional financial sector because they do not have an official ID.

The private sector sees a significant opportunity, through digital identity systems, to optimize the delivery of e-government services, such as social protection and direct benefit transfers. As the McKinsey Global Institute estimates, digital identity systems could be leveraged to save roughly 110 billion hours currently spent on the distribution of government services. This time-saving potential represents a significant revenue opportunity for private sector organizations looking to provide services to the public sector. Cost saving opportunities are not limited to the public sector: by reducing onboarding costs and payroll fraud through enhanced "smart" authentication techniques, digital identity systems could result in savings of 1.6 trillion US dollars globally. The benefit of these systems would not only accrue to organizations but could also improve the livelihoods of individuals. By offering individuals economic and political inclusion, digital identity systems could pave the road to broader equality of access and control of information [8].

As the International Federation of Red Cross and Red Crescent Societies (IFRC) and other humanitarian agencies expand their digital offerings, they are beginning to explore digital identification as a way to enhance existing services for beneficiaries and to provide new ones. The IFRC is leading the technical implementation of the Dignified Identities in Cash Assistance (DIGID) project [9] with a consortium of the largest NGOs in Norway including the Norwegian Red Cross, Norwegian Refugee Council, Norwegian Church Aid, and Save the Children Norway. Together they are looking to address the challenges of providing humanitarian cash assistance to people with no recognized IDs.

This report was commissioned by the IFRC with support from the DIGID consortium to analyse the use of digital identity solutions in the humanitarian sector. It is hoped that this report will be useful to anyone in the humanitarian sector looking to invest in or develop digital identity solutions for their organization.

This report is built on a mixed-methods research study comprising a desk-based literature review, interviews with experts and case studies. The interviews were built on seven critical questions compiled by the IFRC, which are commonly asked by humanitarian organizations exploring digital identity solutions (see Appendix I for a list of the questions). Twenty-four experts from humanitarian organizations and the private sector with knowledge and experience on the subject were interviewed (listed in Appendix II). Responses from the interviews were analysed and the findings and recommendations are summarized below. Finally, three case studies were examined to understand the complexities of implementing digital ID systems. These were World Vision International's Sikka platform in Nepal, the SDG Impact Accelerator's Digital ID start-up in Turkey and a pilot project completed by the 121 consortium in Kenya at the end of December 2020. For a detailed description of the research methods, see Appendix III.



Reference No:

AAAHG

PHILIPPINE RED CROSS

37 EDSA corner Boni Ave.
Mandaluyong City, Philippines
Tel. No. (632) 729-0000

BENEFICIARY IDENTIFICATION CARD
Ompong Early Recovery Project

Livelihood

Pangalan: Randolf Pingad Pedroso Edad: Kasarian:
Kapanganakan: [redacted] Blood Type: [redacted]
Status [redacted] Probinsya: [redacted]
Tirahan:
Munisipyo/Lungsod [redacted]
Cellphone no. [redacted]
Social Vulnerability: [redacted]
Uri ng kabuhayan:

RED CROSS 143

Be a part of the wide network of Red Cross 143 Volunteers across the country! Together, let us make a difference!
For more details, dial 143 or (02) 527-0862

Sagip Buhay, Bigay Buhay

Photo credit: IFRC

Philippines, 2018: In response to Typhoon Mangkhut, the Philippine Red Cross (PRC) issued beneficiary identification cards to those receiving shelter and livelihoods assistance. A unique identity QR code was included in the card making it easy for staff and volunteers to authenticate the recipient because the data was linked with the PRC's beneficiary management system.

FINDINGS AND RECOMMENDATIONS

Question 1

In what cases can digital identity solutions be applied, and why are they suitable? What are the limitations to their applicability?

Humanitarian organizations have begun trialing digital identity solutions in a wide variety of contexts. Among the most commonly discussed are cash transfer programmes, health services and the provision of identification credentials for beneficiaries without an officially recognized form of ID [2]. Each case features unique advantages and disadvantages. In addition to summarizing these benefits and drawbacks, this section offers definitions of foundational and functional IDs.

The main use of digital identity by humanitarian organizations is registration or enrolment to assistance programmes. By providing a digital means of confirming that someone is who they say they are, digital identity solutions can facilitate the registration or enrolment process in the humanitarian sector in two ways.

First, humanitarian organizations can provide foundational IDs to beneficiaries who do not have an officially recognized form of ID. A foundational ID is a form of identification which is endowed with a high degree of assurance or trust, such as a passport. It enables users to access a wide variety of services. By providing a form of foundational ID, humanitarian organizations can enable beneficiaries' access to many services both within and outside of the humanitarian context. Such an ID need not possess the same level of assurance, or trust, as a passport, but it can still be useful to beneficiaries in the long term as a form of identification [10]. Examples of foundational humanitarian IDs include the UNHCR refugee ID. In Egypt in 2018, telecommunications providers began recognizing UNHCR refugee credentials as a valid means of proof for purchasing a mobile SIM card [11]. In this way, humanitarian IDs can serve a purpose beyond their limited scope as a facilitator of aid distribution and may be able to contribute to beneficiaries' long-term socioeconomic development [#1][1]. It is critical to note, however, that such a provision is fundamental to the mandate of UNHCR [12].

Second, humanitarian organizations can provide beneficiaries with a form of scalable, functional ID that can, over time, accrue a transaction history and, with it, cultivate a higher degree of trust with traditional service providers. A functional ID is a form of ID issued to provide access to a single service, or a single class of services [13]. This secondary mechanism is similar to that of service providers making use of alternative data sources to develop alternative credit history to enhance the "bankability" of vulnerable populations.

Several humanitarian organizations have also begun to explore the use of digital identity solutions for the provision of volunteer credentials. The Australian Red Cross has developed an online wallet for volunteer credentials [#2]. Using the World Wide Web Consortium (W3C) standard, the technology provider TypeHuman developed an app that anonymously tracks data about volunteer behaviour to support customer and business processes through next-generation digital identity solutions [14].

[1] References preceded by the # symbol refer to interviews. See Appendix I for interviewee names and affiliations.

Last, perhaps the use case of digital identity solutions that has been most frequently piloted in the humanitarian sector to date is cash transfer programming. In such pilot projects, beneficiaries are given access to financial services through the application of a functional ID. One such system, designed by Tykn and piloted on the Sovrin network, enables transactions through a centralized architecture. Another such system is RedRose's decentralized identifier, which can be used to power cash-based transfer payments. A corollary to the use of digital identity to support cash transfer programmes is the use of digital identity for forecast based financing to facilitate the transfer of funds ahead of a disaster, enabling a swifter, more streamlined response. While digital identity technology can introduce unnecessary and cumbersome friction to emergency relief situations (for example, because of its reliance on mobile connectivity that is not always available), it also has the potential to support long term aid and development initiatives. For example, Jimmy Snoek of Tykn outlined a scenario in which individuals who have been identified for previous aid initiatives can continue to be supported with direct cash transfers when a flood is predicted and they will likely need resources to fortify their village [#3].

Recommendation 1A

Cultivate sectoral and cross-sectoral interoperability.

Building long-term, usable identification to support beneficiary registration or enrolment, volunteer credential attribution and cash transfer programming requires interoperability and information sharing across aid and non-aid organizations. To facilitate the use of credentials beyond their original function, humanitarian data storage systems must be made interoperable with those of the organizations that the beneficiary seeks to access [15]. For instance, by using a common health schema and data exchange format, a humanitarian organization could enable a beneficiary to share their health records with a healthcare provider, thereby improving their care outcome. In this case, interoperability must be established not only within the humanitarian sector, but also with the healthcare system. This requires knowledge of and willingness to develop systems in line with established processes in other sectors including, for instance, the Fast Healthcare Interoperability Resources Specification [16]. Another potential use case requiring interoperability is facilitating access to formal spaces, such as interactions with banks or telecommunications companies [17].

It is worth noting, however, that there is skepticism among experts that humanitarian organizations could provide foundational IDs necessary to provide robust, scalable identification. One interviewee [#4] vehemently disagreed with the optimism behind this trend:

> *"I don't see this trend [of including the unbanked] happening. What you do see is banks themselves becoming identity providers. They provide the service and then integrate their services with governments in order to have these identities verified. Your account with the bank thus makes you identifiable to the government. This is a complete opposite trend that has a lot more power behind it than the aspiration to get the unbanked into the banking system with a humanitarian launched identity system."*

Nevertheless, as both humanitarian and non-humanitarian organizations seek to provide beneficiaries of aid with highly functional forms of ID, they will need to cultivate sectoral and cross-sectoral interoperability to make the credentials usable.

Recommendation 1B

Champion the benefits, and recognize the drawbacks, of digital ID systems to galvanize political will and technical knowhow.

Achieving interoperability is often more a question of political will than technical feasibility. To facilitate interoperability at scale, thereby enabling beneficiaries to use their credentials in a wide variety of settings, will require significant lobbying and advocacy work within humanitarian organizations and in other sectors. Even if humanitarian organizations could mount the necessary campaign to develop interoperability, doing so would still require innovation at the technical level. Indeed, attempts to change data recording practices across organizations with radically different information architectures will be met with significant barriers [#5] [#6]. Furthermore, legal limitations (including the development of intellectual property agreements and point-to-point trust frameworks) pose a challenge to implementing any sort of technological change in the humanitarian sector [#7]. While there is significant progress being made in the decentralized identity community on the development of standards, most notably by W3C, there is still much work to be done [14].

Thus, driving convergence on standards in the humanitarian space will require an active push for the cultivation of both political will and technical knowhow. Scholars analyzing political will have focused primarily on four key components:

- a high number of decision makers
- a broad and general understanding of a problem and potential solutions
- widespread support of a solution
- a commitment to iterating to find an effective solution.

While it will largely remain up to each organization to determine how best to seek to influence these four factors of political will, a few initial steps include:

- joining relevant trade and industry organizations to build internal and external expertise
- participating in relevant fora
- engaging in an internal dialogue that seeks to explicitly link the value of an innovation in terms of the organization's mission statement or mandate [18].

Question 2

Pressure is mounting to protect beneficiary data, to implement self-sovereign identity technologies to give beneficiaries more autonomy to manage and own their data, and to lessen the storage of such sensitive data in centralized databases. Given this, how should humanitarian organizations adapt their beneficiary data management systems and practices to responsibly integrate digital ID solutions?

To date, humanitarian organizations have tended to use a range of data management and storage systems to collect and process beneficiary and programme information. Indeed, the ecosystem of data management solutions available to humanitarian organizations is large and complex.

One of the largest data management systems in the humanitarian sector is WFP's SCOPE, which currently houses the data of over 20 million aid recipients and is licensed to other NGOs. Another example is World Vision's Last Mile Mobile Solution, which is used by more than 20 NGOs across 29 countries and contains the data of more than 8 million beneficiaries [19] [20]. A central question faced by humanitarian organizations investigating the potential use of digital identity solutions is how to manage the transition from traditional data storage and management systems, such as beneficiary management solutions, to digital identity solutions.

Recommendation 2A

Invest resources upfront to bring about internal culture change to ensure long term success.

Several interviewees used the term "culture challenge" to describe the difficulties of transitioning from one data management paradigm to another [#5] [#7] [#8]. It is important for humanitarian organizations to establish a common language to educate staff members on not only the mechanisms of digital transformation, but also the reasons behind it [#6] [#7] [#9]. Staff members must buy into the transition process and see it as integral to the achievement of their work. It can often be difficult for humanitarian organizations, so invested in distributing aid to alleviate crises, to justify investments in what can be seen as back-office systems and processes. Nonetheless, as several interviewees noted, it is often the functioning (or non-functioning) of these processes that determines the success or failure of a programme [#6] [#7] [#9]. Therefore, digital transformation leaders within humanitarian organizations must accept education and internal culture change as part of their roles. Culture change is a slow process that requires the alteration of daily habits and organizational processes, and significant upfront investment.

Critical to this culture change is the revision of existing data governance practices and protocols. Several interviewees commented that the transition from traditional data management systems to digital identity solutions is often more an issue of altering data governance practices than effecting technological change. The greatest challenge to deploying responsible data sharing agreements and governance protocols lies in educating humanitarian workers. Humanitarians, like many other modern professionals, often struggle to fully understand, much less manage and protect, their own data [#10] [#11]. Lack of comprehension has led to instances in which organizations trust data from others more than their own because “we know what the caveats and limitations are on our data and we assume others work to higher standards than we do” [#8].

The experts noted that existing challenges related to data governance would need to be addressed to transition from beneficiary management to digital identity systems. Some of these challenges include altering historical attitudes towards data sharing and protection. “It comes with the territory” that most have been historically averse to any kind of data sharing, considering that there is often some nation state or other actor seeking to obtain a file of sensitive information that a staff member has access to [#7]. One participant described it as an “ongoing cat and mouse game to protect the data that we have,” and as a result, “data sharing doesn’t come naturally to our staff” [#8]. Because data protection policies put the onus on the organizations, they need to shift from saying “no, it is too sensitive, we can’t share it” to consistently reflecting on what good practices look like: the purpose and scope of sharing, timelines around access, retention and deletion, and what additional costs are associated with these efforts [#8].

