Dignified Identities in Cash Assistance:
Lessons Learnt from Kenya

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:

Table of Contents

Executive Summary

The Kenya Red Cross Society (KRCS) and the International Federation of Red Cross and Red Crescent Societies (IFRC) carried out a field pilot in May 2021 as part of the Dignified Identities in Cash Assistance (DIGID) project. The project's aim is to understand the opportunities and risks of digital identity (ID) technology in providing humanitarian cash assistance to people with no official IDs. DIGID is governed by a consortium composed of the Norwegian Red Cross, Norwegian Refugee Council, Norwegian Church Aid, and Save the Children Norway, and funded by Innovation Norway. These humanitarian organizations have come together to address challenges related to identification. The consortium aims to ensure that:

- People with no official IDs are assisted.
- Individuals are empowered to control and access their own data.
- The technology solution works in lowconnectivity environments where many vulnerable people reside.
- Such digital IDs are recognized by other humanitarian actors and not siloed within their respective organizations.
- The technology is interoperable, to avoid vendor lock-in and allow organizations to choose the technology partner that meets their needs.

These considerations help promote the dignity of people being served.

There has been increasing interest in digital ID technology from private and public sectors to manage electronically captured and stored personal attributes to prove or authenticate individuals. Digital ID is also regarded as an increasingly important element of humanitarian action. There are several reasons for this. First, because there are over 1 billion people with no official IDs; when they are affected by disasters and crises, their vulnerabilities are exacerbated, and they risk being left behind by humanitarian response. Second, identification is fundamental to humanitarian assistance, because personal details are used to ensure the right individuals receive assistance and they help organizations demonstrate accountability towards donors. Third, large volumes of data are collected from affected communities, with sometimes the same information being collected multiple times by different humanitarian organizations. Such data often include sensitive information that may put individuals at even greater risk if accessed by unauthorized parties, which may also put the organization in disrepute for causing unintended harm.

The field pilot was conducted as part of the KRCS response to the COVID-19 pandemic. Over 2 million Kenyan shillings (KES) (19,000 US dollars) in cash assistance were distributed to 300 households in two locations: the informal urban settlement of Mathare in Nairobi (100 households, 55 per cent without official ID) and the rural Kalokol ward in Turkana county (200 households, 100 per cent without official ID), to address their basic needs. The dual locations allowed the project team to analyse the applicability of digital IDs in different contexts, particularly in lowconnectivity environments.

The results from the DIGID field pilot in Kenya were promising, including digital IDs functioning in lowconnectivity environments, enabling people with no IDs to receive assistance using a humanitarianissued ID and enabling individuals to access and interact with their own data. However, more work is needed to fully meet the objectives and vision of digital IDs for humanitarian action, particularly in providing cash assistance, including further advocacy with the Government of Kenya to recognize humanitarianissued IDs as meeting regulatory requirements, such as "know your customer" (KYC), and the more practical application of interoperability. For KRCS, which has been exploring digital identification technologies since 2019, these efforts are actionable and the vision is attainable. KRCS plans to continue advocacy efforts with other humanitarian actors and with government, as well as looking into other humanitarian contexts where digital IDs could be beneficial.

The central message derived from this field pilot is that the success and trustworthiness of digital IDs in assisting affected communities depends on cooperation between actors and the development of interoperable solutions, rather than on the specific technology selected or the actions of a single humanitarian organization in a given context.

Image 1: *DIGID User consultation, Benane, Garissa County by International Center for Humanitarian Affairs (ICHA). October 2021*

Glossary

Cash and voucher assistance (CVA) - "refers to interventions where cash transfers or vouchers for goods or services are directly provided to recipients. In the context of humanitarian assistance, the term is used to refer to the provision of cash transfers or vouchers given to individuals, household or community recipients; not to governments or other state actors."[1]
Data protection impact assessment (DPIA) - "involves identifying, evaluating and addressing the impacts on Data Subjects and their Personal Data of a project, policy, programme or other initiative that entails the Processing of such data. It should ultimately lead to measures that minimize the risks to the rights and freedoms of individuals and should follow a project or initiative throughout its lifecycle."[2]
Decentralized identity - "an emerging concept that gives back control of identity to consumers through the use of an identity wallet in which they collect verified information about themselves from certified issuers (such as the Government). By controlling what information is shared from the wallet to requesting 3rd parties (e.g., when registering for a new online service), the user is able to better manage their identity online and their privacy – for example, only presenting proof that they're over 18 without needing to reveal their actual Date of Birth."[3]
Digital identity (digital ID) - "a collection of electronically captured and stored identity attributes that uniquely describe a person within a given context and are used for electronic transactions".[4]
Financial services provider (FSP) - "An entity that provides financial services, which may include e-transfer services. Depending upon your context, financial service providers may include e-voucher companies, financial institutions (such as banks and microfinance institutions) or mobile network operators (MNOs). FSPs includes many entities (such as investment funds, insurance companies, accountancy firms) beyond those that offer humanitarian cash transfers or voucher services, hence within CTP [cash transfer programming] literature FSP generally refers to those providing transfer services."[5]
Foundational ID - can often be a legal identity, which is typically issued by national authorities and enjoys a high level of trust from a wide range of other institutions and organizations, so using them allows individuals to access many different services that require identification. Foundational ID enables individuals to prove who they are.[6] Examples include national identity cards and birth certificates.

1 Cash Learning Partnership (2020). *Glossary of Terminology for Cash and Voucher Assistance*
2 International Committee of the Red Cross (2021). *Handbook on Data Protection in Humanitarian Action* (2nd ed.)
3 GSMA (n.d.). *"Decentralised Identity"*
4 GSMA, World Bank & Secure Identity Alliance(2016). *Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation*
5 Cash Learning Partnership (2020). *Glossary of Terminology for Cash and Voucher Assistance*
6 International Committee of the Red Cross (2021). *Handbook on Data Protection in Humanitarian Action* (2nd ed.)

Functional ID - entitles its owner to access only a single, or limited set, of services, usually provided by the same organization who issued the ID in the first place to authenticate the person.[7] Examples of functional IDs include health insurance cards and blood donor cards. People can have multiple functional identities (for example, a student ID and a voter number). DIGID deals with functional IDs instead of foundational or legal IDs for the purposes of delivering humanitarian assistance such as cash.
Guardian - in the DIGID context, a humanitarian organization may act as a guardian for an affected individual who is not able to or may not want to directly administer or manage their digital credentials. The organization therefore acts on behalf of and at the request of the affected individual, who ultimately owns their data, to process such data.
Guardianship - where dependents (or anyone lacking the interest or the technical, legal, or mental capacity to manage their own identity) can entrust another individual or organization to manage their digital credentials and wallet. Guardianship is a temporary condition while the dependent gains the capacity to become self-sovereign or reaches a certain legal age.[8]
Know your customer (KYC) - "This usually refers to the information that the local regulator requires financial service providers (FSPs) to collect about any potential new customer in order to discourage financial products being used for money laundering or other crimes. Some countries allow FSPs greater flexibility than others as to the source of this information, and some countries allow lower levels of information for accounts that they deem to be 'low risk'."[9]
Self-sovereign identity (SSI) - An identity system architecture based on the core principle that Identity Owners have the right to permanently control one or more Identifiers together with the usage of the associated Identity Data.[10]
Verifiable credentials - "Verifiable credentials represent statements made by an issuer in a tamper-evident and privacy-respecting manner."[11] "Verifiable Credentials, in essence, allow for the digital watermarking of claims data through a combination of public key cryptography and privacy-preserving techniques to prevent correlation […] The effect of this is that now, not only can physical credentials safely be turned digital, holders of such credentials can selectively disclose specific information from this credential without exposing the actual data (imagine proving you are above the age of 21 without having to show your ID card!), where third-parties are instantly able to verify this data without having to call upon the issuer."[12]

