Dignified Identities in Cash Assistance:
More Lessons Learnt from Kenya (July – November 2021)

IFRC

ICHA International Center for Humanitarian Affairs
At the Kenya Red Cross Society
Inquire • Understand • Influence

Kenya Red Cross

Acknowledgements

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

Executive Summary

The Dignified Identities in Cash Assistance (DIGID) project consortium, composed of the Norwegian Red Cross, Norwegian Refugee Council, Norwegian Church Aid, and Save the Children Norway, coordinated by the International Federation of Red Cross and Red Crescent Societies (IFRC), and funded by Innovation Norway, aims to understand the opportunities and risks of digital identity (ID) technology in providing humanitarian cash assistance to people with no official IDs. The project began in 2019, with the first field pilots being carried out in Kenya (Kalokol, Tukana and Mathare, Nairobi) in April and May 2021 led by the Kenya Red Cross Society (KRCS) and IFRC. A funding extension enabled further project activities to be carried out in the period July-November 2021. This report briefly describes each activity and highlights the lessons learnt in each case.

During the extension period, DIGID project activities and corresponding lessons included:

- KRCS-internal advocacy to raise awareness of digital IDs and identify opportunities for their application beyond cash transfers - several departments saw potential for using digital IDs in their work
- Preliminary advocacy towards external partners - the Ministry of the Interior within the Government of Kenya is key
- A second cash distribution in Mathare - adaptations to the delivery methods made for clearer communication with people being assisted
- Community engagement in the previous cash distribution locations and sites for potential future digital ID deployments, including in a migration context - cash transfer and migration scenarios have some overlap, but also specificities
- Technical adaptations made to the digital solution by the technology vendor - progress was made in several areas including governance but more practical testing is needed to continue to learn about this relatively new technology
- Analysis of the sustainability of various business models for digital ID implementation - DIGID does not exist in a vacuum and other partners will be critical for its future.

Overall, the DIGID project activities carried out in Kenya during the extension period constitute an important stepping stone, building on the lessons learnt in the run-up to and delivery of the DIGID field pilots in April and May 2021. Next, KRCS and the DIGID consortium partners will engage in exploring digital IDs in the context of migration.

Table of Contents

Introduction

Dignified Identities in Cash Assistance (DIGID) is a project bringing together the Norwegian Red Cross, Norwegian Refugee Council, Norwegian Church Aid, and Save the Children Norway, coordinated by the International Federation of Red Cross and Red Crescent Societies (IFRC) and funded by Innovation Norway. The consortium partners' aim is to understand the opportunities and risks of digital identity (ID) technology in providing humanitarian cash assistance to people with no official IDs. The project began in 2019, with the first field pilots being carried out in Kenya led by the Kenya Red Cross Society (KRCS) in May 2021. A report detailing the lessons learnt during the field pilot build-up and delivery, which also includes technical details about the digital solution deployed has been published.

Further DIGID project activities in Kenya were made possible thanks to a funding extension being granted for the period July–November 2021. This report recounts the lessons learnt during the extension period and is complementary to the first report. For the sake of brevity, it is assumed here that the reader is already familiar with the first report, so details about the DIGID context are purposefully omitted. The DIGID project activities covered by the current and the previous reports were also presented in a series of webinars that may interest the reader.

The project activities and main motivations behind them were as follows:

- **Advocacy**, both within and external to KRCS - to raise awareness across KRCS departments on the one hand and to satisfy know-your-customer (KYC) requirements on the other;
- **Community engagement** in the original cash distribution locations (Mathare (Nairobi) and Kalokol (Turkana)), as well as at sites where digital IDs might potentially prove useful in the future, whether for cash and voucher assistance or in the context of migration - to gather feedback on the use of the solution and give users a sense of ownership over the project;
- A **second cash distribution** using digital IDs in Mathare - to address the challenges identified during the first distribution
- **Technical enhancements** to the digital ID solution deployed - to enhance the solution's interoperability with existing systems
- Analysis of the **sustainability of various business models** - to map the economic landscape in which digital IDs must fit.