Humanitarian organizations must make a significant upfront investment in determining how their data governance practices must change, then begin to secure internal buy-in for a culture change, and then implement. The implementation of a technology transition is often the simplest part of an organizational change that requires broad buy-in and adoption. It must be noted, however, that the path to true culture change will largely depend on the particularities of a given organization. However, like developing political will, steps an organization might take to bring about greater culture change could include mandating that a certain technology be used if a certain programme is to be eligible for funding, joining relevant trade and advocacy organizations and creating an internal dialogue that closely ties the innovation to the organization’s mission statement.

Recommendation 2B

Invest resources upfront in the development of in-house technical expertise.

Central to this transition is improving the technical literacy of existing staff members. This process can be long and arduous, especially when staff have multiple, competing priorities. For one organization, it took 2-3 years of training programmes and strategic internal communications campaigns to ensure any initiative that applied to data was imbued with the same language with which everyone was familiar. The representative admitted that the work will “never be finished, but at least at the level of key decision makers we’re there and I don’t see many conversations in which there are definitional challenges” [#7].

The same cannot be said for the sector at large. Vendors, academics, and practitioners claimed that inconsistent definitions and terminology were a serious source of friction in partnerships. Gravity’s Johannes Ebert was not alone when he claimed that, far from being a second-tier problem, finding a common glossary on digital identity in the humanitarian sector is the issue which he wants to see most immediately addressed [#9]. As the trouble with establishing a common glossary of terms illustrates, upskilling technical staff in an area of active technical development can be a costly and difficult process.

Nonetheless, some methods of upskilling technical knowhow within humanitarian organizations are seeing early signs of success. The Australian Red Cross, in addition to vendors such as Tykn, has assumed this responsibility with a determination to respect the trust placed in them by pursuing privacy-by-design in their digital ID systems [#2]. The principle behind this approach is to reduce the burden of education that would otherwise fall on humanitarian workers to translate to beneficiaries. Instead, even if users were willing to share all of their data, they would never be asked for more than the minimum by virtue of how the digital ID system was designed in the first place. To quote Amanda Robinson, "As an organization that doesn't treat users as a product, we just need to hold true to that and make it transparent to the individuals we serve" [#2]. A tactic another organization employs is to move from data sharing to data access, which should ideally be initiated by the individual via a biometric key, or in a few years via self-sovereign ID (SSI)[2] [#7]. A current strategy is to add temporal limitations to data sharing agreements. However, this conflicts with the mandate of certain organizations such as UNHCR, which has an obligation to archive data. Data minimization can be particularly challenging in the context of a humanitarian response where a large aid organization is fulfilling a coordination function whereby multiple partners are reliant on the data that organization collects – this was called a "nightmare scenario" in terms of minimizing data collection and sharing [#7].

Therefore, it is critical that humanitarian organizations invest in the development of staff members and internal expertise or find solutions such as those described above. For smaller organizations, however, it is not practical to invest significantly in developing in-house technical expertise [#8]. In this case, it will be helpful to train relevant staff members using widely available free tools to create at least a baseline of understanding and familiarity. A good resource for locating such tools is the Linux Foundation [22].

Question 3

Aid organizations have limited resources. Adopting new technologies could imply barriers in terms of costs, skills, and resources (maintenance, support, etc.). Thus, what economic incentives and sustainable business models for the use of digital ID technology apply to humanitarian organizations?

Ever having to balance the trials of fundraising with the allocation of funds to deserving programmes, many humanitarian organizations exist in a constant funding dilemma. In this tundra of obligation, it can often be difficult for humanitarian organizations to justify investment in technologies that fundamentally relate to back-office operations. Without a direct line to the distribution of aid to beneficiaries, humanitarian agencies struggle to raise necessary funding to develop systems such as next generation digital identity solutions. It is also true that the transition to new technologies often requires supplementary investments in upskilling staff and developing maintenance technologies. Therefore, it is critical that humanitarian organizations explore the full breadth of economic incentives and sustainable business models regarding digital identity solutions. Common cost components of operating a digital identity system include the costs of human resources, ID credentialing, a central IT infrastructure, physical establishments, enrolment IT infrastructure, information, education and communication [23].

[2] SSI is "the digital movement that recognizes an individual should own and control their identity without the intervening administrative authorities. SSI allows people to interact in the digital world with the same freedom and capacity for trust as they do in the offline world" [21].

Recommendation 3A

Digital identity systems are costly and may be best financed as a digital public good through the investment of philanthropists and other public sector funders.

Digital identity solutions are costly to implement. As with many new technologies, funds that must be invested in upfront research and development costs, as well as use-case customization, dramatically increases the requisite upfront investment in digital identity solutions. Beyond upfront costs, there is also the long-term need to invest in internal capacity building to power this transition [23]. In the words of one participant: "You reach a whole universe of huge process challenges because policy is high-level while the implementation always requires additional consideration, timelines, investments, and discussions in order to ensure you have the elements that you need secured. It took us three years to move from a data protection policy to in-practice guidelines, and we were working at full speed" [#7]. The need to invest in culture change and internal training was underscored by many participants as the functionality of any data related policy ultimately hinges not on the technology being used, but on the abilities of the people using it. Staff members must "know how to use it and implement it properly and understand the risks if they do not implement it properly" [#7]. Training those managing digital identity systems is seen as a great challenge given how new and difficult to grasp these systems are even for those who have been working in this space for many years, and it is an ongoing investment given the speed at which the relevant technology and practices evolve.

There is a further challenge in that the robust privacy protections in many digital identity systems make it harder for many of them to be adopted at scale. Organizations have largely ruled out the idea of monetizing user data, although there were admissions that some had been consulted by private sector clients to consider doing so. Representatives of the Australian Red Cross and Tykn's CEO both admitted that their unwavering commitment to protecting user data and not even collecting it had caused them to lose business and partnership opportunities [#2] [#3].

Most digital identity efforts consulted were funded by grants from large donors or innovation funds. These sources of funding, however, can create problems for organizations. Donor funding can come with conditions such as requests for lists of programme participants that might compromise an aid organization's commitment to protect user data [#8]. Moreover, some interviewees commented that donor funding for innovations like digital identity were insufficient because they tended to only fund one part of the process rather than the entire process. As a Kenya Red Cross member said, "If you're going to fund innovation, then fund the whole process so we can get a workable solution out of it" [#12]. They went on to note that the costs of a digital identity system should be shouldered by donors and private sector actors who are benefiting from their being established, as financial and mobile network institutions do any time a cash transfer is run via M-Pesa, a mobile phone-based money transfer service [24].

Recommendation 3B

Look to other sectors to justify the upfront cost of investment in digital identity solutions given long-term efficiency gains and cost cutting.

There is also the possibility that efficiency gains from scaling digital identity solutions in parallel domains will make their adoption in sectors like the humanitarian sector less costly in the long term. The interest in applying digital identity solutions to traditional identity and access management challenges, as well as niche use cases such as Covid-19 vaccination and testing credentials, could help lower the adoption costs of digital identity solutions [25]. Even humanitarian organizations that were in the process of developing their own digital identity systems for multiple years acknowledged that financing the further development of these systems needs to come from funds outside of the humanitarian sector, as it is not easy to create a self-contained business in the humanitarian space [#4].

While further development is likely to come from innovation grants or adoption pushed by larger donors, it is more likely that digital identity systems will be improved by private sector actors, likely for a variety of different use cases. Multiple humanitarian interviewees acknowledged this was a time for patience. They noted that they could eventually adapt the tools developed by the private sector to meet their needs, rather than struggling to create their own. As one interviewee [#1] noted:

> *"We tried to be in the driver's seat in the development of a digital identity solution and we've realized that maybe we should no longer be in the driver's seat. That opens up a different way of looking at how you can fund these things, even if that means you may have to wait a little bit until the right solution comes. In the meantime, we have the funding sorted for how we do information management because we just use an open source tool stack like the Open Data Kit for KoBo".*

Recommendation 3C

Where possible and practical, make use of implementation grants to fund software-as-a-service licensing, not one-off innovation grants.

Several interviewees advised that humanitarian organizations ought to finance the development of digital identity solutions from implementation grants. Often much larger than innovation budgets and with greater capacity to alter budgets post-hoc, programmatic grants may provide the volume necessary to develop and implement digital identity solutions at scale [#4]. Furthermore, several sources noted that structuring this investment as a service could alleviate long-term challenges in funding and implementing digital identity solutions. An example of such a software-as-a-service (SaaS) funding opportunity was identified by vendors and aid organizations [#7]. The Australian Red Cross is considering a tiered subscription model whereby other non-profits pay to access the database of volunteer credentials. Tykn CEO Jimmy Snoek was also excited about the potential of SaaS pricing where the value that is created by verifying people could be used with external service providers in the sense that financial services providers or mobile network providers would pay for verification costs. The SaaS model could offer a threefold victory: service providers get a new customer base, beneficiaries get a slightly higher degree of socioeconomic inclusion and aid organizations can use and extend the system without having to cover the costs of research and development [#3].

Question 4

What does interoperability among humanitarian organizations using digital IDs look like? When answering this question, one should explore the interoperability of data produced regardless of the technology backend used (e.g., digital credentials issued by different digital ID technologies but using standards such as decentralized identifiers, verifiable credentials, etc.) as well as the processes and willingness to share data between organizations to prevent duplication.

Interoperability is a critical challenge in the development of any digital infrastructure. The MITRE Corporation, an American not-for-profit managing federally funded research and development centres, defines interoperability as "the ability to use resources from diverse origins as if they have been designed as parts of a single system" [26]. Certain legacy technology systems such as email and https power large scale, open ecosystems where users can plug into a variety of providers, services, and other users through an interoperable format for data exchange and portability.

The transition to digital identity solutions is taking place in several industries as users begin to demand better forms of data management that protect their privacy and enhance the security of their data. Similarly, as organizations see cost reductions from the adoption of digital identity solutions, more and more of them are beginning to invest in the development of open standards and frameworks for interoperability. As the ecosystem converges on models of interoperability, humanitarian organizations invested in the development of digital identity solutions are beginning to explore how they might generate interoperability among humanitarian organizations. For humanitarian organizations, realizing effective technical interoperability could mean being able to deliver a wider range of services to beneficiaries, and potentially enabling them to use humanitarian credentials to access services in other sectors.

Critically, interoperability within humanitarian organizations must also be expanded to the variety of stakeholders that humanitarian organizations engage with through the implementation of programmes, which include but are not limited to financial instructions, telecommunications providers, civil society organizations, and community-based organizations. The need for interoperability within the humanitarian sector is especially acute. Multiple organizations can simultaneously have a need for the same beneficiary data. If a single registration can enable beneficiary data to be shared among humanitarian organizations, this would save organizations time and money, sparing beneficiaries from the potential trauma [#2] [#13] (or simply time and hassle) associated with registration processes.

Recommendation 4A

Look to open standards for interoperability and data exchange and portability being developed in other sectors to leapfrog into an open, interoperable ecosystem.

It is likely that, as frameworks for interoperability are developed outside of the humanitarian sector, humanitarian organizations can begin to adopt open data formats and templates from other sectors. However, it is worth noting that there are several challenges to bringing about long-term interoperability within the humanitarian sector. These include:

- financial incentives and competition, which encompass varying needs of humanitarian organizations in terms of access to beneficiary information [#7] [#8]
- the required cultural change
- a general lack of trust in data quality
- complications regarding user trust in environments where they often lack digital literacy.

Recommendation 4B

Cultivate sectoral political will to bring about effective interoperability.

Achieving technological interoperability is often more a question of political will than technical feasibility. Galvanizing the requisite interest in interoperability among key stakeholders is of great importance to the cultivation of meaningful interoperability in the humanitarian sector. Furthermore, organizations need different forms of beneficiary information, so designating one organization to register beneficiaries that will access services from multiple organizations will require a large upfront investment of time and effort to coordinate the needs of all the partners [#7] [#8].

Nonetheless, in the long run, interoperability could yield significant benefits for humanitarian organizations. Digital identity solutions could enable interoperability both within the operations of a single humanitarian organization and among several. Rather than duplicate datasets several times to integrate the efforts of several actors, digital identity systems could enable integrated, real-time access to data and programme operations. Such integrations would dramatically enhance the ability for humanitarian organizations to deliver aid, thereby helping them to accomplish their missions.

Question 5

The promise of self-sovereign ID depends on several factors: digital literacy of end users, infrastructure and access to hardware such as smartphones. Such factors are barriers in places where potential beneficiaries can be among the most vulnerable. How can humanitarian organizations implement digital ID technologies in settings where connectivity is low?