7 ibid.
8 Evernym (2019). *Making Digital Identity Work For All: The Role of Guardianship in SSI*
9 Cash Learning Partnership (2020). *Glossary of Terminology for Cash and Voucher Assistance*
10 Sovrin (n.d.). *"Glossary"*
11 World Wide Web Consortium (2019). *"Verifiable credentials data model 1.0"*
12 Tykn (n.d.). "*What are verifiable credentials?*"

1. Introduction

Background

People without official identity documents face barriers to accessing certain services and enjoying basic rights, such as voting, healthcare, education, banking, and social protection. They can also be excluded from humanitarian response.[13] In Kenya, the national ID system only covers about 88 per cent of those over 18 years old[14] and about 20% of people are considered unbanked.[15] People in Kenya who do not have official IDs can see their vulnerabilities exacerbated when disasters or crises occur.

The Kenya Red Cross Society (KRCS) estimates that 25 per cent of its humanitarian support caseload do not have governmentissued IDs. This creates a challenge to inclusion of the most vulnerable, who remain invisible because they are not recognized by government systems. Assisting affected communities of people with no official IDs often requires more effort to collect and verify personal data, and to ensure the right people are targeted for assistance.

KRCS aims to scale up its assistance in the form of cash and vouchers,[16] giving dignity and choice to people being served. Giving cash, however, becomes a challenge when humanitarian organizations use financial service providers (FSPs) to distribute money. Such providers are bound by financial regulations, such as "know your customer" (KYC), which require a governmentissued national ID. At present, to receive cash from an FSP, people without a recognized ID have to ask someone with an ID to collect money on their behalf. This procedure entails certain risks and can cause tensions within families and communities and does not promote financial inclusion for people with no IDs.

The Dignified Identities in Cash Assistance (DIGID)[17] project was started in January 2019 by a consortium of four large Norwegian NGOs – the Norwegian Red Cross, Norwegian Church Aid, Norwegian Refugee Council, and Save the Children Norway – and supported by Innovation Norway. The International Federation of Red Cross and Red Crescent Societies (IFRC) was the technical implementation lead. The aim of the DIGID project is to understand the opportunities and risks of digital ID technology in providing cash assistance to people with no recognized ID.

The implementation of the DIGID pilot project in Kenya was led by KRCS and IFRC. The other partners have a local presence in Kenya and participated as observers in project activities. In 2020, KRCS also implemented a separate project with the 510 team of the Netherlands Red Cross[18] that included a digital ID component that provided another opportunity to learn about the technology and its application.

Digital ID in humanitarian assistance, as several studies[19] have indicated, has a broad range of definitions for different stakeholders. One basic definition asserts that a digital ID is a collection of attributes about a person stored in electronic form, used to identify and authenticate that person. For DIGID, this goes beyond storage of personally identifiable attributes, which is already achieved by many humanitarian actors' beneficiary management systems. Rather, DIGID is interested in how personal data are accessed and controlled by individual data owners themselves and how those owners could use their data to access services from other organizations. The digital ID technology implemented and tested by KRCS and IFRC was based on standards of decentralized identity and verifiable credentials stored in digital wallets, which differs from traditional, centralized databases owned and managed by organizations themselves. These concepts are defined in the glossary.

13 IFRC (2018). *World Disasters Report: Leaving No One Behind*
14 Caribou Digital (2019). *Kenya's Identity Ecosystem*
15 World Bank (2017).*The Unbanked*
16 KRCS (2020). *KRCS Cash Transfer Programming*
17 DIGID website. *https://hiplatform.org/digid*
18 *https://www.121.global/portfolio/isiolo-kenya/*
19 IFRC (2021).*Digital Identity: An Analysis for the Humanitarian Sector*

Methodology

The findings and observations shared in this report are based on reflections after each milestone of the DIGID pilot project, from design to field implementation. Key informant interviews and focus group discussions were conducted with key stakeholders, including members of affected communities. Surveys were also conducted for post-distribution monitoring (PDM) to better understand feedback from communities in a more confidential manner.

This report's main limitations are that it captures observations from a narrow span of time and focuses on field pilots conducted in only two locations and the project activities leading up to them. There was not enough time to monitor whether users of digital IDs were able to use them to access future assistance.

Image 2: *DIGID disbursement in Mathare, Nairobi County by International Center for Humanitarian Affairs (ICHA). March 2021*

2. DIGID Field Pilot Overview

Project Milestones

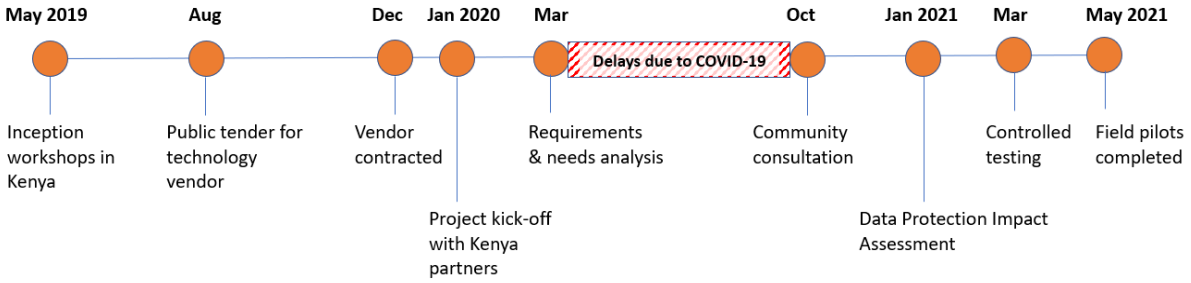


Figure 1: Timeline and major milestones for the DIGID field pilot in Kenya

The Kenya Red Cross Society has been exploring the innovative use of digital IDs through DIGID since 2019. Figure 1 shows the project timeline, its various activities and milestones. The project team started with a rudimentary understanding of digital IDs and gradually built up their knowledge of key concepts and technologies through research, discussions with technology experts, prototyping, and the practical application of concepts during the project.

To get a baseline understanding of key concepts and opportunities of digital IDs for humanitarian assistance, IFRC hosted inception workshops[20] in May 2019 in Nairobi, which brought together multi-stakeholder participants, including representatives from government, mobile money providers, and partner NGOs. These workshops also helped establish a baseline of requirements for the project and were used to source a technology vendor.

Following delays due to COVID-19, the community consultations[21] were successfully conducted in October 2020, followed by the technical architecture design and implementation of the solution. A series of controlled testing was done with KRCS volunteers, staff, and partner NGOs before introducing the solution to disaster affected communities. In parallel, a data protection impact assessment (DPIA) was formally conducted to identify the risks related to protection of personal data. The field pilots where digital IDs were issued to beneficiaries and used to authenticate them during cash distribution were carried out in April and May 2021.