Findings and observations

Internal advocacy

Image 1: *DIGID advocacy workshop with KRCS staff members from various departments*

A digital ID advocacy workshop was organized in September 2021 for representatives of departments from across the KRCS to introduce the DIGID project, share lessons from the field pilots, and discuss the opportunities and value of digital IDs in other services provided by the organization.

All departments mentioned that digital ID was a new concept for them. After being introduced to the topic, the workshop participants identified opportunities for applying digital IDs (besides those presented in the context of the DIGID cash distributions) in managing health and volunteer data. A representative from the organizational development department pointed out that digital ID wallets could be useful beyond simply identifying volunteers. Digital wallets could store credentials such as code of conduct adherence records or training certificates for the prevention of sexual exploitation and abuse. Further, because volunteers often provide support to multiple organizations, digital credentials for volunteers (or, indeed, for people being assisted, as noted in the DIGID field pilot report) would ideally be recognized by other organizations.

A representative of the disaster management (DM) department also expressed potential interest, albeit with a "wait-and-see" approach. Others, such as the Global Fund liaison, indicated that they would follow DM's lead. In other words, if other KRCS departments were to see DM adopting digital IDs, they would likely follow suit. It was noted that adopting digital IDs across KRCS would be beneficial not only for the organization (e.g., because to do so would be more efficient than current systems), but also – importantly – for the people KRCS seeks to assist, whether they already have official IDs or not.

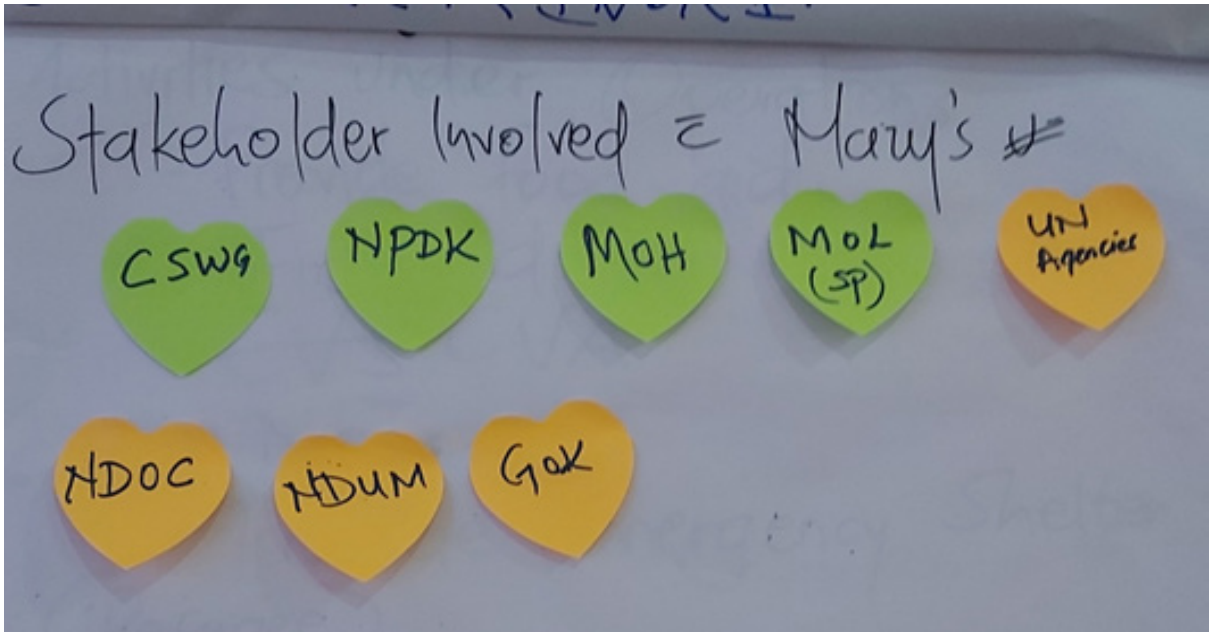

Image 2: *Group activity during the internal KRCS advocacy workshop identifying the various stakeholders to involve*

So, departments across KRCS see a value in digital IDs, at least in theory as expressed in the context of an internal advocacy workshop. In the future, KRCS should continue to promote interdepartmental collaboration to maximise the applicability of digital IDs, for instance by including other departments as observers during the testing or field pilots and by having meaningful discussions on the KRCS services offered to certain communities that may benefit from the use of such digital IDs.