One of the greatest challenges in implementing digital identity solutions in humanitarian settings is a lack of robust connectivity. While there are several workarounds being pioneered by technology vendors across the space including the use of QR codes and paper-based identity documents as a backup for digital systems [#3] [#9] [#14], several key functions performed by digital identity solutions nevertheless require access to stable connection. To perform deduplication, for instance, many digital ID solutions require access to a stable internet connection. However, it is possible to perform certain functions of a digital identity system without a stable connection [27].

Recommendation 5A

In low-connectivity settings, leverage analogue failsafe mechanisms to facilitate authentication without local devices.

Beneficiaries of humanitarian aid often do not have access to sustained connectivity or a local device, such as a smartphone, feature phone, or tablet. In many humanitarian settings, beneficiaries without feature phones will borrow others' phones for certain interactions, including with aid agencies. Despite these challenges, it is possible for humanitarian organizations to implement digital identity systems in low-connectivity settings. Several vendors are exploring partial workarounds for a lack of connectivity. By caching data locally and synchronizing it with other storage nodes when the local device comes into a stable connectivity environment, these solutions can support the identity lifecycle without full and regular access to stable connectivity [#3] [#9] [#14].

To maintain control over their information in a low-connectivity setting, beneficiaries could leverage shared digital wallets [#3] [#9]. By storing several wallets on a single, common device with unique access mechanisms per user, multiple users could access their credentials remotely. Still, the operation of several kinds of digital wallets depends on possession of a smartphone, which many beneficiaries of humanitarian aid do not have. In these cases, the use of analogue authentication mechanisms could support the identity lifecycle without a device. A paper-based barcode, for instance, could enable a beneficiary to authenticate themselves at a point of interaction and gain access to their credentials on a local device hosted by a humanitarian organization [#3] [#9].

Recommendation 5B

In low-connectivity settings, make use of guardianship to facilitate authentication without personal devices.

In low-connectivity settings, it is also possible to make use of workarounds such as guardianship and hosted wallets. Guardianship is a process by which one user takes on the responsibility of managing the credentials of another user [#3]. For example: an elder or young person with physical credentials, or someone without their own phone or having temporary lost their SIM card may have their data managed by a trusted intermediary, such as a family member. A variety of technological approaches can power user centric guardianship of information. For instance, biometrics or voice authentication can be used to provide the user with control over their information on a guardian's device at a point of interaction [#3] [#9] [#14]. Other mechanisms of facilitating user-centric guardianship include the use of split keys [#1] [#9]. By splitting a key among three or more beneficiaries, and then reconstituting a single key at a point of interaction, a beneficiary can control their data across a variety of non-native devices.

Question 6

Tension exists between individuals' desire to retain control over their own data (decentralizing data storage and control for the beneficiary) and organizations' wishes to use individuals' data for coordination purposes (to avoid duplication and fraud) and to be accountable to donors (to demonstrate that assistance is delivered to real people). What are the trade-offs involved in resolving this tension? How can a balance be struck? What are the pitfalls to avoid?

Perhaps the central tension in the implementation of digital identity solutions is between individual and organizational control. The concept of self-sovereign identity is founded on a belief in the sovereignty of an individual's control over their information. The digital world is far from self-sovereign. Powered by relatively few large data brokers, the internet is founded on a federated model of data ownership, whereby users prove their identity through an intermediary. The vision of self-sovereign identity is to subvert this paradigm, placing control of information in the hands of the individual. While many consumers are demanding more user-centric models of data management, organizations continue to argue that, to provide efficient, optimized services, they must process individuals' data. The central tension of the movement for self-sovereign digital identity is, in this sense, the central tension of digital technologies at large.

Recommendation 6A

Humanitarian organizations must recognize that digital identity solutions, properly implemented, could enhance organizational processes all while granting beneficiaries enhanced control over their information.

Digital identity solutions could enable humanitarians to access standardized and verified identity data and programme operations across several different organizations. Perhaps more importantly, digital identity solutions could also streamline and make more efficient registration within an organization.

However, these advantages can only be realized through a negotiation with other organizational priorities and considerations such as providing beneficiaries with access and control over their data. At present, beneficiaries have minimal, if any, control over their information. One Red Cross digital identity pilot expert mentioned that while beneficiaries could input data themselves, they could not determine which aspects of their identity would be shared with which organizations [#12]. Therefore, digital identity solutions could facilitate organizational processes all while enhancing individual beneficiary experiences.

Recommendation 6B

Educate beneficiaries and humanitarians alike to establish meaningful consent and effective systems.

Realizing the above benefits, however, depends on gaining meaningful consent from beneficiaries of humanitarian aid. It can be difficult, or even impossible, to gain true meaningful consent from beneficiaries in programmes leveraging novel technologies such as digital identity solutions. Several interviewees noted that, in addition to the reality that many beneficiaries of humanitarian aid lack basic digital literacy skills, there is also a power asymmetry between those giving and receiving aid, complicating many interactions [#6] [#9] [#12]. Several interviewees noted that humanitarian organizations have a responsibility to build guardrails into the design of digital ID systems such that they inherently minimize and protect user information, so that when users do consent, their information remains as well protected as possible [#2] [#10].

As a white paper published by the Mozilla Foundation notes, "Digital IDs should be designed from their inception to prevent their use as a tool to enable and amplify government and private surveillance. Countries should critically examine whether logging of authentication requests is needed at all, and should certainly put into place laws to limit the retention, accessing, and sharing of authentication records" [28].

To ensure that beneficiaries not only understand what they are consenting to, but are invested in making the programme successful, digital identity solutions must be made useful for them. It is well documented that refugees and displaced people have strategies to resist and play into the framework of aid-related procedures and categories that surround them. Paul Currion cautioned that digital identity solutions may remove many of those resistance strategies and make it more difficult for beneficiaries, rather than less [#6]. For one data rights expert, the existence of channels of contestation and the ability for affected individuals to truly make use of them is the bare minimum that needs to be in place for beneficiaries to have any claim to be seen as legitimate, equal, and rights-bearing human beings. Without the option to resist and contest digital identity-related practices or forms of information control, beneficiaries' data become a "limbo zone in which you can dip in to create things and to collect things ad libitum" [#15]. This was acknowledged by the vendor Tykn, who argued that users need to have the option not to use digital identity solutions from the start and should retain the ability and right to have their data removed from the system even after they have joined [#3].

Question 7

What training in data literacy do beneficiaries of digital IDs require to be able to use them safely? How do these requirements differ between smartphone and feature phone users?

One of the most challenging elements of implementing a digital identity solution is user education. To implement a digital identity solution that is useful to beneficiaries and effective for humanitarian agencies, it is critical that extensive digital literacy and training campaigns be offered to beneficiaries.

Recommendation 7A

Reframe digital literacy training and education as an iterative, two-way process.

Digital identity solutions are both a burden and a privilege for users. While they enable users to manage their information, they also burden individuals with the responsibility of control – not every individual, for example, will be able to make informed decisions about the implications of sharing their data with different types of organizations. Digital identity also presumes a base level of digital, linguistic, and numerical literacy that may not be widespread in humanitarian and development contexts.

Crucially, education must occur at the outset of a digital identity implementation. It must be considered a two-way process by which users enhance their digital literacy and organizations learn how to better serve beneficiaries. Through investing in user-centric design, solutions providers can refine and optimize their solutions for local contexts. For example, vendors Gravity and Tykn use voice authentication rather than cumbersome password-based authentication to better meet the needs of beneficiaries [#3] [#9] [#14]. Likewise, the Netherlands Red Cross followed the suggestion of an elderly woman in St Maarten who complained about the non-intuitive design of their administrative system. In response, the self-completed vulnerability assessment was designed in the style of a WhatsApp conversation whereby beneficiaries supply the information required in a Q&A process with a chatbot. By adapting their solutions to the needs of beneficiaries, vendors can contribute to the long-term adoption, and therefore success, of their technologies.

However, it must be noted that digital literacy can often be a cover for the delivery of services. Several interviewees cautioned that it can reflect neocolonial politics to presume that beneficiaries do not understand or care about their data privacy [#10] [#11]. Humanitarian agencies, they commented, must recognize it is their obligation to help people understand what is happening to their data in a digital identity solution. Most organizations recognize an urgent need to do more to educate their staff and affected communities. Indeed, there is a difference between informing as a box-ticking exercise, and the feeling of being informed. In the words of one interviewee: "I can tell you I have informed someone, but that doesn't mean they have understood it. It's that difference between informed and understanding" [#8].s

Recommendation 7B

Require vendors to incorporate the learning process into their development roadmaps.

Technology vendors should develop digital identity solutions that include learning and beneficiary applications in the interface itself. For example, differences in data types are clearly explained on the interface if users opt to "learn more". When asked for their consent, users can first read what the "do not share" option will mean for them in practice regarding their access to services [#10]. Regardless of whether users attempt to consent or not, they will be presented with another brief statement on the consequences of this option and will be asked again to confirm their selection. The goal is, within the interface, to convey why something needs to be done. The notion of "informing/educating by design" was also echoed by the Netherlands Red Cross. It would be particularly useful, it was argued, if self registration for aid were linked to more intuitive administrative processes [#6]. For example, forms could be filled out in the format of a WhatsApp conversation with a bot. At each step of the process the interface - via text or audio - should explain exactly why they are asked to supply specific information. Indeed, vendors ought to be required to build this sort of user-centric thinking into their development roadmaps to make their solutions more intuitive for beneficiary populations.

121 Consortium Direct Cash Aid in Kenya

Photo credit: Kenya Red Cross Society

Overview

The 121 platform is a direct cash aid system initiated by the 510 team of the Netherlands Red Cross (NLRC). The consortium launched two pilots to test the platform, one in Kenya and another in the Netherlands. In December 2020, a successful pilot was completed in Kenya with support from the GSMA and the IKEA Foundation [29]. The pilot findings give important insight into issues related to the use of digital ID systems in low-connectivity settings (particularly in relation to digital literacy challenges and communication with beneficiaries), the shortcomings of implementing self-sovereign identity (SSI) in humanitarian settings, as well as challenges associated with interoperability and responsible data use in the sector.

The system being piloted consists of two components: digital identity creation and the distribution of cash. The goal is that through a digital identity that beneficiaries create themselves, they have a way to identify themselves with multiple humanitarian organizations. To achieve this value, the project was split into two tracks, one focused on human centred design (HCD) and the other on technology. The technological track covered the creation of the digital ID as well as the cash aid distribution. The main concepts tested included: self-registration, SSI, automated one-way communication through SMS, cash program management and platform integration with M-Pesa. Preparation started in April 2019 to launch the pilot of the minimum viable product in November 2020.

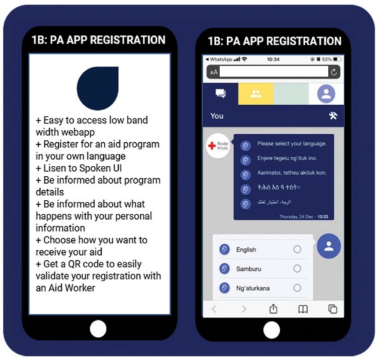
Roles

Integral partners supported different aspects of the pilot. The HCD track was led by NLRC/510 and facilitated by the Kenya Red Cross. Part of this track saw co-design workshops being run with affected people, aid workers from the Kenya and British Red Cross, and representatives from Safaricom. The technological track featured a partnership between NLRC/510 and Tykn. Tykn developed the backend for the SSI component and NLRC/510 developed all the other backend systems, the front-end, and managed the integration of both systems. Disberse was selected to support the development of the backend money flow system, but changes in the timeline due to the global Covd-19 pandemic led the IT departments of NLRC/510 and the Kenya Red Cross to work instead with a local financial services provider, Africa's Talking [30], to distribute the cash aid. The aid distribution stakeholders were the Kenya Red Cross and M-Pesa. Messaging services were semi-integrated with Twillio. For payments, the pilot successfully realized integrations with M-Pesa through Africa's Talking.

Technologies

Beneficiary-based structures

In the Kenya pilot, some affected individuals owned feature phones, while the Kenya Red Cross hardware included tablets with speakers as well as smartphones. Aid was distributed via an M-Pesa SMS or agent. Technology components covered self-registration, communication, and SSI. Users could register via a low-bandwidth web application. Thanks to a WhatsApp chat-style system, users would register for and be informed about the aid programme in a language of their choosing.[3] This 121 tone of voice was co-written by the HCD team and volunteers, Kenya Red Cross volunteers, and a volunteer professional user experience (UX) copywriter. Registration could also be done by listening to a spoken user interface; the interface voice was recorded via WhatsApp message by local volunteers. A copy of all the text was held on the Transifex platform so that it could easily be translated and then loaded back onto the NLRC/510 system. This made it easier for local volunteers to help translate additional aspects for end users. UX changes were made in response to difficulties encountered by users concerning the design of buttons in the interface – beneficiaries tended to press and hold rather than simply tap these.