Field Pilots

Locations	Mathare, Nairobi (urban)	Kalokol ward, Turkana (rural)
Cash amounts	One tranche of KES 5,800 (USD 52)	Two tranches, total KES 7,600 (USD 68)
Number of households targeted	100	200
Proportion of recipients with no official IDs	55%	100%

20 IFRC & KRCS (2019). *Kenya Digital ID Workshop Summary*

21 Gravity (2020). *DIGID Project User Consultation Report*

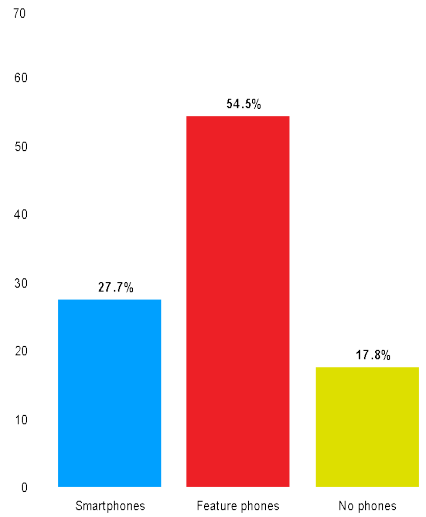
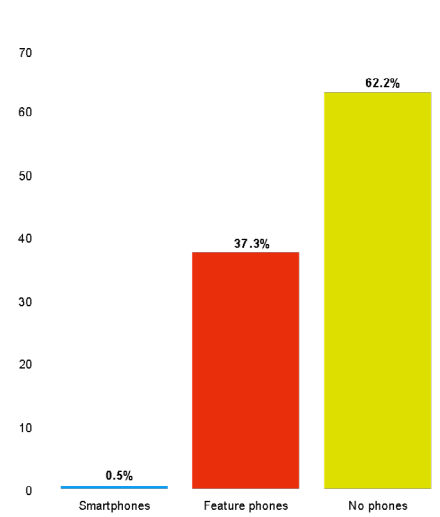
Locations	Mathare, Nairobi (urban)	Kalokol ward, Turkana (rural)
Date of cash distribution	April 2021	May 2021
Phone ownership		

Table 1: *DIGID field pilot comparison*

Image 3: *DIGID pilot project field locations in Kenya.*

Image 4: *A family in an informal settlement in Mathare, Nairobi being verified using the digital ID issued by Kenya Red Cross Society for cash assistance. April 2021.*

Image 5: *A community member from the Kalokol ward in Turkana county being registered using mobile data collection. April 2021.*

Over KES 2.1 million (19,000 US dollars) were distributed to 300 households as part of the field pilots to help address basic needs entailed by the COVID-19 pandemic. The selected beneficiaries had previously received assistance from KRCS and were chosen for the pilot based on their level of vulnerability caused by the pandemic. The cash assistance in this pilot was given as a top-up to the previous cash they had received, to continue to address the impact of the pandemic. Because of the limited budget for cash distribution, priority was given to people who 1) had no official forms of identity, 2) were highly vulnerable, and 3) were living in disasterprone areas.

The digital ID solution was tested in both an urban and a rural setting to highlight the needs of communities living in different contexts, and with varying access to digital connectivity and networked devices such as phones. A hundred households were reached in Mathare, an urban informal settlement in Nairobi, and 200 households were reached in the rural area of Kalokol ward in Turkana.

Figure 2 shows the process used in the field pilots. From beneficiary registration to cash distribution and PDM, the steps taken were largely the same as in a typical cash intervention and followed KRCS' standard operating procedures. This also included communicating with communities, local leaders, and authorities, to sensitize them to the programme and the digital IDs issued. Information desks and feedback mechanisms, including a telephone hotline, were made available in case there were questions or concerns from the communities.

The pilots also introduced new steps to the process: the creation of the digital wallet and digital credentials for the beneficiaries (Step 3 in Figure 2), the generation of an identity quick response (QR) code (Step 4) and using the identity QR code to verify the person when they came to claim their cash assistance (Step 5). All the other steps remained the same, which helped reduce the need for retraining of staff and volunteers on parts of the process they were already familiar with.

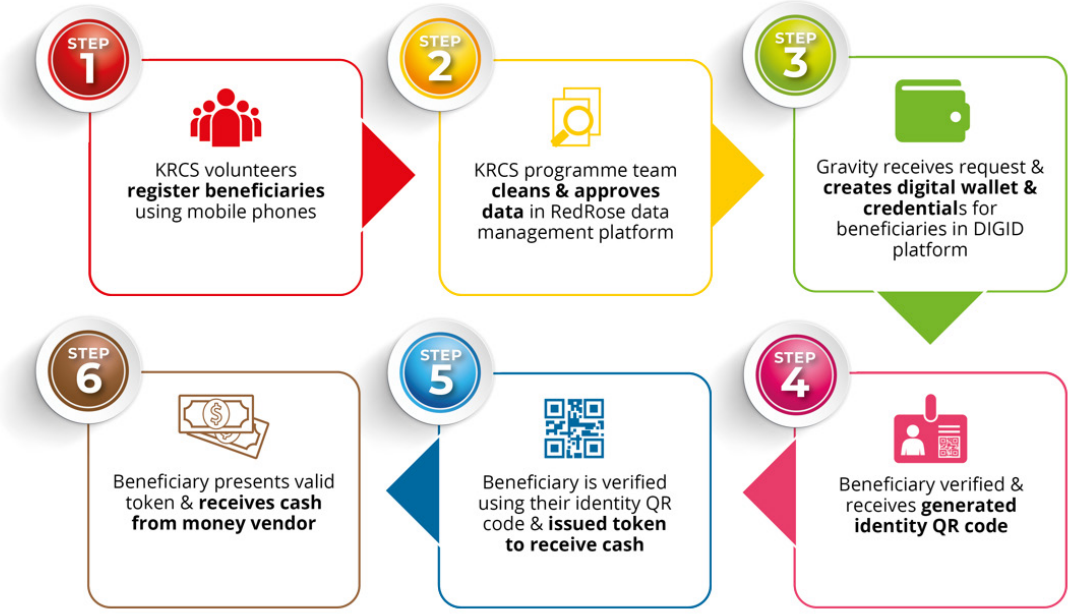


Figure 2: *KRCS DIGID field pilot process*

For beneficiary and programme management, the RedRose[22] solution was used, as it was already used by KRCS in other programmes. Mobile phones were used to register beneficiaries and the data were automatically uploaded to the RedRose platform, where they were reviewed, cleaned, and approved. Once approved, data were automatically sent to the DIGID system developed by the technology solution

22 https://redrosecps.com/

provider Gravity[23] to initiate the creation of digital wallets and credentials for each beneficiary. Not all data were sent from RedRose to create digital credentials. Instead, a selection of attributes was used to create digital credentials, based on the minimum set of information required for claiming cash, such as: name, location, age range, and photo. Details of the attributes used in the digital IDs in the pilot project are given in Appendix 2.

The creation of digital wallets and issuance of a digital ID depended on whether the end recipient had a smartphone, a feature or basic phone, or no phone. This was to ensure inclusivity for those who do not have access to digital means, and to distinguish the level of interaction with their digital identity data for those with devices. (See the related section on the findings related to low connectivity and inclusivity).

If an end user did not have a phone, their digital wallet was created for them by the humanitarian organization as their guardian[24] (in this case, KRCS) and an identity QR code was printed and handed over to them with a personal identification number (PIN) that they set during registration. If they had a feature phone, they received an SMS with their PIN and a printed identity QR code. Those with smartphones received an SMS to create their wallet and a QR code was generated in a web application. Appendix 1 gives more details on the various modes of interaction with phones.

Before the real-world creation of digital wallets, a hands-on training activity was carried out with members of affected communities who owned phones, to get a better understanding of how they could interact with their identities using their mobile devices. In Mathare, 55 per cent of target households had basic or feature phones, while 28 per cent had smartphones. In Turkana, most target households did not have a phone and network connectivity was not reliable, so participants there all received an identity QR code. This QR code was presented to a volunteer who verified them and once successful, a token was given to participants to use to claim their cash assistance (Step 5).