External advocacy

An advocacy plan was drafted with the help of the policy department that included an analysis of key external stakeholders, their potential interest, concerns, or influence regarding digital IDs, key advocacy messages, and a timeline for engagement. The external-facing advocacy concerning DIGID mainly targeted local stakeholders and partners, such as local administrators and county commissioners. In both Kalokol and Mathare, the county steering groups (CSGs), composed of government and non-governmental stakeholders implementing cash interventions, were engaged through the DIGID field pilot and convened by Kenya's National Drought Management Authority (NDMA).

Government and financial service providers

By the end of the extension period, advocacy towards the Government of Kenya and financial service providers remained in the planning stage. KRCS intends to continue the activities outlined in the advocacy plan.

KRCS' initial conversations with Safaricom via the GSM Association in July–August were not fruitful. The regulatory environment and "know your customer" (KYC) requirements in Kenya are such that Safaricom's hands are tied with respect to KRCS seeking to obtain SIM cards to distribute as part of DIGID. To facilitate the latter, Safaricom will need approval from the institutions regulating mobile phone operators in Kenya. SIM cards are indeed needed to enable people being assisted to register and control their own M-Pesa (mobile money) accounts through which they could receive funds directly, thereby eliminating the need for KRCS to go through a money agent. Indeed, a humanitarian-issued (digital or analogue) ID is not currently considered to fulfil KYC requirements for issuing SIM cards in Kenya. It became apparent to KRCS that there is a need to engage the Government of Kenya, specifically the Ministry of the Interior (MoI), and other regulatory institutions on KYC requirements for mobile money

phone network operators.
Based on this observation, KRCS will seek to better articulate the notion that such digital IDs are functional in nature and are not meant to replace or undermine foundational IDs, as is already the case for humanitarian-issued, paper-based IDs. Indeed, KRCS or any other humanitarian organization could already issue people in need with QR codes on laminated cards that would link to their data on a beneficiary management system, such as Red Rose. The differences offered by digital IDs as proposed by DIGID are that users would have direct control and access over their own data, enhancing their dignity, and that (hopefully, someday) a single digital ID might be recognized by multiple organizations. Above all, KRCS must determine how to navigate the interface between its humanitarian imperative to help all people in need regardless of other criteria and the requirement to follow local laws.

National Drought Management Authority

NDMA was engaged regarding Turkana in particular, which is a drought-prone region. NDMA is mandated by an act of parliament to coordinate drought risk management and to establish mechanisms, either on its own or with stakeholders, to end drought emergencies in Kenya. At the county level, NDMA plays the role of CSG secretary and chairs the cash technical working group (TWG) in Turkana. KRCS sought to inform NDMA about DIGID's potential, and the two organizations coordinated with each other during the DIGID field pilots. Representatives from the cash TWG carried out a survey with people assisted in this way in Turkana, seeking to understand their thoughts on the digital IDs used. The main concern brought to light was that, given the multitude of organizations in Turkana running cash transfer programmes, no consolidated data set exists that contains the whereabouts of people receiving cash within Turkana county, leading to repetitive registration and identification processes.

Following the advocacy efforts with NDMA in Turkana and Garissa, KRCS intends to continue the collaboration with NDMA on follow-up DIGID activities and see how DIGID might complement NDMA's efforts. KRCS will also build on experiences and feedback from the NDMA teams in Turkana and Garissa in its advocacy for digital identities to other key stakeholders.