1B: PA APP REGISTRATION

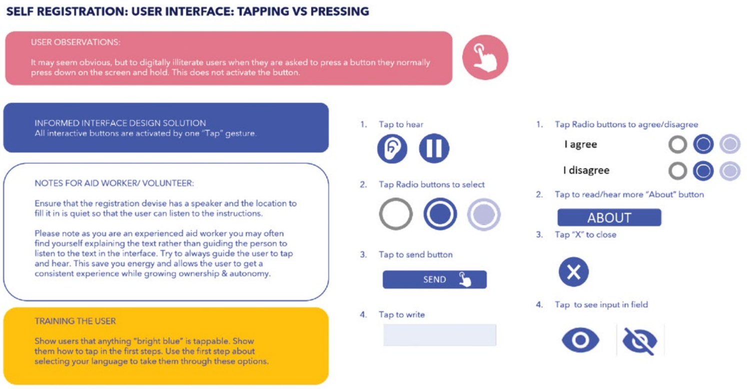
+ Easy to access low band width webapp
+ Register for an aid program in your own language
+ Lisen to Spoken UI
+ Be informed about program details
+ Be informed about what happens with your personal information
+ Choose how you want to receive your aid
+ Get a QR code to easily validate your registration with an Aid Worker

1B: PA APP REGISTRATION

Please select your language.
Enjere tegelu ng'ituk ino.
Aarimatoi, tetheu akituk kon.
ትሕስ እስ ዓ ተስተ፡፡
الرجاء اختيار لغتك
Thursday, 24 Dec - 10:33

English ○
Samburu ○
Ng'aturkana ○

Source: 121 Product Roadmap, December 2020, p.13



SELF REGISTRATION: USER INTERFACE: TAPPING VS PRESSING

USER OBSERVATIONS:

It may seem obvious, but to digitally illiterate users when they are asked to press a button they normally press down on the screen and hold. This does not activate the button.

INFORMED INTERFACE DESIGN SOLUTION
All interactive buttons are activated by one "Tap" gesture.

NOTES FOR AID WORKER/ VOLUNTEER:

Ensure that the registration devise has a speaker and the location to fill it in is quiet so that the user can listen to the instructions.

Please note as you are an experienced aid worker you may often find yourself explaining the text rather than guiding the person to listen to the text in the interface. Try to always guide the user to tap and hear. This save you energy and allows the user to get a consistent experience while growing ownership & autonomy.

TRAINING THE USER

Show users that anything "bright blue" is tappable. Show them how to tap in the first steps. Use the first step about selecting your language to take them through these options.

1. Tap to hear
2. Tap Radio buttons to select
3. Tap to send button
4. Tap to write

1. Tap Radio buttons to agree/disagree
2. Tap to read/hear more "About" button
3. Tap "X" to close
4. Tap to see input in field

Source: 121 Product Roadmap, December 2020, p.16

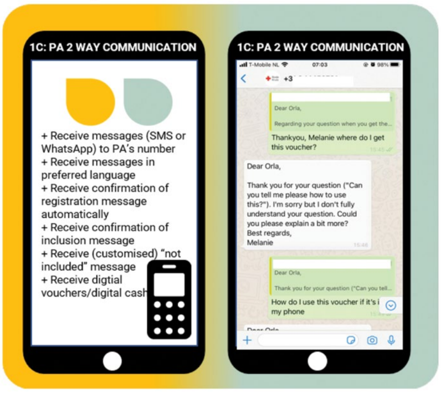
[3] Current translations include Turkana, Samburu, Arabic and Tigrinya, with plans to translate to Dutch, French and Kiswahili.

Tykn and NLRC/510 entered into a technical partnership to further the SSI agenda in the humanitarian sector by developing and integrating the technology into the wider 121 platform. The technical infrastructure was functional, but did not add value for those affected, in part due to constraints such as low smartphone penetration and poor internet connectivity. The difficulties encountered led 121 to conclude that Sovrin and SSI currently have no value for the 121 platform.[4] Beneficiaries' digital wallets were stored centrally as the team did not continue the development of decentralized storage. A cloud-based server remains an option, as do an independent python server and Sovrin. Nonetheless, SSI was found to have value in that it promoted privacy by design and responsible data use. It also "paved the way" for self-registration, which can significantly cut registration times, although this is not a given and depends on instructions, the length of the registration process, and so on.

Systems for Humanitarian Organizations

The portal for cash information management was designed to handle bulk registrations and support handling sensitive data. The humanitarian organization portal is a software solution accessible through any browser. It enables managing the cash-based aid programme from start to finish, including communication via SMS and WhatsApp and payment completion via digital vouchers and M-Pesa.

Payments can be completed with a push of a button, although complete technical registration with the financial services providers involved is challenging. It is worth clarifying that this challenge does not come from the coding requirement or application programmer interface (API) integration. Rather, it is the process of accessing contacts and changing processes within the humanitarian organization that are challenging. Likewise, the team found it essential to be able to distribute cash in physical form when digital vouchers or cash were problematic. A better understanding of the market size of technical integration of financial services providers with humanitarian practices is a key priority for the near future.



1C: PA 2 WAY COMMUNICATION

+ Receive messages (SMS or WhatsApp) to PA's number
+ Receive messages in preferred language
+ Receive confirmation of registration message automatically
+ Receive confirmation of inclusion message
+ Receive (customised) "not included" message
+ Receive digtial vouchers/digital cash

1C: PA 2 WAY COMMUNICATION

Dear Orla,

Regarding your question when you get the...

Thankyou, Melanie where do I get this voucher?

Dear Orla,

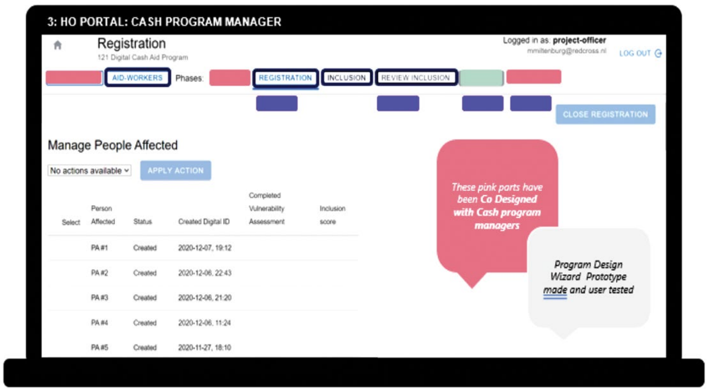
Thank you for your question ("Can you tell me please how to use this?"). I'm sorry but I don't fully understand your question. Could you please explain a bit more?
Best regards,
Melanie

Dear Orla,

Thank you for your question ("Can you tell...

How do I use this voucher if it's i my phone

Source: 121 Product Roadmap, December 2020, p.20



3: HO PORTAL: CASH PROGRAM MANAGER

Registration
121 Digital Cash Aid Program

Logged in as: **project-officer**
mmiltenburg@redcross.nl

Manage People Affected

Select	Person Affected	Status	Created Digital ID	Completed Vulnerability Assessment	Inclusion score
	PA #1	Created	2020-12-07, 19:12		
	PA #2	Created	2020-12-06, 22:43		
	PA #3	Created	2020-12-06, 21:20		
	PA #4	Created	2020-12-06, 11:24		
	PA #5	Created	2020-11-27, 18:10		

These pink parts have been Co Designed with Cash program managers

Program Design Wizard Prototype made and user tested

Source: 121 Product Roadmap, December 2020, p.27

Analysis

The Kenya case study illustrates important points about the challenges associated with driving interoperability and responsible data practices in the humanitarian space, as well as the incompatibility of self-sovereign identity systems, and ways to overcome barriers imposed by low-connectivity settings.

Many of the points covered in this analysis correspond with findings from the interviews presented above with key stakeholders who repeatedly emphasized that digital ID deployment in the humanitarian sector is severely constrained by the operating culture within humanitarian organizations and their

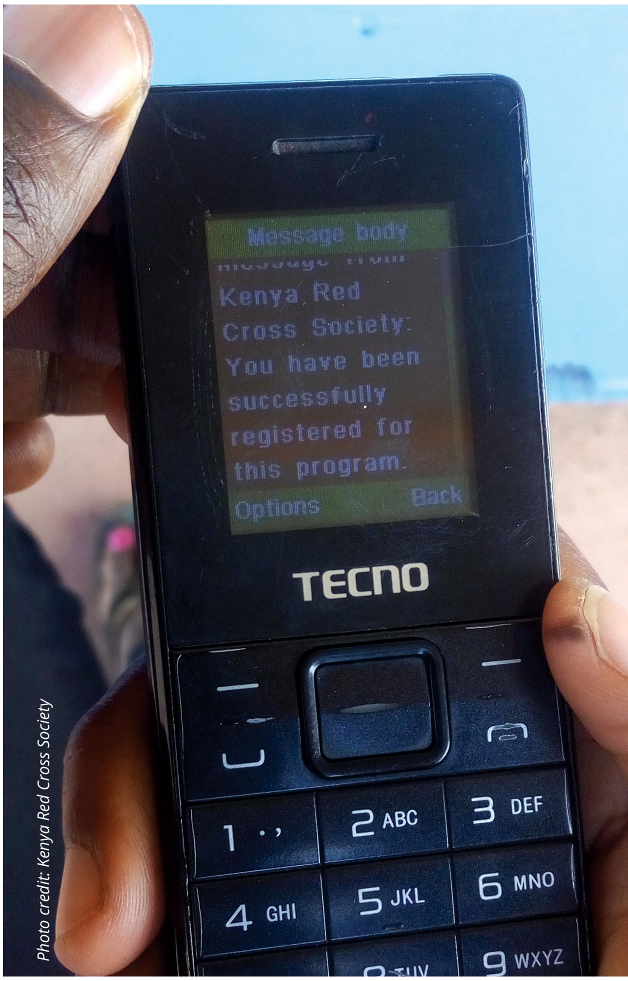
[4] This conclusion was confirmed in an unpublished set of meeting notes from 3 November 2020.

own lack of digital literacy. This is despite significant advances in and successful deployments of the necessary technical infrastructure.

Interoperability

From their work on various pilots, NLRC/510 concluded that it cannot be assumed that all organizations desire digital interoperability. According to NLRC/510's vision report for 2021, "It is difficult to test whether organizations will want to standardize their data collection across the sector." Interoperability must also be improved with financial services providers, perhaps by having them open services through programmable interfaces. Most challenging is the need for trust. Humanitarian actors need to accept the validated identity attributes created by partner organizations. While technology on its own may make this a possibility, organizations must coordinate to make interoperability work in practice. As confirmed by interviewees, a significant obstacle is the fact that there is no previous experience with interoperability among humanitarian organizations. Coordination is required not just regarding registration, but also for targeting, selection criteria, amounts, and so on. NLRC/510 believes that such coordination mechanisms must be centrally organized and that some functionalities could be included in the 121 platform to support these coordination mechanisms. For example, a beneficiary being obliged to share their record of receiving aid upon registration. This could both reduce duplication and improve coordination as it would increase organizational awareness of previous programmes. This functionality is still to be developed, meaning deduplication using SSI is not easy. Moreover, even if such functionality were to be established, technology does not solve all coordination issues. Organizations would still have to trust this system and it would only work once a network effect had been established. As with most challenges facing the use of digital ID systems in humanitarian contexts, sociopolitical and technical challenges are intertwined.

Photo credit: Kenya Red Cross Society



Message body

Message from Kenya Red Cross Society: You have been successfully registered for this program.

Photo credit: Kenya Red Cross Society

From 121 project implemented by Kenya Red Cross Society, 510, British Red Cross and Funded by GSMA.

SSI currently has no value for the 121 platform

At the end of 2020, NLRC/510 concluded that SSI currently has no value for the 121 platform. SSI was too difficult to implement given the lack of responsible data practices, constraints presented by low connectivity settings, and regulatory challenges. Across a range of pilot projects, it was observed that humanitarian organizations wish to work with partners familiar with the affected populations or with a human in the loop, rather than digitally accepting beneficiary identities. Organizations would also have to enhance internal digital literacy to work with SSI. Whether organizations involved in a given SSI-based programme are sufficiently digitally literate or not is difficult to verify, which raises uncertainty and undermines trust. This speaks to a wider issue of digital transformation within the sector that was evident with challenges posed by lacking data security practices. At present, there is no way to prevent the collection and digitization of surplus data. Moreover, legal reasons and donor requirements may pressure organizations to store personal information for set durations. Like other interviewees, NLRC/510 reported facing requests to enable humanitarian organizations to access and even download personal information.