Because of "know your customer" (KYC) requirements, the targeted community members who did not have a legally recognized ID could neither own a SIM card nor have an M-Pesa account, so a cash transfer via M-Pesa was not a viable option for this pilot project. Cash distribution was done via Flex, a money distributor contracted by KRCS. The money distributor had agents to distribute cash on-site. The agents received the tokens provided by targeted households and distributed the cash (Step 6). At the time, discussions with the government and mobile money provider, Safaricom M-Pesa, were still in progress regarding the acceptability of these humanitarian digital IDs as an option for KYC. (See the related section on the acceptability of humanitarian digital IDs in actions taken so far.)

Two tranches of cash distribution were carried out in Turkana. An additional monitoring step took place before aid recipients received their second tranche, so the project team could identify whether there were issues or concerns with the digital IDs before the next distribution. Finally, PDM was implemented in both locations to determine whether the programme objectives were met (e.g., how cash was used) and to see whether there were additional issues, concerns, or feedback from communities regarding their digital identities.

Over KES 2.1 million (19,000 US dollars) were distributed to 300 households to help address basic needs entailed by the COVID-19 pandemic.

23 www.gravity.earth/

24 In this pilot, KRCS acted as the guardian for the data of those registered for cash assistance. The guardian safeguards the data on behalf of an individual and may share or update data if requested by that individual, who remains the owner of their data.

3. Findings and observations

Empowering individuals to own and control their data

Registering beneficiaries for assistance programmes is a common practice conducted by humanitarian organizations. This involves asking personal details of affected people, some being very sensitive (e.g. health conditions, religion, ethnicity). Data are stored in files or systems, sometimes for an indeterminate period, so they can be used to authenticate people targeted for assistance. Individuals do not have direct access to such systems, nor their data.

A token, such as a beneficiary card, might be printed with basic information (name, location, photo) about the person affected and handed to them to claim humanitarian assistance. Such a card is typically printed and distributed for a specific response intervention (or duration of a programme) and handed back to the organization for audit purposes later. An example of the beneficiary card is shown in the photo below.

Image 6: *Kenya 2017, Photo by Kenya Red Cross Society from Illeret town by Lake Turkana, where a community member shows her beneficiary card, which enables her to receive support from the Red Cross.*

In Kenya, beneficiary cards issued by KRCS are sometimes kept by their users and shown to others, including other NGOs, to prove that assistance has been received from the Red Cross. Even though the cards are not recognized by other institutions, the users feel some sense of personal value for a piece of paper or card with their names and basic details, especially when they did not previously have any other forms of ID.

The value of an ID, particularly one issued by a humanitarian organization, equates to its ability to be recognized and allow the owner to receive assistance. An ID is a means to an end, such as receiving cash assistance. The term "digital identity", however, was a concept that was difficult to grasp for many aid recipients. During the user consultation in October 2020, participants indicated the need for an ID but showed preference for a printed or physical form of ID, since its tangibility made them feel safer.[25] This perception may also be influenced by lower digital literacy and a lack of access to digital means, including mobile devices, in some communities.

Based on these initial learnings and observations, DIGID incorporated increased community engagement and accountability efforts in its project activities to allow KRCS volunteers and staff sufficient time for in-depth discussions with affected persons. Such engagement aimed to help demystify and explain the purpose of the digital IDs being issued by the KRCS – what data would be collected, how it would be used, and what end users could do with the digital IDs – as well as to get users' feedback on the overall solution and the problem it sought to address.

During the field pilots, the targeted individuals could receive a printed QR code with basic information (see photo below) or access and interact with their identity data using their phones. The field team monitored how the individuals used the printed QR code, checked whether people tried to view or access their data if they had a phone, and whether there was still a personal value attached to having such a digital form of ID.

Image 7: *A targeted community member in Turkana was given a digital ID in the form of a printed QR code with basic information. Scanning the QR code and entering their secured PIN unlocked more details about their personal data. May 2021.*

25 IFRC & KRCS (2019). *Kenya Digital ID Workshop Summary*

Some key observations emerged:

- **SAFEGUARDING TOKENS -** Some people (8 per cent of the PDM respondents) who received the QR code indicated that the printouts were easy to lose or misplace and deteriorated easily. This is consistent with any form of physical tokens, so it is important for organizations to address these issues. Also, end users were told that their digital IDs could be accessed via feature or smartphones, but this was not as helpful in areas with low connectivity and low access to mobile devices. Of the 200 people who were issued QR codes in Turkana, only two came to the second cash disbursement without their QR code because they had forgotten to bring them. This indicates that most people understood that they need to keep and safeguard their QR codes.
- **UNDERSTANDING OF DIGITAL ID -** It was not very clear to some end users what they could access with their digital IDs. In some consultations, people asked if they could use it to register for a phone line or receive transfer through M-Pesa. Between the two tranche distributions in Turkana, some aid recipients were asked why they thought their digital IDs were important. Most indicated access to humanitarian services. But 15 per cent of respondents indicated that they thought the IDs had legal value. When asked again during the PDM, a few weeks after the last distribution, none of the responders in Turkana indicated the legal value. This shows that the KRCS sensitization and communication efforts helped clarify that perception.
- **PERSONAL DATA OWNERSHIP -** Ownership and access to personal data was encouraged in the field pilot through the sensitization process, advertising the tollfree phone numbers to reach KRCS about the digital IDs, as well as posters and notice boards in schools and the local chief's office. However, people did not actively seek to own and access their data during the field pilot. There are three possible explanations for this. First, the digital ID users have inherent trust in KRCS to take care of their data, as was found during the community workshop[26]. Second, they may not perceive their data as valuable and worth expressing ownership over – this is unlikely to be the case, as community members indicated knowing the value of their own data when asked.[27] Finally, it may simply be the case that not enough time passed during the field pilot for participants to need or want to update or interact with their data. So, the project team indicated the need for more incentives for people to own and manage their data. For instance, KRCS could ask communities to use their digital IDs as proof of eligibility to access other services beyond cash distribution. Additionally, when eligibility is tied to changing attributes, such as family size, there might be more motivation to ensure personal data is up to date.
- **FUTURE OF INTEROPERABILITY -** Fifty-four per cent of PDM respondents indicated that they understand that their digital IDs could be used to access services provided by other NGOs. However, KRCS sees this as a future possibility rather than something that could be achieved immediately. Having other organizations use the digital IDs issued to screen eligible community members may also provide an incentive for individuals to own and manage their data.

> ***The value of an ID, particularly one issued by a humanitarian organization, equates to its ability to be recognized and allow the owner to receive assistance.***

26 IFRC & KRCS (2019). *Kenya Digital ID Workshop Summary*
27 Ibid.

Acceptability of humanitarian digital ID by government and FSPs

The digital IDs issued by KRCS are not meant to replace governmentissued IDs or be a form of legal ID. They are intended to allow people to receive humanitarian assistance consistent with the KRCS mandate. However, that mandate is difficult to achieve when a lack of IDs becomes a barrier to assistance such as cash. KRCS uses M-Pesa mobile money as the default for its humanitarian cash assistance. However, people can only receive money via M-Pesa if they have a SIM card and are registered for M-Pesa, both of which require a valid official ID because of KYC and SIM registration requirements.