Other humanitarian organizations

During the DIGID extension period, KRCS consulted with other humanitarian organizations involved in delivering cash transfer programmes in situations similar to the field pilots. None revealed any major concerns in terms of digital IDs presenting risks to people being assisted.
One organization in Turkana mentioned having previously tried to use digital IDs in delivering aid. This effort was unsuccessful, so the organization in question would be very interested in seeing the results obtained by KRCS and offered to lend its influence when communicating with the Government of Kenya. On the other hand, the same organization underscored the importance of cooperation between organizations, because of a concern that multiple organizations issuing digital IDs would be no more efficient than the current proliferation of paper-based systems. KRCS should integrate the notion of cross-sector collaboration in its advocacy strategy, to demonstrate the potential efficiency gains made possible by applying digital IDs.
One partner in Turkana suggested building the case for digital IDs in humanitarian contexts by running a field pilot in the whole county, gathering more data from more people. For example, 80 per cent of residents might not have legal national ID, serving to illustrate a problem that is widespread in Kenya (people in a migration context not being taken into consideration here). Gathering specific statistics would further strengthen the case for support.
As highlighted in the first DIGID learning review, coming together as a group of humanitarian organizations is key to realizing the overall benefit of digital IDs. Therefore, organizations such as those that expressed interest in DIGID during the pilot phase have been included in the KRCS advocacy strategy. For instance, there is a national cash working group including consortium partners and other organizations, where advocacy for humanitarian digital IDs could be highlighted.

Community engagement

KRCS staff sought feedback on digital ID from members of two broad community categories: relatively stable local residents who were targeted for cash distributions (or might be in future) on the one hand, and (international and internally displaced) migrants who might use digital IDs along their journeys on the other.

The locations visited were:

- Mathare (Nairobi), where cash distribution had taken place during the first DIGID field pilots, as well as a second time in November 2021 (see below)

Figure 1: *Map of Mathare, Nairobi*

- Kalokol ward and Kang'atotha ward (Turkana county), where the initial DIGID field piloting also took place

Figure 2: *Map of Kangatotha ward*

Figure 3: *Map of Kalokol ward*

- Benane ward (Benane and Kambi Samaki) and Modogashe ward (Baraquqe and Garsen) within Garissa township (Garissa county)

Figure 4: *Map of Garissa County*

- Dadaab refugee complex (Ifo camp) (Garissa county), Migori and Nyatike (Migori county) and Kalobeyei integrated settlement and Kakuma refugee camp (Turkana county).

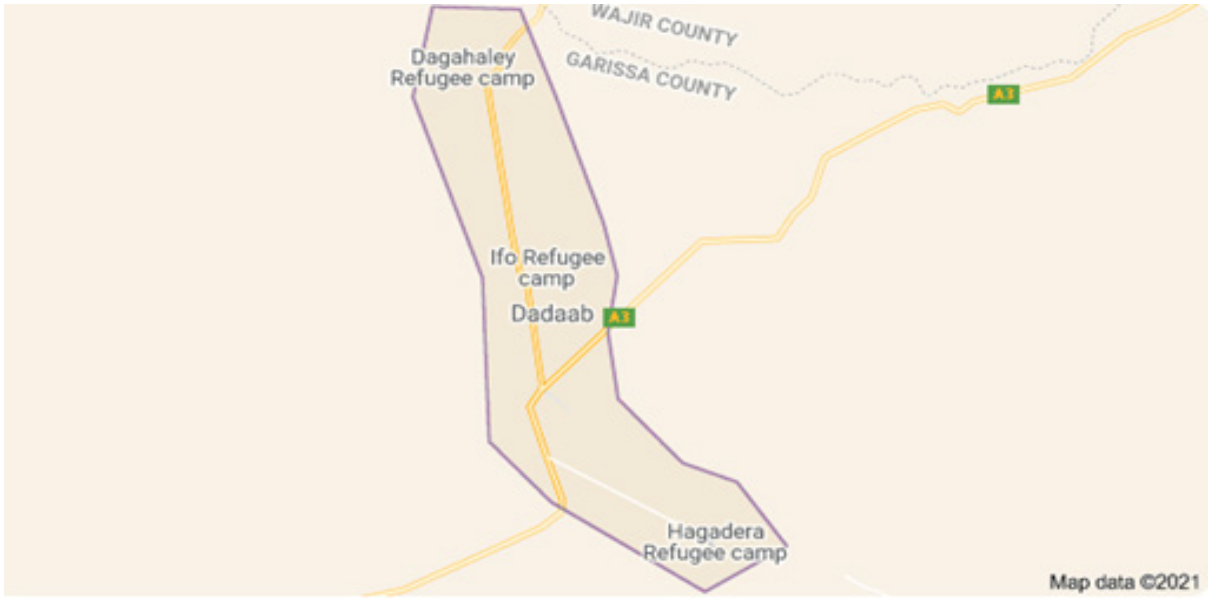

Figure 5: *Map of Daadab Refugee complex*

Figure 6: *Map of Migori county*

Image 3: *KRCS facilitating focus group discussions with migrants in Migori county*