Most importantly, it is not clear that there is a need for reusable digital identification. Humanitarians have mentioned the benefit of moving from functional digital ID to more foundational forms of identification or even building behavioural trails to be used as alternative forms of credit scores or risk assessments to help beneficiaries in the long-term, but at present these are mere hopes as nowhere has the regulatory environment adapted to realize this goal. This removes the grounds for an argument for SSI based on the value of a reusable digital ID. NLRC/510 affirmed that governments must first prioritize privacy and act on it for the privacy movement, of which the SSI aspiration is a component, to catalyse any changes.

Finally, SSI is impractical because it requires users to have good internet connectivity and (for full functionality) smartphones, as well as high digital literacy – all of which are unlikely in conditions where most humanitarian organizations work. Likewise, SSI development is resource intensive and the aid sector is a conservative one. NLRC/510 has committed to stop working towards SSI, removing SSI components from existing systems, and to move forward with central data storage and simpler, less resource-intensive solutions.

Digital ID in low-connectivity and low digital literacy settings

Design decisions taken in the project responded to the constraints of a low-connectivity setting. One example is the WhatsApp-style communication system for registration and user support. This component was added specifically in high-digital but low-physical access situations, such as:

- undocumented migrants in the Netherlands
- people affected by conflict in Ukraine
- people in post-hurricane St Maarten.

Another example is the use of an audio-based interface. The limited internet connectivity and low smartphone penetration also led the team to abandon an SSI-based solution. The technology track partners even applied for funding to develop a solution for feature phones, but the application was unsuccessful.

The Kenya pilot revealed important lessons on how to best communicate with beneficiaries unfamiliar with operating a digital interface. A workshop was held to help users create and remember their passwords. The concept of a password can prove challenging and recall can be particularly difficult for trauma survivors. Interface components that proved challenging included: buttons in general (difficult to use), “about” buttons in particular (not used or poorly understod), typing, the concepts of accounts and data privacy.

Sikka Distributed Ledger Technology-based Digital Asset Transfer Platform

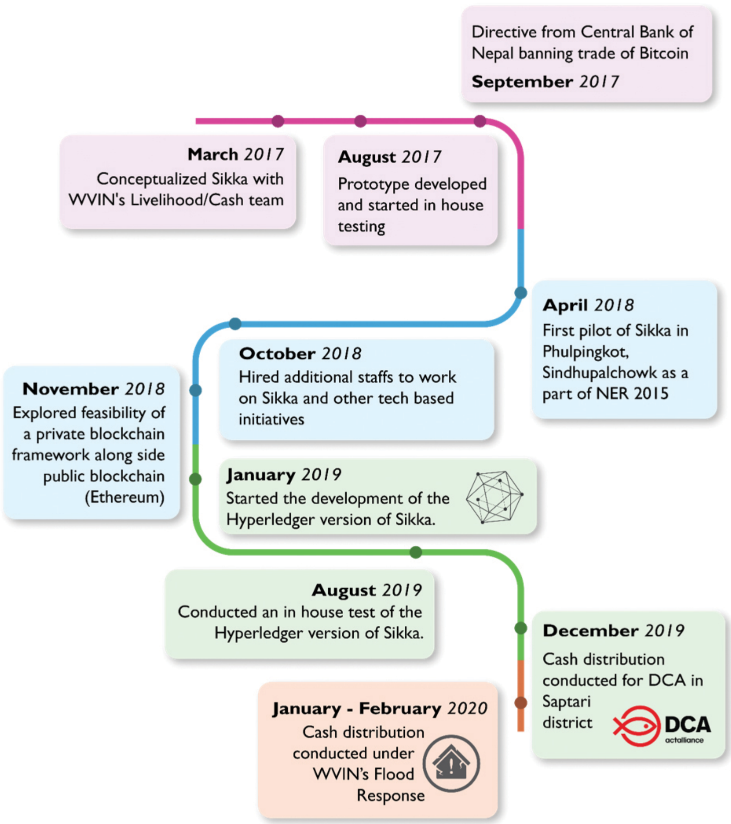
Photo credit: World Vision International

Overview

Sikka, which means “coin” in Nepali, is a digital assets transfer platform designed, funded, and deployed by World Vision International’s Nepal Innovation Lab in Kathmandu. The platform addresses the challenge of financial access in the form of cash-based assistance during crises by relying on blockchain technology and digital tokens. In disaster response situations, manual cash-transfer processes generate logistical complications, operational costs, and have limited transparency. These challenges are further complicated by a lack of infrastructure and services in rural areas. Blockchain technology serves to enable digital token transactions via cellular networks. Users can securely access cash or commodities through the digital wallets they receive upon enrolment. Wallets are linked to a mobile number, which serves as the user ID on the Ethereum blockchain (which has one node and one controlling entity). Sikka does not implement its own identity management system. As a locally designed solution based explicitly on human-centred design, Sikka’s services are designed with the end user’s existing knowledge and available technology in mind: all services are based on

SMS functionality compatible with any basic feature phone and low-connectivity scenario. In addition to values of accessibility and network resilience, Sikka emphasizes accountability as every transfer between beneficiaries, vendors and cooperatives takes place via immutable transaction logs. The images below illustrate how Sikka has matured and how it works. Since 2020, Sikka has been deployed in response to the Covid-19 pandemic [31]. Future developments include exploring the creation of a new token standard, a hyperledger version of Sikka and the implementation of an existing blockchain-based identity verification process.

Sikka Timeline



Directive from Central Bank of Nepal banning trade of Bitcoin
September *2017*

March *2017*
Conceptualized Sikka with WVIN's Livelihood/Cash team

August *2017*
Prototype developed and started in house testing

April *2018*
First pilot of Sikka in Phulpingkot, Sindhupalchowk as a part of NER 2015

October *2018*
Hired additional staffs to work on Sikka and other tech based initiatives

November *2018*
Explored feasibility of a private blockchain framework along side public blockchain (Ethereum)

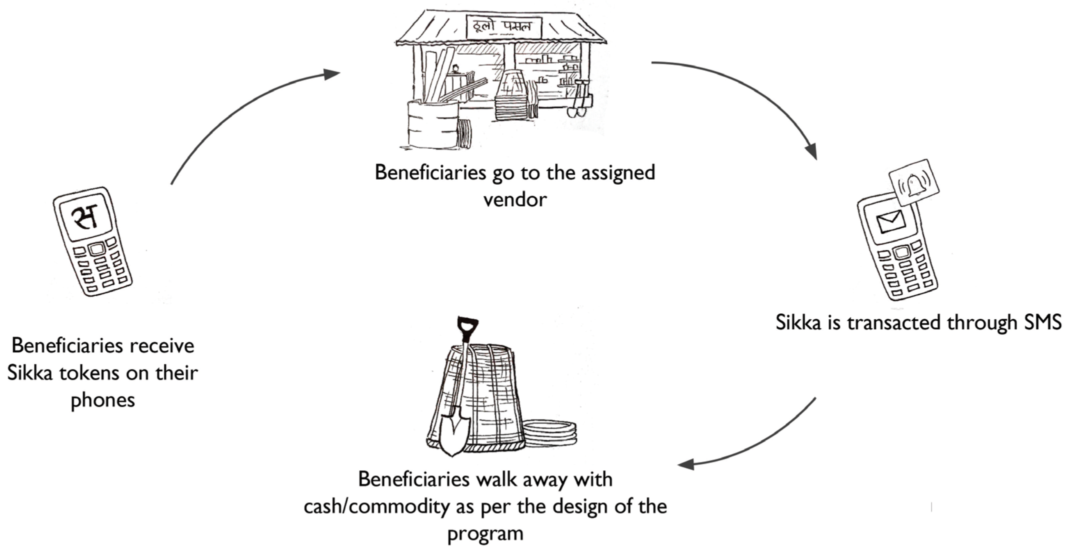
January *2019*
Started the development of the Hyperledger version of Sikka.

August *2019*
Conducted an in house test of the Hyperledger version of Sikka.

December *2019*
Cash distribution conducted for DCA in Saptari district

January - February *2020*
Cash distribution conducted under WVIN's Flood Response

A user's perceptive of Sikka's funds pathways



Beneficiaries go to the assigned vendor

Sikka is transacted through SMS

Beneficiaries walk away with cash/commodity as per the design of the program

Beneficiaries receive Sikka tokens on their phones

Roles

Sikka's functionality is embedded within an ecosystem of aid actors. The system is described as a digital asset transfer network because the tokens can represent access rights to a variety of goods. The token will hold value only within the web of interactions between the aid organization, beneficiaries, vendors and/or financial cooperatives, and these agents are responsible for setting the token's value. Crucially, Sikka works with local vendors and financial services providers to reduce the hassle whereby beneficiaries must travel long distances to receive support. For beneficiary identity registration and management, Sikka relies on partner NGOs to use their own existing processes. Between designing and funding the system through World Vision International, outsourcing these processes, partnering with locally active financial actors, deploying their token contract to the Ethereum main network, and running the system through SMS and thus via mobile network operators, no additional external support is required to operationalize the Sikka system. That said, Sikka does work with financial cooperatives in Nepal to help them address their tendency to have high liquidity risks, which often impedes them from working with aid or charitable organizations. As project coordinator Soujanya Acharya explained, "By tracking assets over a distributed ledger, Sikka provides the basis upon which some basic banking software features can be implemented to digitize processes and records, which [helps build trust between parties]." Sikka is also exploring using Infura's infrastructure as an alternative to maintaining their own node. In terms of funding, Sikka is "fully owned by World Vision International and conducts its own fundraising through traditional methods according to established organizational rules and policies" [32]; for these reasons it will never run on initial coin offering (ICO).

Technologies

Ethereum-based

Sikka operates via a single controlling entity on the Ethereum main network to manage the creation, distribution, and validation of transactions within aid programming. The token is an ERC20 (Ethereum Request for Comments 20) contract. Because the tokens can represent access rights to a variety of goods, Sikka can be used to represent any currency or digital asset to be pegged to commodities (such as a litre of oil, a bag of rice, or construction materials) relevant to the needs defined by aid organizations, beneficiaries, vendors or financial cooperatives present in the situation in question. Tokens are not cryptocurrency; their value is determined by the ecosystem of actors. Users trade through their Sikka wallets, which are tied to their mobile phone numbers and received upon enrolment. Mobile numbers serve as the user's ID on the blockchain. Sikka tokens are then sent via SMS to purchase goods, services, or redeem tokens as e-vouchers for cash or at a local financial cooperative. Whenever a user makes a transaction through SMS, a transaction is triggered on the blockchain. Once the transaction is complete, the user receives a confirmation by SMS.

Photo credit: World Vision International

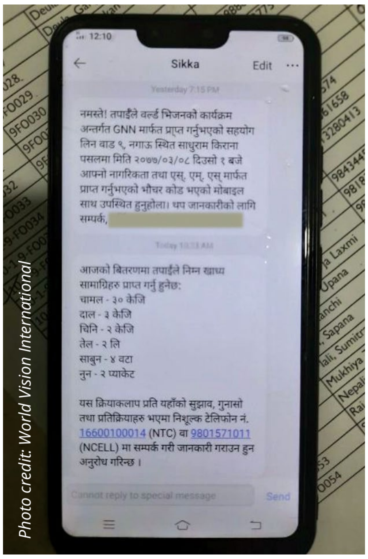
Photo credit: World Vision International

Digital ID Functionality

Having no proprietary identity management system, Sikka relies on partner NGOs to register and enrol their beneficiaries. This decision is based on the complicated and sensitive nature of implementing a digital ID solution. Sikka may soon work with an existing solution that "might include a blockchain based identity verification process" [32]. In 2018, an API was developed to allow existing beneficiary management systems to directly plug Sikka into such a system. The goal of this functionality is to allow aid agencies to incorporate Sikka as a last-mile payment option into their existing ID management system. The API has been in operation since 2019 to support the disbursement of tokens and retrieval of transaction data.

Security

Sikka benefits from the security of Ethereum's hashrate and therefore does not need to run their own privacy network. Tokens on the blockchain benefit from cryptographic security features including being immune to counterfeiting and the element of transparency and verifiability of transactions [33]. Digital wallets are stored on Sikka's servers and are associated with the user's SIM card such that funds can only be accessed via network vendors or financial cooperatives that have been approved. The team pledges to follow industry standard security practices for web-based applications and to constantly re-evaluate these and implement updates. Data are backed up; from the onset, Sikka follows the principle of data minimization such that no unnecessary personally-identifiable information is stored on their servers or anywhere on the blockchain [34]. Data sharing practices with partners' systems reflect this commitment: a list of beneficiary phone numbers is shared along with an optional unique identifier to facilitate report generation.