During the 2019 inception workshop, an expert source noted that "the context for humanitarian purposes was important particularly in disaster emergencies, because of the lifesaving nature as well as a sense of temporary, time-bound activities… by working on advocacy with the government, there is a good chance for the acceptance of digital ID's issued by humanitarian organizations."[28] When FSPs were asked if they would accept KRCSissued IDs, they said they would defer to the government. If approved by the government, FSPs would be happy to accept such IDs with respect to KYC requirements. They have an incentive to support this initiative, as it has the potential to provide their services to the unbanked. The workshop report noted, "the financial services sector in Kenya is thriving and already quite advanced, but the challenge seemed to be that the laws need to keep up with the technology".

In 2020, KRCS reached out to both Safaricom and the Communications Authority of Kenya to explore the possibilities of using KRCSissued digital IDs to allow people with no official IDs to receive MPesa services. The communications authority has previously approved the use of SIM cards with limited functionality for closedloop or voucherlike transactions for humanitarian purposes.[29] The communications authority approved the KRCS request to pilot the use of SIM cards with limited functionality and to use digital IDs to facilitate cash transfer specifically for non-refugee populations.

KRCS communicated with Safaricom regarding the approval by the Communications Authority, but Safaricom required an official approval from the Financial Reporting Centre (FRC) as a regulator. The FRC approves all rules and regulations set by the KYC department and is part of the Ministry of the Interior. KRCS, with support from the GSM Association (GSMA), reached out to the FRC Head of Regulatory to seek approval.

The consultations with Safaricom and regulatory bodies continued in 2021, however feedback and approvals were not received in time for the DIGID field pilot to allow the KRCSissued digital IDs to fulfil the M-Pesa KYC requirements. KRCS continues to have these discussions and perform advocacy to the government and authorities.

In addition, KRCS is also maintaining a discussion with the government about linking humanitarian assistance with government social protection programmes, where many of the most vulnerable may not have official IDs. Obtaining approval from regulators to allow the use of humanitarian digital IDs for those seeking social protection and unable to attain official IDs would be another valuable opportunity for KRCS to extend its assistance to vulnerable people, who otherwise cannot access the services.

Discussions and advocacy with government bodies, authorities, and FSPs can be complex and time consuming, but are critical to achieving greater acceptability of humanitarian digital IDs.

28 Ibid.

29 GSMA (2017). *Refugees and Identity: Considerations for Mobile-enabled Registration and Aid Delivery*

Protecting individuals' data: is the solution safe and secure?

During the user consultation in October 2020, [30] the communities consulted found it difficult to understand the implications of digital identity, in terms of both its use and its impact on their personal data. They expressed the fear that their data might be misused or that they might become victims of fraudulent schemes, while indicating that there are certain data they are more willing to share (e.g., name and location) than others (e.g., national ID number, phone number). However, when humanitarian assistance is involved, communities seemed more willing to share personal data, particularly with KRCS. This highlights both the trust people have in KRCS to properly manage people's data, but also raises questions about the difficult choices vulnerable people must make when data are requested in return for material assistance. This puts more responsibility on KRCS to protect the data of the people they serve, the most vulnerable.

Mitigating the risks to individuals and their personal data was of the highest importance and was carefully considered throughout the DIGID field pilot, from design to implementation. Several actions were taken to ensure proper understanding of these risks; mitigations included:

- Reviewing and adhering to the KRCS data protection policy and the Data Protection Act of Kenya.
- Conducting a data protection impact assessment (DPIA)
- Consulting community members during the design process
- Facilitated prototyping for communities to better understand how to interact with their digital IDs
- Communicating with communities to sensitize them to the project and how the digital ID would be used to facilitate a cash transfer in support of COVID-19 response efforts
- Providing channels for complaints and feedback during the pilot (including a telephone hotline)
- Monitoring during and after the pilot.

From a technical standpoint, the implementation of a decentralized identity, as opposed to a traditional centralized database, sought to strengthen data security. The data storage mechanism used state-of-the-art encryption and privacy protection methods, such as splitting data across different nodes. This helped mitigate the potential for centralized hacking or unauthorized access. More details about the technical architecture are given in Appendix 3.

The DPIA analysed the data flows – the various systems that data pass through and where they are stored including the actors who process them. The DPIA also analysed the various legal bases, looking at which ones would be applicable for the provision of digital IDs to receive assistance from KRCS, but also for KRCS to take on a role as a guardian of such data, which could be used for other humanitarian purposes outside of KRCS services. One of the risks that the DPIA uncovered was the use of a third-party service for voice authentication instead of PINs to secure digital credentials, since literacy and language were issues highlighted by communities. The third-party vendor did not seem to have strong enough protection when handling beneficiary data, so it was decided not to use it for the pilot project. This data protection risk had to be balanced against convenience and ease of use of the system, but it was not felt that the benefits outweighed the risks. Box 1 gives for more details on the DPIA.

30 KRCS, Gravity, IFRC (2020). *DIGID Project User Consultation Report*

Box 1: Lessons from conducting a data protection impact assessment (DPIA)

Risks related to data protection and privacy of individuals, especially related to the use of new technology, were identified early on and monitored throughout. A key process to identify such risks and minimize their impact was the Data Protection Impact Assessment (DPIA) conducted during the design phase of the project. The process involved multiple stakeholders, including KRCS staff members from various units, including ICT, policy, innovation, cash, programmes and operations, and their data protection focal point. The technology vendor, Gravity, was also involved. This pilot project required a DPIA because the new technology in use had integration points with other, thirdparty systems, whereby personal data obtained from vulnerable communities would be processed which could have included sensitive information, and could pose risks to the individuals, KRCS, and its partners.

The DPIA referred to the KRCS data protection policy, the IFRC data protection policy, GDPR, and Kenya's Data Protection Act, which came into effect in 2019. The various international policies were considered because the technology's potential use outside Kenya by DIGID consortium partners.

The key lessons learnt were as follows:

- The DPIA was carried out based on the issuing of digital IDs and their use in providing cash assistance. Combining two different purposes created additional complexities in the analysis. For instance, the legal basis for the provision of emergency cash assistance might rely on legitimate interest or public interest, but not consent. And for the simpler use case of creating digital wallets, consent might be appropriate. In the future, the project team should consider analyzing the purposes separately.
- Conducting a DPIA is not a one-time activity to check off a deliverable, but rather the DPIA should be analysed and revised during and after the project implementation. The project complexity should not be underestimated, because the situation on the ground might change. Therefore, it is important to revisit the DPIA, evaluating and updating it as necessary.
- The DPIA is a tool that helps highlight risks and determine mitigation measures. However, the real work lies in the actions needed to address these risks. This may involve strengthening contracts with third party vendors, clarifying and communicating the various parties' roles and responsibilities, assigning an owner for specific dataprotection risks or concerns, and periodically monitoring the risks.

Accessing the digital credentials was done using PINs, which was not ideal because they were easily forgotten, but it served as a basic protection to prevent theft or fraud. Other options are being explored to provide more user-friendly ways to secure and access these credentials. For the pilot, since the QR codes were encrypted, the individuals had to enter a PIN code to authenticate and access the credentials. Users of feature phones received an SMS with the PIN. Smartphone user authentication was done by logging in on the device.

Monitoring activities were conducted. A survey was delivered in Turkana before providing the second tranche of cash assistance, and postdistribution monitoring was carried out a few weeks after the final cash distribution in both Turkana and Mathare. Only one survey participant out of 220 asked whether the data they provided would be kept confidential. This person was from the urban community. No other questions related to privacy, nor concerns related to digital identity, were brought up. There were some respondents who indicated wanting to learn more about digital ID and its use. Perhaps the lack of

direct questions and concerns relating to personal data was due to users' gaps in understanding of the direct impact on their privacy and personal data. Further engagement with communities may see them be more open to asking questions about and discussing privacy and data protection.