KRCS have written individual reports about each location chosen for community engagement.
Overall, digital literacy did play a role as to how communities understood the concept of digital IDs, a relatively new concept for all those consulted who had not participated in the field pilots (for whom they had also been new at the time). Once introduced and explained by the team, the concept was relatively easy to understand and most especially for those slightly digitally literate participants, who knew how to operate a mobile device; smartphone or feature phone. Following learnings from the Mathare and Turkana pilot in April/May 2021 and despite the fact that prototyping could not take place with the consulted communities, the team did employ a bit of demonstration and illustration using printed QR codes and the web based app, to ensure that even beneficiaries who did not have phones and were slightly less literate could visually see and better understand the concept. Digital literacy did also play a role in how communities understood and perceived the concept around PINs. In the urban context of Mathare, people were largely aware of the concept of a personal identification number (PIN) from using the M-Pesa mobile money application, although they tended not to keep their PINs secret. In the DIGID project, PINs are used to unlock the identity data stored in users' QR codes. PINs were not familiar to residents in rural locations (especially Turkana), who expressed a preference for facial recognition as a means of authentication (see also the sub-section on biometrics below).
In the settlements and camps, the people consulted stemmed from migration scenarios (but were not

officially recognised as refugees, whose identification is handled by the United Nations Refugee Agency). This population was mainly concerned with how digital IDs could help them along their journeys, as a means of storing the various documents they might be issued by an assortment of organizations and institutions. In addition, newly-arrived migrants perceived KRCS primarily as a source of healthcare, and expressed the hope that digital IDs might facilitate access to such services. Another potential advantage of digital IDs perceived was the possibility of reducing the repetitiveness of registering with organizations at several stages along a migratory path. Relatedly, the DIGID consortium has also commissioned a report on consultations with migrants in Colombia, Niger and Kenya about their perspectives on digital IDs, published separately.

While some migrants expressed a concern over being tracked by authorities, both populations - local and migrant - displayed a high level of trust in KRCS with respect to data privacy and protection. That being said, the true extent to which individual community members are concerned about such questions is unclear and may be highly variable according to their circumstances.

The above concerns can be mitigated through zero knowledge proofs possible through digital identity solutions. Zero knowledge proofs allow users to share proofs with relying parties without the need to actually demonstrate the entirety of the information. This is particularly important for the humanitarian context given the sensitive nature of data regarding migrants. The DIGID Platform currently does not support zero-knowledge proofs, but this may be developed if required as part of the migration context.

Second cash distribution in Mathare

The DIGID extension period included a return visit by KRCS staff to distribute a second tranche of cash 5,800 Keynan shillings (52 US dollars) per targeted household in Mathare (Nairobi) in November 2021. This second distribution featured several changes based on lessons learnt during the first DIGID field pilot in April 2021.

On a practical level, the physical QR codes distributed to users in April were not robust. Many faded over time and suffered wear and tear. KRCS therefore used darker printing and improved lamination for the second round of QR codes.

In addition, while some people targeted for the cash disbursement in the first instance owned smartphones, many of their devices were not of the same standard as those used by KRCS when testing the DIGID solution. So, they were not able to use the web application and had to rely on the USSD menu developed for basic/feature phone users instead. In the second instance, several smartphone users were directed to use the feature phone procedure instead, saving time and effort for both KRCS and their users.

During the extension period, additional prototyping was carried out in Mathare to help participants understand how to use their phones to interact with their digital IDs. In May, only a select number of users were able to join the prototyping session, but during the extension, all targeted users with phones were included as part of a more rigorous training session.