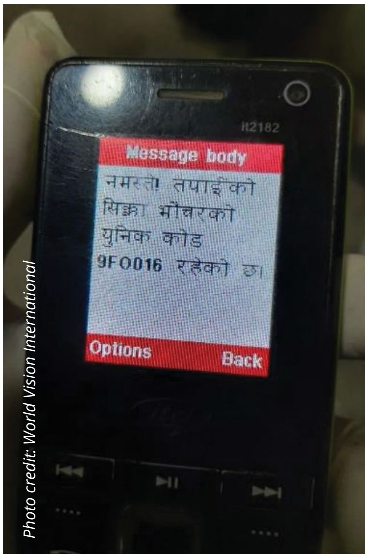
नमस्ते! तपाईंले वर्ल्ड भिजनको कार्यक्रम अन्तर्गत GNN मार्फत प्राप्त गर्नुभएको सहयोग लिन वाड ९, नगाऊ स्थित साधुराम किराना पसलमा मिति २०७७/०३/०८ दिउसो १ बजे आफ्नो नागरिकता तथा एस्. एम्. एस् मार्फत प्राप्त गर्नुभएको भौचर कोड भएको मोबाइल साथ उपस्थित हुनुहोला। थप जानकारीको लागि सम्पर्क, [redacted]

आजको बितरणमा तपाईंले निम्न खाद्य सामाग्रिहरु प्राप्त गर्नु हुनेछ:
चामल - ३० केजि
दाल - ३ केजि
चिनि - २ केजि
तेल - २ लि
साबुन - ४ वटा
नुन - २ प्याकेट

यस क्रियाकलाप प्रति यहाँको सुझाव, गुनासो तथा प्रतिक्रियाहरु भएमा निशूल्क टेलिफोन नं. 16600100014 (NTC) वा 9801571011 (NCELL) मा सम्पर्क गरी जानकारी गराउन हुन अनुरोध गरिन्छ ।

Photo credit: World Vision International

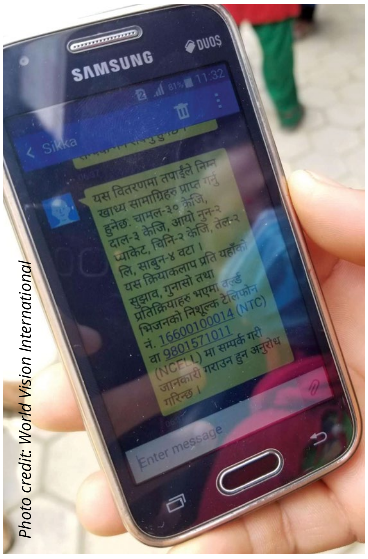
Image 1: Humanitarian accountability messaging



नमस्ते तपाईंको सिक्का भौचरको युनिक कोड 9FO016 रहेको छ।

Photo credit: World Vision International

Image 2: Voucher code sent through SMS from Sikka in a feature phone



यस वितरणमा तपाईंले निम्न खाध्य सामाग्रिहरु प्राप्त गर्नु हुनेछ: चामल-३० केजि, दाल-३ केजि, आयो नुन-२ प्याकेट, चिनि-२ केजि, तेल-२ लि, साबुन-४ वटा । यस क्रियाकलाप प्रति यहाँको सुझाव, गुनासो तथा प्रतिक्रियाहरु भएमा वर्ल्ड भिजनको निशूल्क टेलिफोन नं. 16600100014 (NTC) वा 9801571011 (NCELL) मा सम्पर्क गरी जानकारी गराउन हुन अनुरोध गरिन्छ ।

Photo credit: World Vision International

Image 3: Beneficiary reading sikka message about the details of distribution

No to Dapp or ICO

Sikka is not a distributed application (Dapp) nor does the team aspire for this in the future as they do not find it relevant given their current problem statement. UNOPS Blockchain support analyst Jef Davis has also confirmed that Sikka will never run on ICO as this process is designed to enable investors to profit from the value of a utility token used within the application. Sikka tokens are not market-traded commodities themselves nor is there a need for such a token to meet the needs addressed by Sikka.

Upcoming Technological Features

The Sikka team is looking into a blockchain-based identity verification process, implementing a new token standard, exploring an alternative infrastructure rather than maintaining their own node, and developing a hyperledger version of Sikka. The new token standard is defined in ERC865 and would help reduce transaction costs for Sikka tokens. This standard allows a third party to carry out transactions on behalf of the sender, meaning there would be no need to provide beneficiaries' wallets with Ethereum to carry out individual transactions. Cost reductions would also be possible also possible if Sikka were to use Infura's infrastructure; this would cut costs associated with maintaining their own node and server. Although cost reduction may be an objective, Sikka reduced the cost per beneficiary by 78 per cent[5] in the 2019 pilot. A hyperledger version of Sikka is also in preparation to run in tandem with the current Ethereum version; this should allow agencies to use Sikka's voucher system openly when working in countries where there are strict policies in place around blockchain and cryptocurrencies. Even though Sikka tokens are not a cryptocurrency, "gas charges" associated with their use will require payments to be made in Ethereum which may block Sikka as an option for aid agencies operating in regulatory environments that do not support blockchain- or cryptocurrency-based transactions.

Analysis

Sikka is an interesting use case of digital ID because it represents a high-tech project that is highly effective over time in a variety of contexts, with a range of partners, including in low-tech settings. In addition, the first generation of the system has proven flexible enough to encourage continued innovation in terms of technological advances such as a hyperledger iteration as well as adaptation to a broader range of use cases. The challenges Sikka has faced are also informative.

Design and deployment decisions are based on a commitment to meeting user needs. The interface and infrastructure fit the needs and skills of the end users. Likewise, local design is a cornerstone of the project; the team is managed and the code developed and maintained by Nepali nationals in Nepal. For these reasons, Sikka's solution is entirely based on the knowledge of the end users' existing knowledge. For example, Sikka makes use of text messages because this is what most users are already familiar with. Furthermore, there is no requirement for organizations to distribute any additional hardware or materials (such as debit cards) to beneficiaries for Sikka to function. Like many other contemporary digital ID based humanitarian assistance programmes, the team is looking into implementing Interactive Voice Response services to drive accessibility.

Photo credit: World Vision International

Photo credit: World Vision International

[5] In the 2018 field trial, the cost per beneficiary was 6.972 US dollars. In 2019, the figure was 1.54 US dollars (1.42 Swiss francs / 1.29 euro). 583,000 Nepali Rupees (5,500 US dollars) were distributed to 73 beneficiaries; and the costs for Ethereum and SMS amounted to less than 0.50 US dollars per beneficiary.

Despite these intentional design choices, Sikka has faced a range of challenges from regulators and end users. A major barrier is the need to educate regulators about how blockchain works. Blockchain is often associated with misconceptions and assumptions related to illegal activity. This is not just a marketing or branding difficulty, but something that influences the regulatory environment. In 2017 for example, Sikka were ready for their first pilot but Nepal Rastra Bank banned all activities related to the transfer of cryptocurrencies. Though Sikka did not deploy a cryptocurrency, they took a step back to reconsider their design structure to make sure to never be misunderstood as a cryptocurrency-trading platform. The current decision to explore a hyperledger version of Sikka is a response to the same regulatory challenge. Beneficiaries also faced challenges. Those who subscribed to smaller mobile carriers had difficulty sending and receiving SMS while others did not know how to use a feature phone well enough to redeem tokens without assistance. The new token standard is a response to this challenge such that Sikka can still work for fringe cases that require additional assistance due to impaired vision or a lack of network connectivity, technical understanding, phones or literacy skills.

Sikka may lend itself to three unexplored use cases. First, it could help strengthen microfinance services if adequate normative and ethical boundaries we established, according to the Convergences platform [35]. Second, HumanityX used Sikka as an example in their decision tree to help weigh the benefits and risks of using blockchain for humanitarian aid; Sikka demonstrated how tokenizing fiat helps avoid volatility and regulations surrounding cryptocurrency and boosts transparency [36]. Third, the Sikka team believes Sikka might act as a surrogate system for accessing other vital services during disasters (such as cash for work during response, recovery and reconstruction) which could add a layer of functionality among communities with established financial services partners [33].

Photo credit: World Vision International

Photo credit: World Vision International

Photo credit: World Vision International

SDG Impact Accelerator Digital ID Pilots in Turkey

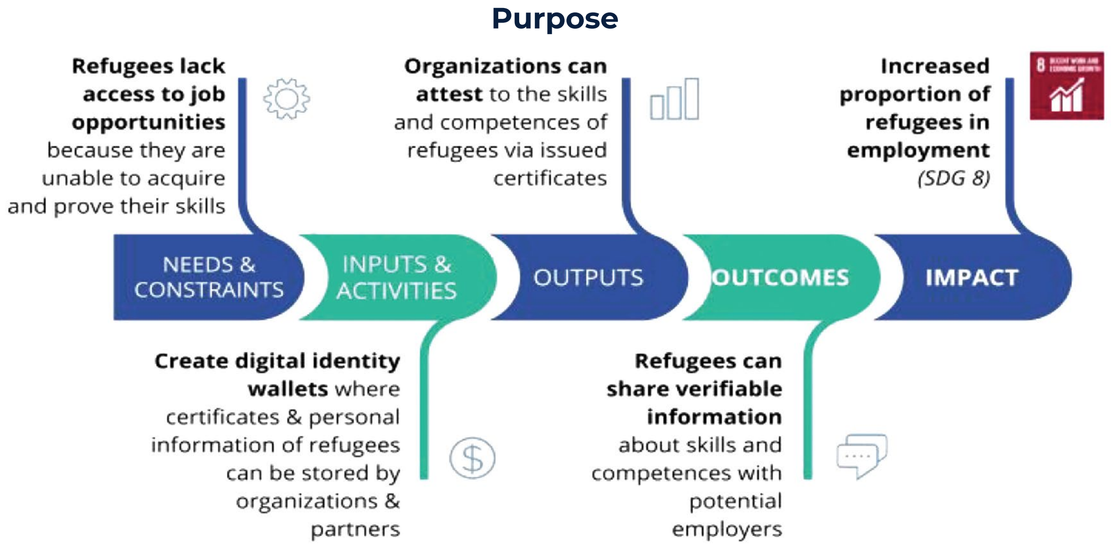
Photo credit: Gravity

Overview

The Sustainable Development Goals impact accelerator (SDGia) was established by the Turkish Ministry of Foreign Affairs and UNDP to generate market-creating innovations for refugee and least developed country populations [37]. The programme's first "Accelerator Bootcamp" was launched in July 2019 in Istanbul and Ankara. One of the startups involved is the influential technology partner for humanitarian digital ID projects: Gravity. Although other digital ID-related pitches were presented, including by Tykn, the technology partner in the 121 consortium, Gravity's work is selected as a case study here because their solution included close collaboration with four other organizations from the start. It thus offered a rife example of interoperability challenges associated with digital ID systems, as well as how the same systems may be used to overcome existing coordination challenges. Moreover, Gravity has made more documentation of this project publicly available.

Gravity positioned their decentralized identity platform to enhance "humanitarian coordination" through a digital wallet for educational credentials [38]. The project's beneficiaries are displaced people who have attended vocational training and Turkish language courses at the Gaziantep Chamber of Industry and the Gaziantep Chamber of Artisans and Craftsmen. Following the pitch, the project took place over the course of six months (July-December 2020).

Gravity observed that refugees needed to overcome significant barriers to maximize their chances for employment, and that there were too many organizations providing training opportunities with no coordination mechanism. This led to beneficiaries taking random courses rather than those needed to develop a specific skill. Organizations were not able to identify duplicates. The solution was to use Gravity's decentralized identity platform to create digital wallets for beneficiaries. Beneficiaries store their training certificates on their digital wallet. Programme managers can then reach out in a targeted fashion to certain segments of the population based on skills or demographics. Donors can follow anonymized trajectories of people through the system up until employment to measure impact. The system maintains total privacy, for at no point is there a requirement for sensitive identity data to be stored or exposed. The final product improves refugees' chances for employment and organizations' accountability to donors.



Refugees lack access to job opportunities because they are unable to acquire and prove their skills

Organizations can attest to the skills and competences of refugees via issued certificates

Increased proportion of refugees in employment *(SDG 8)*

Create digital identity wallets where certificates & personal information of refugees can be stored by organizations & partners

Refugees can share verifiable information about skills and competences with potential employers

Source: Thakur, January 2020 via Medium

Roles

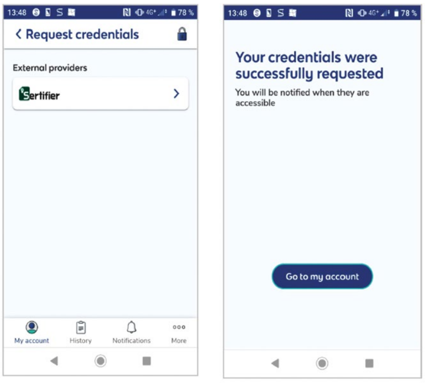
Gravity partnered with consortium partners, Sertifier and Mark Labs, to create the collaborative platform, as well as with two local governance branches, the Gaziantep Chamber of Industry (GSO) and the Gaziantep Chamber of Artisans and Craftsmen (GESOB), which provide language and vocational training for displaced people. In the second phase of the pilot, local employers also took part.