Making digital ID work in low connectivity settings

A key concept for implementing digital ID is "self-sovereign identity" (SSI), which refers to individuals maintaining control over their identity, providing autonomy for end users to use, manage, and store their identity attributes. To date, SSI has usually required good, stable internet connections, smartphone devices, and a good level of digital literacy among end users. The end user can initiate the creation of their own digital credentials stored locally on their smartphone and share claims electronically to third parties that need to verify their data in a secured, cryptographic manner. End users can also request to revoke their digital credentials. Here, the ownership is purely with the individual instead of an organization or third party holding their data.

However, applying SSI in humanitarian contexts is currently a big challenge. Many, if not most, of vulnerable, affected people are still living in rural areas, where infrastructure and good connectivity are not available. Also, very few people in these remote communities own phones at all, let alone smartphones.

In December 2020, KRCS and the 510 team of the Netherlands Red Cross conducted a pilot of the application "121" in Isiolo, Kenya. Among the conclusions was that SSI technology "currently has no value for the 121 platform",[31] one of the reasons being that "SSI is impractical because it requires users to have good internet connectivity and (for full functionality) smartphones, as well as high digital literacy".

Through DIGID, KRCS aimed to get a digital ID solution to work in lowconnectivity settings by addressing the following issues:

- Users having different devices (smartphones versus feature phones) or no device. Those without devices received an encrypted QR code with limited data.
- Feature phone users could opt for Unstructured Supplementary Service Data (USSD) interactions, while smartphone users were offered a web-based application that did not require a separate application to be installed.

It was noted that some connectivity is needed for digital IDs to be generated and verified in real time. The solution is not feasible for completely offline contexts. In Turkana, some residents were asked to go to an area with connectivity to have their identity QR codes issued and verified. This raises an important question about the digital divide, and how tackling this challenge is key to facilitating better access to identities and services. It is important not to create inequalities or exclusion for those who are not able to access digital services as easily as others are.

DIGID sought to compare the behaviours of end users from the urban and rural settings. Over 80 per cent of the members of the targeted communities in Mathare (an informal urban settlement) had access to a mobile phone, of which almost a third had a smartphone while others had only a feature phone. In Turkana (a rural area), 62.5 per cent did not own a phone of any kind. Some of the targeted individuals were also concerned about having to use their data credits or bundles to interact with the DIGID platform, meaning that the cost of using their phone's data connection could be a barrier using the platform within connected communities.

Issuing a printed QR code was a solution for those who did not have a mobile phone. The QR codes contained certain basic credentials and were encrypted and secured with PINs chosen by the users. QR codes did not confer users with the ability to directly manage their data, but they did provide a safe and secure way to authenticate themselves when needed. QR code recipients had to rely on the

31 IFRC (2021).*Digital Identity: An Analysis for the Humanitarian Sector*

organization that issued their credentials, in this case KRCS, if they would like to update or confirm the information being held. In this scenario, KRCS acts as a guardian of the individual's digital credentials. Existing beneficiary management systems currently manage data in a similar way, except that the QR code provides a layer of authentication that is not as easy with traditional beneficiary management systems.

There were some technical issues observed during the pilot, including some QR codes being unscannable and having to be replaced. Response time seemed slow, possibly due to bandwidth issues. Some users also needed more time to learn how to use the web-based application on their phones as they were not used to using applications. It is therefore important to provide more direct assistance to end users, as well as to test the solution in more varied contexts to see what the technological gaps are.

> ***... the cost of using their phone's data connection could be a barrier using the platform within connected communities.***

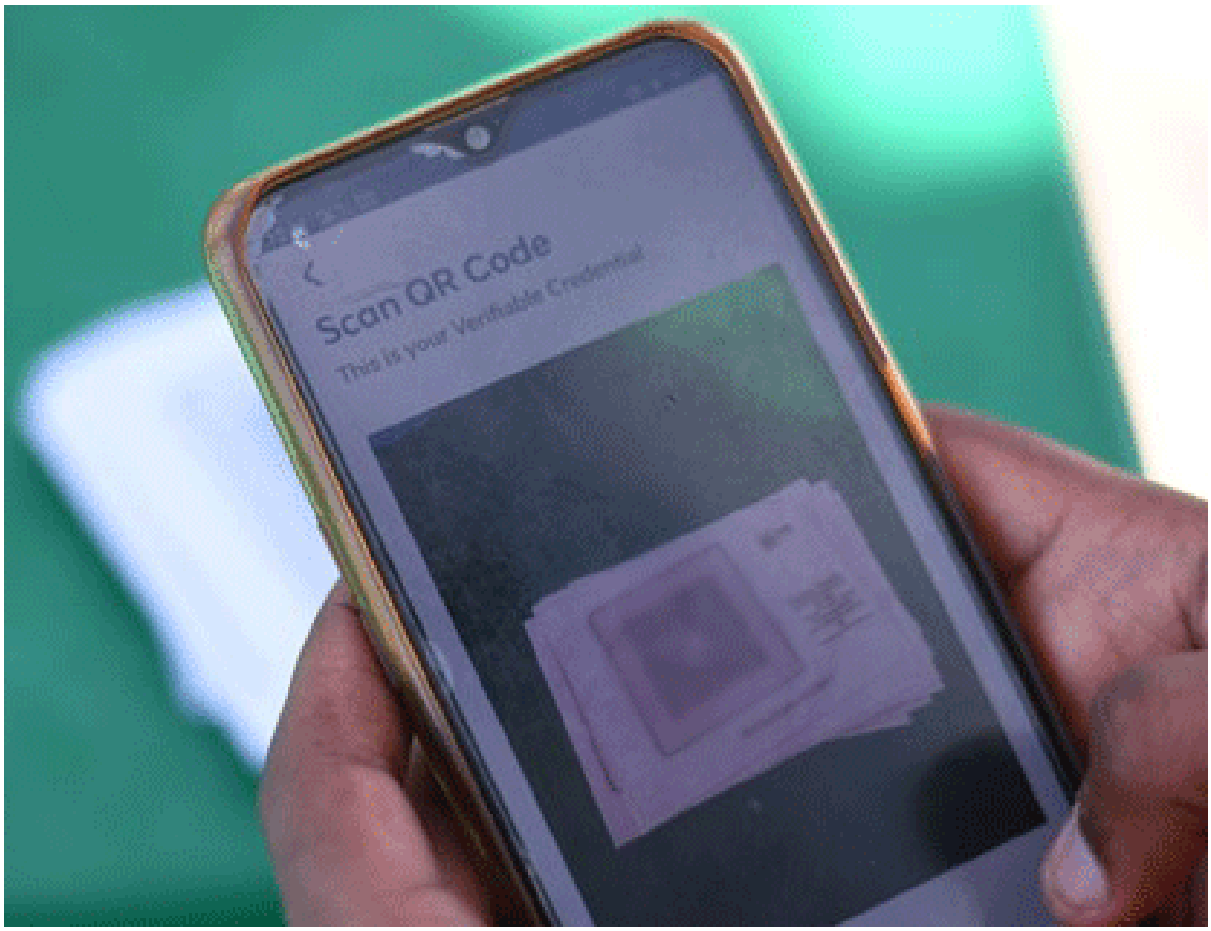


Image 8: *Verifying digital credentials required a smartphone that could scan QR codes. Mathare, May 2021.*

Adapting digital ID to the current technology ecosystem and processes

Many humanitarian organizations have invested in their own beneficiary management systems, which typically collect, store, and process personal data of aid recipients. Such systems are primarily used by organizations for their own purposes, to manage their programmes, to deliver and track assistance and to be accountable for the use of donor funds. These systems might hold large volumes of data, including sensitive personal information, such as biometrics, and they usually do not provide direct access for aid recipients to view, update, correct, or delete their own information.