While at the time of the first distribution, several users in Mathare were familiar with the concept of a PIN from using M-Pesa (much more so than in Kalokol (Turkana) for instance), they did not tend to keep their numbers secret, sharing them freely with family and trusted friends. After the second distribution and associated explanations, older women especially displayed much more guarded behaviour with their PINs, having understood that their digital IDs could potentially open many more doors than just accessing cash. Interestingly, several phone owners in Mathare contacted KRCS between the two cash distributions seeking to update their data in order to use their digital IDs to receive other humanitarian services, despite these not being made available yet. This seems to indicate awareness of their personal data guarded by KRCS and interest in accessing it.

Post-distribution monitoring (PDM) was conducted four weeks after the extension period cash distribution in Mathare.

The results were compared to those from the PDM after the May distribution, leading to the following general observations:

- Awareness increased that the DIGID IDs could be used to access cash, other KRCS services, and

services offered by other NGOs. However, there was also a slight (3 per cent) increase in the number of people who thought they could use their DIGID IDs as legal identification, which is not the case.

- There was an increase in end users' positive experiences of the identification process, the use of the QR codes, and having a digital wallet. In particular, the concept of a digital wallet was not highlighted during the first PDM, while 28 per cent of respondents mentioned liking the concept of the digital wallet at the second PDM.
- In terms of challenges with using digital IDs or with the identification process, fewer respondents raised issues (from 24 per cent in May to 17 per cent during the extension period). Many of the issues highlighted were similar to the ones previously reported, including difficulties reading fingerprints, the time needed to scan the QR codes, or not having enough mobile data credit on their phones to check their identity data.
- When asked whether targeted users were provided enough information about the identification process for using their digital IDs, the positive response showed an increase from 61 per cent in May to 80 per cent during the extension period. This increase demonstrates the value of returning to the community and getting their feedback when increasing the training or prototyping with phone users.

Technical enhancements

The vendor selected to provide the digital ID solution as part of the DIGID field pilots was Gravity.[1] During the DIGID extension period, Gravity aimed to develop technical enhancements to make the platform more responsive to KRCS' needs and those of the communities being served, based on the lessons learnt during the first field pilots and the associated data protection impact assessment. In addition, testing sessions helped provide continuous feedback from the product's end users to improve the user interfaces and experience. Technical issues and scheduling conflicts prevented the planned prototyping activities to be part of the community consultations planned from taking place. Feedback from prototyping with end users is important and it is proposed that more be collected in the future.
Given the lessons from the field pilots particularly how end users interacted with the DIGID solution, Gravity decided to re-factor their code to improve their technical solution. Although this caused some technical issues that prevented some of the planned prototyping, Gravity felt this was better done as early as possible before scaling up the solution where unpredictable issues might come up.

Data governance interface

Gravity launched a first release of its data governance interface in the form of an application programming interface (API), which is key to making the solution interoperable between organizations. This API enables an "ecosystem administrator" to assign the rights and permissions for each organization involved in managing digital IDs: who can issue credentials, who can verify them and so on. It remains unclear who the ecosystem administrator would be in the context of DIGID (Gravity plays this role for the time being), in part because the costs incurred by the administrator (in terms of personnel for example) are not yet evident. The governance policy will also need to be defined in the future. In addition, Gravity plans to improve the API user experience for KRCS staff and add further controls to increase data protection and security.

Biometric authentication

It was also foreseen for Gravity to research, implement and test biometric authentication methods for digital ID users to unlock access to their data and credentials. Biometric authentication, using an unalterable, unique part of a person's body (such as fingerprint, iris or voice patterns), presents several

1 *gravity.earth*

advantages. Notably, biometrics cannot be lost, shared or forgotten and they are not easily forged or stolen, unlike PINs for example. On the other hand, because they cannot be altered, biometrics are especially sensitive and must therefore be protected more closely than other authentication methods. Two considerations stand out when considering biometrics: usability and data protection.