Sertifier [39] is an implementation partner; beneficiaries' education certificates are issued through Sertifier's interface directly onto their digital wallets. Mark Labs provides the capability to create a data ecosystem to track and optimize impact [40]. GSO and GESOB were consulted to review the status quo of beneficiary data collection and management, and to understand the journey of beneficiaries from receiving training to gaining employment. In their feedback on the pilot project, GSO and GESOB reported they found the decentralized data sharing platform useful in terms of coordination and to uphold beneficiaries' data privacy [41]. Placing beneficiaries at the core of data sharing reduced the friction local partners might otherwise face when interacting with beneficiaries and employers alike. In the product development phase of the pilot, Gravity developed a new feature so that beneficiaries could share their credentials with whomever they like, even if they are outside the Gravity ecosystem. Currently, beneficiaries can share certificates with seven enterprises in industries ranging from hardware and mechanical manufacturing to information technology and cosmetics. These employers, in turn, can view the history of a beneficiaries' completed training with GSO and GESOB and verify their origin and authenticity. This process had previously consisted of GSO and GESOB introducing beneficiaries to employers by visiting their premises.

Technologies

Gravity deploys decentralized identity such that every beneficiary can receive, store, and share data on a digital wallet to which only they have access. Users control what information is shared with which entity such that no other entity can access this data without their consent. Participants receive guidance on how to create and use their wallets via an informational video and in-person assistance. Few difficulties[6] in registration were reported in the pilot and those that surfaced were channeled into refining features and process flows for the next iterations. The Gravity web-based application is available in Turkish and Arabic, to allow beneficiaries, GSO and GESOB personnel and potential employers to use the platform easily.

Integrations were required between Gravity and Sertifier so that digital credentials could be certified. Additional features were built so that users could share credentials with any interested employer or third party and so these could in turn verify that the credentials were indeed issued by GSO or GESOB via a browser-based verification portal. Images of the integration between Gravity and Sertifier and the employer verification portal are below.



‹ Request credentials

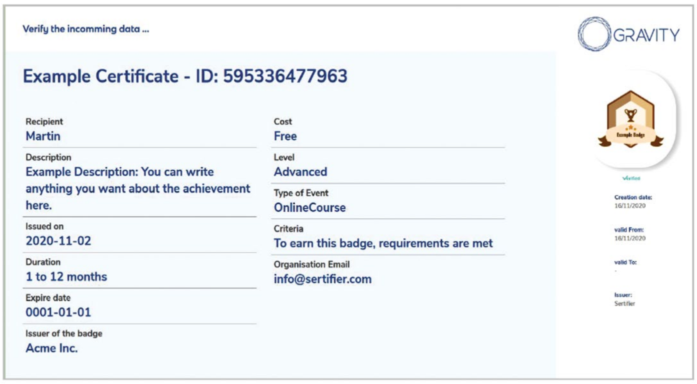
External providers

Sertifier ›

Your credentials were successfully requested

You will be notified when they are accessible

Source: Thakur, January 2020 via Medium



Verify the incomming data ...

Example Certificate - ID: 595336477963

Recipient
Martin

Description
Example Description: You can write anything you want about the achievement here.

Issued on
2020-11-02

Duration
1 to 12 months

Expire date
0001-01-01

Issuer of the badge
Acme Inc.

Cost
Free

Level
Advanced

Type of Event
OnlineCourse

Criteria
To earn this badge, requirements are met

Organisation Email
info@sertifier.com

Verified

Creation date:
16/11/2020

valid From:
16/11/2020

valid To:
-

Issuer:
Sertifier

Source: Thakur, January 2020 via Medium

Analysis

Gravity's experience in Gaziantep demonstrates the value of public-private partnerships as well as how substantial interoperability can be achieved without sacrificing data privacy or individuals' control over their own data. The example also demonstrates a valuable use-case of how digital ID systems can help migrants throughout their journey. Digital ID systems are commonly piloted to support crisis response or more immediate humanitarian assistance, including initial registration for aid as well as short-term assistance, whether in the form of food or cash transfers. Gravity's work facilitates a vital next step: helping refugees acquire and prove their education and training credentials so they can advance their level of socioeconomic inclusion. Crucially, the Gravity solution was able to help all stakeholders: beneficiaries, aid and training organizations and employers.

The potential for digital ID systems to generate long-term value for migrants on their journeys is only enhanced by comments from the Gravity team in their interviews. Multiple Gravity representatives were enthusiastic about the potential for digital ID systems to help beneficiaries establish an alternative credit trail whereby their trustworthiness could be established by their record of interactions with training providers, employers, and even financial institutions. Ideally, this could help them interact with formal financial structures and support their continued socioeconomic integration.

[6] Issues encountered by about 5 per cent of beneficiaries during registration were: not having an active SIM card (required to receive one-time password) and difficulties uploading the cryptographic key file (particularly affecting iPhone users).

Unresolved problems with this model must be addressed. It is unclear how the project can be funded in a more sustainable manner that is independent of SDGia grants. Another issue is how the programme can avoid furthering patterns of exclusion based on unequal levels of access to mobile phones and digital literacy that are prominent even in recently resettled migrant populations living in Gaziantep. This point is particularly pressing as patterns of exclusion often disadvantage women.

Photo credit: Gravity

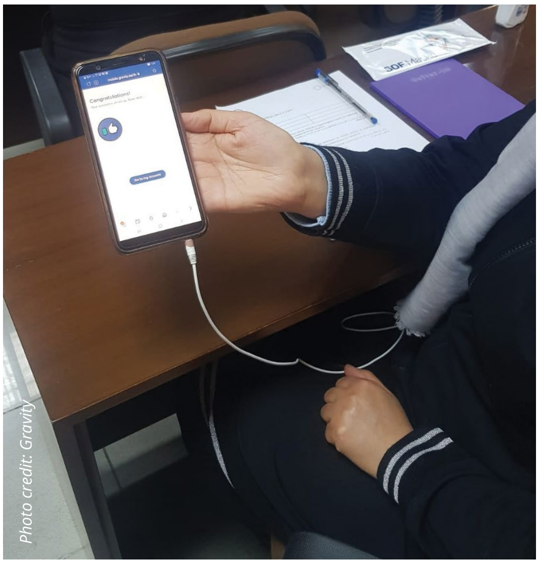


Photo credit: Gravity

Photo credit: Gravity

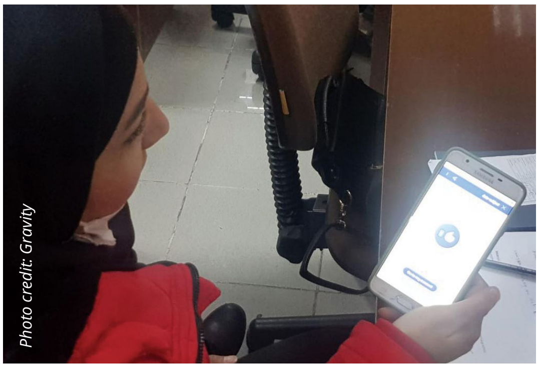


Photo credit: Gravity

Photo credit: Gravity

CONCLUSIONS

Being able to prove one's identity is becoming increasingly important in our connected, digital world. Whether for accessing healthcare, financial services, or government subsidies, the ability to offer proof of identity is a vital enabler of inclusion. For the more than one billion people worldwide without any form of recognized ID, this reality is acutely felt. Given that humanitarian agencies serve many of the world's most vulnerable populations, it is especially important that they familiarize themselves with the emergent solutions and debates on digital identity. While the process of identification has been traditionally facilitated by paper credentials, today, identification processes are increasingly reliant on digital technologies [1]. Humanitarian agencies are not new to these questions. Many have engaged with them for decades through beneficiary and information management systems. And yet, currently, a wide variety of organizations including telecommunications providers, financial institutions, governments and other organizations are beginning to undertake new digitalization efforts to adapt to new developments in the identity and access management and decentralized identification sectors [2]. It is critical, therefore, that humanitarian agencies continue to engage in these debates to further progress their digitalization strategies.

While there is growing consensus around the value of digital identity to the delivery of digital services, it remains an open question whether any single organization should invest in the technology. The potential for digital identity to broaden access to social, political, and economic inclusion makes it a potential path to furthering the mission of many humanitarian and development agencies. That said, these technologies also raise important and unanswered questions around achieving meaningful consent from beneficiaries. It is important not to expect technologies to solve these challenges and in some cases its application may worsen these power asymmetries. Rather than investing early in the development of a digital identity system, it may be prudent for humanitarian organizations to work with solutions providers that have already developed a product that can then be customized to the needs of the agency. This could save significant time and financial resources. Several organizations interviewed noted that the required investment of upfront resources to achieve digital transformation made digital ID programmes prohibitively costly. Still, being able to engage fruitfully depends on enhancing expertise in this growing area of innovation. By continuing to learn, humanitarian agencies can ensure that their involvement in digital identity is active.

As this report has illustrated, there are several complexities that a humanitarian organization should consider throughout the process of engaging with digital identity. Interoperability and how best to achieve it effectively both within and beyond the humanitarian sector remain critical and as-yet unresolved issues. In seeking to make progress on this topic, humanitarian agencies can look to alternative financing options and funding arrangements. By using models such as software-as-a-service, humanitarian organizations could streamline innovation financing, increasing the likelihood of a successful long-term engagement with new technology. Furthermore, humanitarian agencies should not act in a vacuum. Rather, by working with relevant industry organizations and cultivating cross-sectoral collaboration, humanitarian organizations could benefit from the progress being made in relevant external domains.

While humanitarian agencies do face a variety of challenges in implementing digital identity solutions, such as low-connectivity settings, innovations in other sectors (such as the decreasing cost of smartphones) could dramatically enhance the ability for humanitarians to mitigate these risks, while realizing the benefits of new technologies. Ultimately, digital identity technologies could offer benefits to organizations and beneficiaries alike, but only if they are implemented with careful consideration for local particularities and the necessary guardrails to ensure safety and efficacy.

REFERENCES

(All URLs last accessed on 8 February 2021)

[1] Financial Action Task Force/OECD. (2020). "Guidance on Digital Identity: Executive Summary." Available at https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity-Executive-Summary.pdf

[2] Slavin, A. (2019). "Distributed ledger identity systems in the humanitarian sector." Available at https://sovrin.org/wp-content/uploads/14A-Report.pdf

[3] PR Newswire. (2020). "Digital ID Solutions Industry Projections, 2020-2024: Increased Adoption of the Cloud-Based Digital Identity Solutions, Wide Adoption of Authentication Across Verticals." Available at https://www.prnewswire.com/news-releases/digital-identity-solutions-industry-projections-2020-2024---increased-adoption-of-the-cloud-based-digital-identity-solutions-wide-adoption-of-authentication-across-verticals-301020601.html

[4] Bostrom, N. and Sandberg, A. (2011). "The Future of Identity." Report commissioned by UK Government Office for Science. Available at https://nickbostrom.com/views/identity.pdf

[5] Mastercard. (2019). "Digital Identity: Restoring Trust in a Digital World." Available at https://www.mastercard.us/content/dam/mccom/en-us/issuers/digital-identity/digital-identity-restoring-trust-in-a-digital-world-final-share-corrected.pdf

[6] Microsoft. "Own your digital identity." Available at www.microsoft.com/en-us/security/business/identity/own-your-identity

[7] Crunchbase. "Okta". Available at www.crunchbase.com/organization/okta

[8] White, O., Madgavkar, A., Manyika, J., Mahajan, D., Bughin, J., McCarthy, M., and Sperling, O. (2019). "Digital identification, a key to inclusive growth." Available at www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth#

[9] Humanitarian Innovation Platform. "Dignified Identities (Digid) in Cash Programming" Available at https://hiplatform.org/digid

[10] GSM Association. (2018). "Using Mobile Technology to provide Functional Identities." Available at www.gsma.com/mobilefordevelopment/blog 2/using mobile technology provide functional identities

[11] ICRC. (2019). "Do No Harm in the Digital Era." Event on 29 August 2019 at Marriott Hotel, Kigali, Rwanda. Available at https://www.icrc.org/en/event/do-no-harm-digital-era

[12] UNHCR. (2013). "The mandate of the High Commissioner for Refugees and his Office." Available at www.unhcr.org/uk/protection/basic/526a22cb6/mandate-high-commissioner-refugees-office.html

[13] World Bank. "ID4D Practitioner's Guide: Levels of assurance (LOAs)". Available at https://id4d.worldbank.org/guide/levels-assurance-loas

[14] World Wide Web Consortium. "Verifiable Credentials Data Model 1.0". Available at https://www.w3.org/TR/vc-data-model/