Such personal data might also be required for other internal purposes and might be replicated in other systems or linked using reference data. An example of this would be finance or enterprise resource planning systems. For cash and voucher assistance, there could be an integration of internal systems with an FSP's system to automatically transmit the data of people to whom cash should be distributed. It is therefore important for organizations to examine their technology ecosystem to understand where beneficiary personal data is used, stored, or referenced, and to see how a digital ID solution might help improve privacy for individuals, while still addressing the organization's internal and institutional needs. More importantly, organizations should ensure data are not stored unnecessarily in multiple systems. One model could be to have beneficiary personal data stored only in the digital ID platform and having all other systems store only references to such data so there are no replicated copies.

Layering digital ID systems may seem duplicative, as data may reside also in internal systems, such as beneficiary databases as mentioned above. A thought piece published by the DIGID consortium[32] explored the differences between these systems and opportunities for complementarity. The article indicated, "it is possible that emerging digital ID solutions layered on top of traditional data management systems could offer humanitarian organizations the ability to enable beneficiaries to manage their own information, while offering efficiency gains for the agencies, themselves." Figure 3 compares the two systems and highlights, in particular, that beneficiary management systems are more likely to store programmatic information which has a limited duration (i.e., only needed for the duration of the programme) and should be deleted once purposes including audit are met.

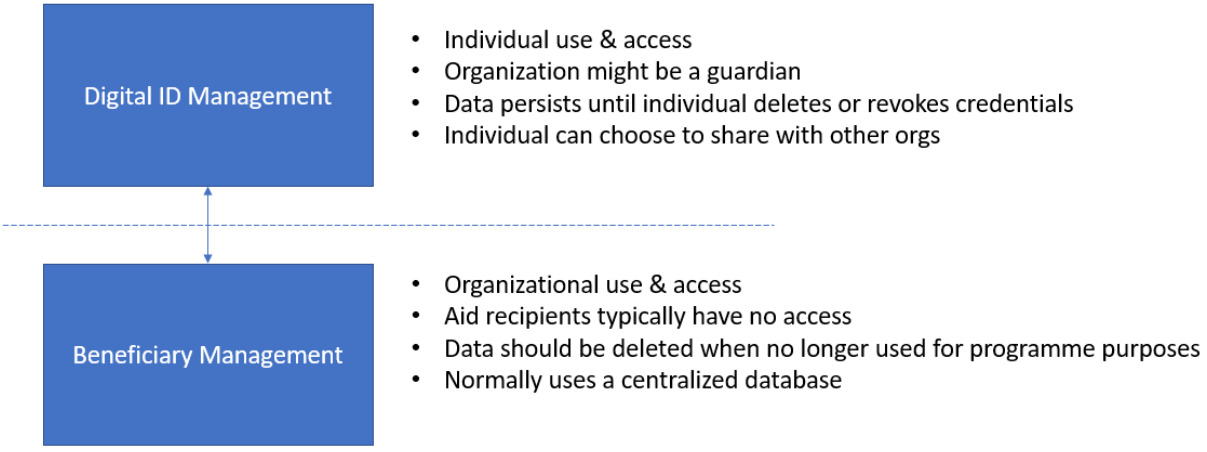


Figure 3: *Comparison of properties of beneficiary management vs. digital ID management*

A problem arises when data in beneficiary management solutions are used for more than the intended programming purposes and reused for other purposes, which could mean storing and processing data for longer than the initial purpose or need. This not only preserves duplicate copies, providing opportunities

32 DIGID (2020). *"Layering digital ID on top of traditional data management"*

for hackers and unauthorized users to access beneficiary data stored in multiple places, but also violates data protection principles.

For DIGID, the following was considered:

KRCS already uses the RedRose data management platform for beneficiary and programme management. What changes in the system and processes for registering beneficiaries would have to be made when integrating with a digital ID platform?

How to deal with data updates and deletion?

How would the digital ID platform be used for cash distribution. Specifically, how would FSPs use these data to authenticate aid recipients?

Since KRCS already had a data management platform for registering beneficiaries and managing programmes, it was decided to integrate the DIGID platform with RedRose instead of building a separate system or a new interface for registering beneficiaries[33]. The assumption was that data in RedRose would be used only for the limited time of the programme, while data in the DIGID platform would persist for the aid recipients to use for future assistance programmes or with other NGOs.

Keeping the existing beneficiary management solution helped maintain many of the existing processes (from registration to assistance provision) and the system that was already familiar to the field team. This saved time, from not having to re-train people with new solutions nor drastically change processes imposed by new systems.

There were some issues, however, when updating data, because integration with RedRose was only devised for the creation of digital credentials. When data updates were needed, they had to be done in both systems. Since there was no interface to update data in the DIGID system, this had to be done manually. The decision not to create a separate interface for DIGID was to ensure it did not duplicate functions provided by existing data management solutions. This integration to allow for updates in the RedRose system and automatically updating the DIGID solution should be prioritized in future.

Also, during the pilot, it was decided that the beneficiary data collected and stored in the RedRose platform would not be deleted during the programme because (1) deleting data in RedRose might have compromised the overall dataset, since there was not enough time to understand how the datasets were linked internally and risked data integrity issues, and (2) the personal data was needed to create the distribution list and deleting these data would mean having to re-extract data from the DIGID system when the operations from registration to distribution were done in a relatively short timeframe. These issues highlighted the need for more thorough analysis of the data flows and the implications of updating and deleting data. This also suggested the need for better data governance, from creating digital credentials, through updating attributes, to deleting and revoking credentials. With integrated systems, changes done in one system may impact another.

Deciding which data collected during beneficiary registration would be used to create digital credentials was also not straightforward. Not all the data collected during beneficiary registration and stored in RedRose for programme use were converted to digital credentials. One school of thought was to store basic data that are typically collected by KRCS programmes so that these could be readily available for future programmes. Another school of thought asked the question, "Which data would be needed by the FSP to distribute cash?" and suggested minimizing the data in the digital credentials. In the end, KRCS decided to store basic programmatic data, including more information than just that required by an FSP (see Appendix 2).

33 This was a different approach taken compared to the 121 project by KRCS and the Netherlands Red Cross 510 team, where an end-to-end system was used, featuring a new registration interface that created digital credentials and requiring KRCS to manage data in a separate system than what they had previously been using.

There is still much to learn in integrating existing beneficiary data management solutions with digital ID systems, but the experience in the pilot project suggested that having a technical architecture that allows for modular services or systems to be plugged in has the potential to lower the barrier to introducing digital ID systems, because this would not be seen as replacing existing investments and drastically changing the processes by introducing new systems.

Figure 4 shows how the DIGID platform was integrated with the KRCS technology ecosystem. The technical DIGID architecture (see Appendix 3) allowed for flexibility in changing the digital ID provider as well as the data collection, data management, and financial service providers used by the humanitarian organization, so the latter could have a choice of which solutions would be better for them (see the section on interoperability with other digital ID technology providers).

Modular architectures offer flexibility, so organizations are not locked in when a given technology are no longer able to meet their needs.