The International Committee of the Red Cross (ICRC) recommends decentralizing biometric data storage, for instance by encoding biometric data in a physical token, such as a printed QR code, given only to the user.[2] Separately from its work on DIGID, Gravity is working with ICRC on a prototype technical solution using fuzzy vault matching with potential future applications in the DIGID environment.

Gravity investigated the use of voice recognition as a form of biometric authentication. The low literacy levels encountered among the population being served by DIGID meant that using interactive, voice responsive (IVR) menus might be easier than having them remember a PIN. However, the IVR vendor in question was not transparent about their data storage. Instead of IVR menus, the unstructured supplementary service data (USSD) method was examined instead. With repeated usage, it was observed that users became more familiar and therefore autonomous in using the USSD interface to view, request and share their identity data.

While both IVR and USSD are well established and competitive in Kenya, they are not universally present in other countries where digital IDs might be applicable to humanitarian assistance (for example, Gravity has unsuccessfully sought to use USSD on another project in Somalia, where mobile phone operators can be hard to reach). The interoperability requirement at the heart of the DIGID project therefore meant that voice recognition was not a viable option for biometric authentication.

Overall, the time constraints, in combination with the low-connectivity environments (lack of mobile phone signal; variable phone type ownership, if any) imposed by the social and infrastructure conditions where cash assistance and other humanitarian services are most needed in Kenya (and elsewhere), meant it was not possible for Gravity to implement biometric authentication in the DIGID solution.

Red Rose integration

While the DIGID solution was already integrated with Red Rose (the beneficiary management system used by KRCS) in time for the April/May 2021 field pilots, certain areas for improvement were noticed that Gravity sought to address during the extension period. For example, the data flow from Red Rose to Gravity was smooth when an ID was first created, but when the data were (inevitably) updated at the Red Rose end, the changes were not propagated to Gravity. Too much manual effort between the systems was still needed. This point was noted by KRCS volunteers using the solution at each step from registration to cash distribution, highlighting the importance of field tests and first-hand, frontline feedback.

Gravity's product roadmap called for third-party solutions such as Red Rose to install a server-sent event (SSE) to "listen" for updates on the DIGID end and update Red Rose in real time. It was realised, too late, that Red Rose is not programmatically designed to allow SSE installation. Gravity designed an alternative method using an HTTPS connection and configuring Red Rose to refresh periodically and receive updates. A key lesson here is that digital ID solutions must be developed flexibly, so that they can be integrated with humanitarian organizations' existing software environments.

Deployment readiness

According to Gravity, the DIGID platform is ready to be deployed by other organizations aiming to improve the identification process in humanitarian assistance. The platform could be useful in contexts requiring secure exchange of verifiable data at scale while preserving users' privacy and control. Depending on the organization and the use case, the following aspects of the DIGID platform may need to be customized: Remote procedure call (RPC) agent hosting: The DIGID ecosystem accepts multiple organizations as issuers of beneficiary data. Each issuing organization would have to host an instance of the RPC agent

2 ICRC (2019). *Policy on the Processing of Data by the ICRC*

from where they would issue credentials about their beneficiaries. Such an agent is contained on a docker image and can either be automatically deployed on a remote machine or manually installed by said organization. The choice depends on the organization's technical capacities, internal policies and preferences.

Integration with beneficiary management systems (BMS): One of DIGID's principal objectives has been to decouple identity management from beneficiary management systems (for programme purposes). So, the DIGID platform has been developed to complement BMS, rather than replace or disrupt them. Organizations can therefore choose how they want their existing BMS to interact with the DIGID platform: either by integrating their BMS with the DIGID platform to allow for data collected through the BMS to automatically be issued as credentials, or by keeping the BMS and DIGID platform separate and using the latter to issue credentials.

Data schemas: Data schemas help standardize the process of issuing and verifying credentials. These schemas may depend on the specific data that are relevant for a particular use case. In the case of the KRCS cash distribution, identity-related data were seen as relevant because they helped verify beneficiaries' identities at the point of cash distribution. However, data fields for a health use case may be different and will therefore need to be defined by the organization in advance and communicated to Gravity so that a dedicated schema can be developed and deployed. These schemas may then be used by other organizations also dealing with health data.