[15] World Bank. "ID4D Practitioner's Guide: Interoperability". Available at https://id4d.worldbank.org/guide/interoperability

[16] Health Level Seven International "FHIR Overview". Available at https://www.hl7.org/fhir/overview.html

[17] Financial Action Task Force. (2020). "Guidance on Digital Identity." Available at http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-on-Digital-Identity.pdf

[18] Post, L., Raile, A., and Raile, E. (2010). "Defining Political Will." Politics & Policy. Vol.38(4):653-676. Available at: https://doi.org/10.1111/j.1747-1346.2010.00253.x

[19] WFP. (2014). "SCOPE In Five Minutes." Available at https://documents.wfp.org/stellent/groups/public/documents/communications/wfp272586.pdf

[20] World Vision International. "How LMMS works." Available at https://www.wvi.org/disaster-management/how-lmms-works

[21] Sovrin Foundation (2018). What is Self-Sovereign Identity? Available at https://sovrin.org/faq/what-is-self-sovereign-identity

[22] Rodriquez, K. (2020). "Linux Foundation Training Announces a Free Online Course-Developing Blockchain-Based Identity Applications." Available at https://linuxfoundation.org/press-release/linux-foundation-training-announces-a-free-online-course-developing-blockchain-based-identity-applications/

[23] World Bank. (2018). "Understanding Cost Drivers of Identification Systems." Available at http://documents1.worldbank.org/curated/en/702641544730830097/pdf/Understanding-Cost-Drivers-of-Identification-Systems.pdf

[24] Safaricom. "M-Pesa". Available at www.safaricom.co.ke/personal/m-pesa

[25] Hawkins, L. (2020). "Secure digital ID verifying Covid vaccine status to launch." Available at www.healthcareglobal.com/digital-healthcare/secure-digital-id-verifying-covid-vaccine-status-launch

[26] Bollinger, T. (2000). "A Guide to Understanding Emerging Interoperability Technologies." Available at http://www.mitre.org/sites/default/files/pdf/bollinger_interop.pdf

[27] UNHCR. (2019). "Global Virtual Summit on Digital Identity for Refugees, Concluding Workshop: Summary Conclusions and Recommendations." Available at www.unhcr.org/idecosystem/wp content/uploads/sites/69/2019/12/Conclusions_and_Recommendations.pdf

[28] Kak, A., Ben-Avie, J., Munyua, A., and Tiwari, U. (2020). "Bringing Openness to Identity." Available at https://blog.mozilla.org/netpolicy/files/2020/01/Mozilla-Digital-ID-White-Paper.pdf

[29] The Netherlands Red Cross. (2021). "GSMA Consortium Pilots 121 in Kenya". Available at https://www.121.global/gsma-consortium-pilots-121-in-kenya/

[30] Africa's Talking. "Homepage." Available at https://africastalking.com/

[31] World Vision International Nepal. (2020). "Nepal COVER Project". Available at https://reliefweb.int/sites/reliefweb.int/files/resources/Nepal%20COVER%20Project%20SitRep%2011%20%28Updated%208%20July%202020%29.pdf

[32] Davis, J. (2018). "Sikka: Working at the intersection of blockchain and humanitarian innovation." Available at https://medium.com/@davisjef/sikka-working-at-the-intersection-of-blockchain-and-humanitarian-innovation-2c752332c616

[33] World Vision International Nepal Innovation Lab. (2018). "Sikka: A digital asset transfer platform designed for the financially marginalized." Available at www.sikka.me/docs/SikkaConceptPaper.pdf

[34] Acharya, S. and Pandey, S. (2019). “Sikka: One Year Later, Lessons Learnt and Recent Developments.” Available at https://medium.com/@saujanyaacharya/sikka-lessons-learned-and-recent-developments-8fda5b1b83cf

[35] Coppi, G. (2018). “Blockchain and microfinance: hype or promise?” Available at https://www.convergences.org/en/blockchain-and-microfinance-hype-or-promise/

[36] Dodgson, K. (2018). “Blockchain for Humanitarian Aid Decision Tree.” Available at https://blockchain.humanityx.nl/uploads/toolkit/Blockchain-decision-tree-offline-toolkit-v2.pdf

[37] SDG Impact Accelerator. “About.” Available at https://www.sdgia.org/about-sdgia/

[38] SDG Impact Accelerator. (2019). “Live from #SDGIA Demo Day in Istanbul - 13 Sept 2010”. YouTube livestream on 13 September 2019. Available at www.youtube.com/watch?v=nimVxveZ5Kg

[39] Sertifier. “Homepage.” Available at https://sertifier.com/en/

[40] Mark Labs. “Homepage.” Available at https://www.marklabs.co/

[41] Thakur, S. (2019). “Results from the field: Improving livelihood prospects for refugees through decentralized identity in Gaziantep, Turkey.” Available at https://medium.com/gravity-earth/results-from-the-field-improving-livelihood-prospects-for-displaced-persons-through-digital-5786587308f8

ADDITIONAL SOURCES CONSULTED

Coppi, G. and Fast, L. (2019). "Blockchain and distributed ledger technologies in the humanitarian sector." Available at https://odi.org/en/publications/blockchain-and-distributed-ledger-technologies-in-the-humanitarian-sector/

Ebert, J. (2019). "Learnings from the SDG Impact Accelerator." Available at https://medium.com/gravity-earth/learnings-from-the-sdg-impact-accelerator-90abe6c13669

eSatya. (2020). "Blockchain and Sustainable Development." Available at https://esatya.io/collection/blockchain-and-sustainable-development/

Humanitarian Innovation Platform (2020). "Layering Digital ID on top of Traditional Data Management." Available at https://hiplatform.org/blog/2020/5/20/layering-digital-id-on-top-of-traditional-data-management

Innovasjon Norge. (2021). "Dignified identities in cash programming II (DIGID II)." Available at www.innovasjonnorge.no/no/subsites/hipnorway/innovation-projects2/dignified-identities-in-cash-programming-ii-digid-ii/

Intersolve. "Homepage." Available at https://intersolve.nl/

Myler, J. (2019). "Sikka: The Blockchain-Based Application Putting Money in the Hands of Nepal's Rural Communities." Available at https://medium.com/@asiap3hub/sikka-the-blockchain-based-application-putting-money-in-the-hands-of-nepals-rural-communities-81ab9067a309

UNDP Turkey, and Gravity. (2021). "Improving livelihood prospects for displaced persons through digital identity in Turkey.". Available at https://drive.google.com/file/d/1jKn4oz_vUODUcen98c90P7jjCJnP343_/view?usp=sharing

APPENDICES

APPENDIX I: Interview Questions

Question 1: In what cases can digital identity solutions can be applied, and why are they suitable? What are the limitations to their applicability?

Question 2: Pressure is mounting to protect beneficiary data, to implement self-sovereign identity technologies to give beneficiaries more autonomy to manage and own their data, and to lessen the storage of such sensitive data in centralized databases. Given this, how should humanitarian organizations adapt their beneficiary data management systems and practices to responsibly integrate digital ID solutions?

Question 3: Aid organizations have limited resources. Adopting new technologies could imply barriers in terms of costs, skills, and resources (maintenance, support, etc.). Thus, what economic incentives and sustainable business models for the use of digital ID technology apply to humanitarian organizations?

Question 4: What does interoperability among humanitarian organizations using digital IDs look like? When answering this question, one should explore the interoperability of data produced regardless of the technology backend used (e.g., digital credentials issued by different digital ID technologies but using standards such as decentralized identifiers, verifiable credentials , etc.) as well as the processes and willingness to share data between organizations to prevent duplication.

Question 5: The promise of self-sovereign ID depends on several factors: digital literacy of end users, infrastructure and access to hardware such as smartphones. Such factors are barriers in places where potential beneficiaries can be among the most vulnerable. How can humanitarian organizations implement digital ID technologies in settings where connectivity is low?

Question 6: Tension exists between individuals' desire to retain control over their own data (decentralizing data storage and control for the beneficiary) and organizations' wishes to use individuals' data for coordination purposes (to avoid duplication and fraud) and to be accountable to donors (to demonstrate that assistance is delivered to real people). What are the trade-offs involved in resolving this tension? How can a balance be struck? What are the pitfalls to avoid?

Question 7: What training in data literacy do beneficiaries of digital IDs require to be able to use them safely? How do these requirements differ between smartphone and feature phone users?

APPENDIX II: Interviewees

Individual interviews:

Number	Name	Role & Affiliation
#1	Anonymous F1	Digital ID project team, aid organization
#2	Amanda Robinson	Head of Social Innovation & Humanitech, Australian Red Cross
#3	Jimmy Snoek	CEO, Tykn
#4	Anonymous F3	Digital ID project team, aid organization
#5	Anonymous A	Programme manager, UN aid organization
#6	Paul Currion	COO, Disberse
#7	Anonymous D	Data services lead, UN aid organization
#8	Anonymous B	Project manager, large humanitarian organization
#9	Johannes Ebert	CEO, Gravity
#10	Sharanya Thakur	Project Manager, Gravity
#11	Alexandros Yiannopoulos	n/a
#12	Safia Verjee	Innovation Manager, Kenya Red Cross
#13	Natalie Brinham	Programme Officer, Institute on Statelessness and Inclusion
#14	Andrew Tobin	Managing Director (EMEA) & VP Customer Delivery, Evernym
#15	Anonymous C	Researcher, human rights advocacy organization
n/a	Jennifer Gilbertson	Coordinator for Humanitarian Innovation, Norwegian Red Cross
n/a	Anonymous F2	Digital ID project team, aid organization

Focus group:

Name	Role & Affiliation
Margie Cheesman	PhD migrant data rights, Oxford Internet Institute
Emrys Schoemaker	Digital ID expert, Caribou Digital
Amos Doornbos	Director of Strategy & Systems in Disaster Management, World Vision International
Vincent Graf Narbel	Strategic Technology Advisor, ICRC
Giulio Coppi	Global Digital Specialist, Norwegian Red Cross
Hakan Büyükbayrak	Director, RedRose
Christine Leong	Global Lead, Blockchain ID & Biometrics, Accenture

APPENDIX III: Detailed Methodology

Interviews

Interviews with key stakeholders from the humanitarian sector supported the desk research and case study analyses. The research team worked with IFRC to prioritize and reach out to key participants. In total, 24 individuals were consulted. They represented major development donors, humanitarian organizations currently deploying digital ID systems, activists for humanitarian data rights, data privacy experts from the IFRC and UNHCR, private sector actors such as Accenture, technology providers, and researchers from major academic institutions. A list of all the interviewees is given in Appendix II.

Most interviews were conducted individually between 3 December 2020 and 15 January 2021. Seven of the participants were part of a virtual focus group session hosted on 16 December 2020 with the support of the Oxford Technology and Management Centre for Development. All interviews were conducted in English using Microsoft Teams. One participant submitted responses via email.

The individual interviews followed a semi-structured format. Participants received the list of seven key questions used in this stud ahead of time. Microsoft Teams was chosen for the platform's security features included in the licensing agreement with the University of Oxford, to which the research team had access. To improve the chances of preserving stable internet connections, participants were not asked to use video. Time was allocated at the beginning of the call to build rapport and answer any questions participants may have; this helped cultivate a personal atmosphere and establish the trust required for participants to feel comfortable enough to share insights openly.

The focus group followed a stricter format. Participants were sent the list of key questions in advance and were asked to choose three of them to answer, with time allocated for responses and open discussion in reaction to each presentation. In contrast to individual interviews, the use of video was encouraged for the focus group to have a round-table style atmosphere.

The interviews and focus group conversation were recorded using the Voice Memos app on the research team's iPhones to facilitate the transcription process. The recordings were immediately uploaded to an encrypted hard drive and transcribed using Nvivo. At the start of each call, interviewees were asked to state their verbal consent to join the study. Participants were also asked whether they wished to remain anonymous. Several participants opted for this; their names and institutional affiliations are not included to prevent any risk of identification. The insights they shared still informed the research findings. Participants retained the right to request a copy of their recording or to request it be deleted at any point between November 2020 and March 2021. As of the time of writing (April 2021) the recordings have been deleted. All participants were offered a chance to review the final draft of the research report and to request modifications for the final version.

Case Studies

Three case studies were selected for analysis to understand the complexities of implementing digital ID systems. These were World Vision's Sikka platform in Nepal, the SDG Impact Accelerator's Digital ID start-up in Turkey and a pilot project completed by the 121 consortium in Kenya at the end of December 2020. The case studies were selected by the research team and approved by the IFRC. Cases were selected for their diversity in technology and humanitarian actors, maturity and application. This work was based on a review of public documents as well as internal documents provided by the organizations in question. The resources consulted included project pitch videos, lessons learned publications, concept papers, first and second hand accounts, internal meeting notes, product roadmaps and evaluations.

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.

IFRC

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