Data storage location: To store sensitive user data securely, the credential repository may need to avoid international transfers (as recommended by the Data Protection Impact Assessment conducted for the DIGID project). So, the DIGID platform uses private-cloud, decentralized storage, with its nodes set up exclusively in Kenya, in compliance with the Kenya Data Protection Regulation. In future, organizations may continue to use the storage nodes in Kenya or decide to have one in their country of operation.

Business model sustainability

Conversations with various technology providers and other organizations reveal three common ways of financing digital ID services or solutions:

1. **Software licensing** – the organization pays a digital ID provider a monthly or yearly fee to use its solution . This is similar to other, traditional software solutions.

2. **Pay-per-use for identity transactions** – the organization pays based on transactions, such as when a digital credential is issued, verified, or revoked. Each is a separate transaction that incurs a cost. This model is typical for cloud-based services.

3. **Work for hire** – an organization hires a company to develop a solution with their specifications, which is then handed over to the organization to run and maintain on their own. The company may provide maintenance and support if requested. This model is mainly applied for bespoke solutions and assumes the organization has the skills to operate and maintain the solution on a day-to-day basis.

Digital ID providers may also have a mix of these options.

For a model to be sustainable, it is important to realize that many humanitarian organizations have limited IT budgets and will need to ensure the costs can be aligned with their fundraising model. For this reason, costs that repeat on a monthly or yearly basis in perpetuity, while the solution itself might not be in constant use, may not be sustainable.

Pay-per-use models, similar to the Red Rose solution for beneficiary and programme management, can be advantageous because the client (in this case, KRCS) only pays when the solution is used for in-kind or cash distributions that are tied to operations, so they are able to anticipate these costs when planning

their budget. However, given that different transactions have different values, transaction-based costing for digital ID use also does not seem sustainable. One example transaction is a financial service provider verifying an identity to address KYC requirements, while another is an end user simply checking what data are in their credentials. These example transactions differ in terms of value created and may need to be considered individually when pricing pay-per-use transactions. One key informant suggested that truly "per-identity" models are preferable to those based on the volume of transactions.
So, who should pay for the solution?
It is clear from key informant interviews that end users (affected people) themselves should not bear the cost of owning and using digital IDs. And individual organizations themselves should also not be expected to pay on their own for an infrastructure that is meant to serve a wider network.

Three models are worth analysing further:

1. **Cost sharing** – a consortium or group of organizations may come together and decide to fund the infrastructure and decide on how costs related to transactions or identities are shared. This is particularly helpful when the organizations are providing assistance to the same communities, areas, or regions.

2. **Third-party transactions** – private-sector actors, such as FSPs, might be asked to pay the cost of using the identities to verify individuals or fulfil KYC requirements, if allowed.

3. **Institutional donors** – donors might support the costs of running-large scale programmes or assistance during protracted crises.

Discussion between KRCS and Gravity to ensure the DIGID is sustainably financed is still ongoing. Gravity provided a list of costs that would either be one-off or recurrent, based also on a combination of the software licensing and pay-per-use transaction models.\

Image 4: *Verifying digital credentials using a smartphone that scans QR codes. Daadab, 2021.*

Conclusion

In the extension period July–November 2021, the DIGID project featured several activities, each giving rise to insights and lessons for the future. Taking into account these lessons and feedback from communities, as well as the development of policy and advocacy materials, KRCS, with the support of IFRC, is developing a digital ID strategy, to be published separately.

Overall, the extension of DIGID in Kenya, though brief, was a useful exercise to enhance and build upon the impact made up until the field pilots earlier in the year. In the next phase of the project, the DIGID consortium will turn their attention to the opportunities and challenges presented by digital IDs in migration contexts.

South “C” (Bellevue) Red Cross Road, Off Popo Road
P.O Box 40712, 00100 - GPO, Nairobi, Kenya
Tel: (254-20) 3950000/ 2355062/3 Fax: (254-20) 3950444
Mobiles: 0722-206958, 0703037000, 0733-333045
Email: info@icha.net, Website: www.icha.net

ICHA International Center for Humanitarian Affairs
At the Kenya Red Cross Society

Inquire • Understand • Influence