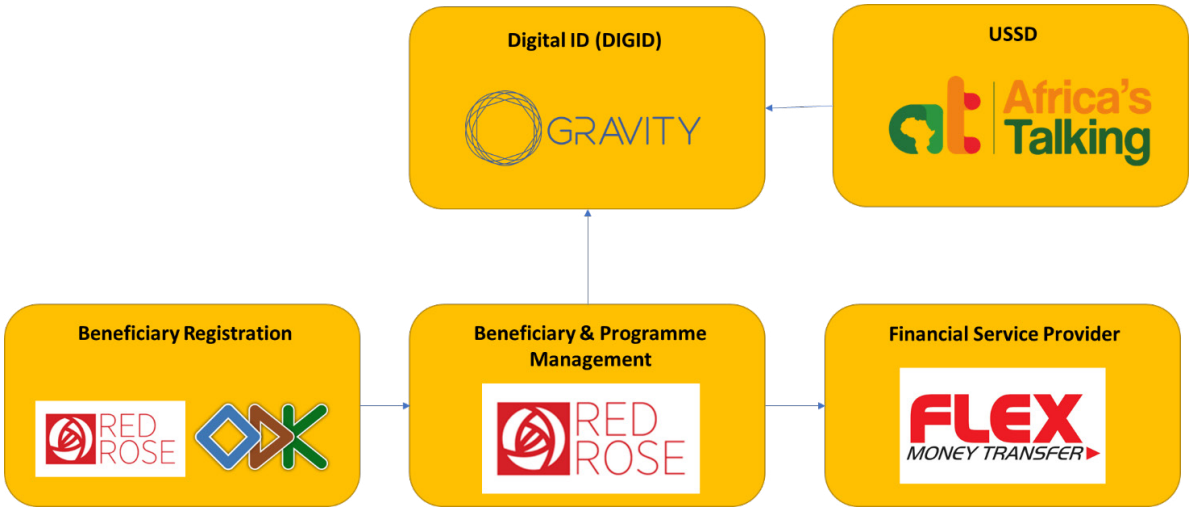


Figure 4: KRCS systems integration

Interoperability with NGOs

During the workshop in 2019, attendees from different humanitarian organizations admitted barriers to sharing data among NGOs (e.g., competition, donor requirements, lengthy negotiations over data sharing agreements). One key informant from an NGO who spoke to the DIGID consortium indicated, "we have our own ways of doing things," and was skeptical about using common systems or sharing common data but did admit that they do have common objectives with other NGOs. There have been efforts to address these barriers "in the spirit of coordination, reducing duplication, and overlaps" as the cost of providing humanitarian assistance is rising, increasing demands on a strained donor and humanitarian system[34]. In fact, for the last two years, international humanitarian aid has dropped, despite the increasing need[35] Humanitarian organizations are investing to become interoperable in terms of the beneficiary data in communities they serve. However, these efforts have been with systems owned by organizations where individuals have no direct access, raising questions of whether individuals have a choice in terms of their data being shared and whether they were informed to begin with. The affected individuals continue to lack control and power over their own data.

All the NGO members of the DIGID consortium have a local presence in Kenya, and in certain regions or locations provide services to the same communities (e.g., in Kakuma, Norwegian Refugee Council, Save

34 IFRC (2019). *Cost of Doing Nothing*
35 Development Initiatives (2021). *Global Humanitarian Assistance Report*

the Children Norway, and KRCS all provide services, as do other NGOs). Some processes are clearly duplicated because these organizations have their own systems and conduct their own registrations, and sometimes multiple different teams or programmes within an organization can have multiple registrations. Reducing the amount of registration by having such data available promises gains in efficiency. More importantly, individuals could access and control their own data and present their digital credentials to such organizations to receive assistance, rather than having to go through multiple registrations, which can cause survey fatigue and, in certain cases, having to relive traumatic experiences multiple times.

With DIGID, the aim was less about direct sharing of information between organizations, but rather the ability for multiple NGOs to read, recognize, and accept the digital credentials issued on their behalf by other humanitarian organizations when such credentials are presented to them by the affected individuals themselves.

The key issue is whether NGOs would trust credentials issued by other NGOs. In emergencies, NGOs ask for beneficiary lists from multiple actors including government authorities, civil society and other humanitarian agencies. In the spirit of providing lifesaving assistance as quickly as possible, some data are shared with or without formal data sharing agreements. Trusting data from other NGOs may depend on the rigor and level of verification that such organizations put in. Also, there are grassroots organizations that have been working with communities and know them better than others. NGOs' reputations and the level of trust they enjoy among communities also play a role. One NGO staff member who observed the DIGID pilot project in Turkana indicated that the use of such digital IDs was positive and important, adding, "we reach communities in different ways and if we [humanitarian organizations] recognized the same IDs, we can minimize duplication and reach more vulnerable people… those who are reached now are usually with IDs and those without are not reached at all."

An attempt was made in the context of DIGID to test this level of interoperability, albeit only in a safe and controlled testing environment and not during the field pilot. When one NGO partner who was present during the field pilot cash distribution was asked, "Do you think your organization will be more efficient in registering community members using DIGID credentials?", they agreed. When asked whether they would trust the KRCS data collection and verification processes used to issue the credentials, they also agreed. These NGO staff members being present during the registration process to see how it was done undoubtedly influenced these opinions.

Interoperability with other digital ID technology providers

DIGID defines "interoperability" between different digital ID providers and technologies to mean these systems' ability to connect and exchange information with each other. This is important because (1) it allows organizations to choose a digital ID provider based on their needs and preferences instead of being locked in, (2) it allows end users to seamlessly use their digital credentials without being siloed to one technology or vendor that organizations might use, and (3) if a digital ID provider no longer exists, then the credentials created should continue to exist. Initiatives such as ID4D and ID2020 are working for meaningful interoperability among digital ID providers.

ID4D, an initiative of the World Bank, which brings knowledge and expertise to support countries in building inclusive and trusted digital identification systems primarily for legal IDs, indicated that "Interoperability is crucial for developing efficient, sustainable, and useful identity ecosystems"[36]. ID2020,[37] an alliance of private and public sector entities that believe in the transformative impact of user-managed, privacy-protecting, portable digital ID, has developed a manifesto[38] that outlines the shared principles

36 World Bank (n.d.). *"Interoperability"*
37 *https://id2020.org/*
38 ID2020 (2020). *"Manifesto"*

guiding an ethical approach to digital ID or what they refer to as "good" ID. One of the principles suggests interoperability as a means for establishing "trust and recognition". They believe in technologies that "focus on modularisation, open standards, open APIs, and the portability of data between component systems, each of which is critical for interoperability, portability and avoidance of vendor lock-in."

For the value of digital IDs to be utilized fully by aid recipients, there needs to be interoperability between NGOs as discussed above, but also interoperability between digital ID technology vendors and providers.

KRCS has run pilot projects with two different digital ID providers: Tykn[39] for the 121 project and Gravity[40] for DIGID. It was therefore convenient to look at interoperability between the two providers as part of DIGID, to understand how interoperability could be achieved in practice. Few attempts have been made to demonstrate interoperability within decentralized identity, and this interoperability test is novel because it is between different decentralized identity wallets based on two distinct protocols that leverage very different technology stacks and networks.

Common standards and protocols contribute to interoperability. The World Wide Web Consortium (W3C) is an organization that helps develop standards, protocols, and guidelines that ensure the growth of the web. Although both Tykn and Gravity adhere to the W3C standards of decentralized identifiers (DID)[41] and verifiable credentials[42], the protocols have different ways of creating connections and exchanging messages and credentials. In addition, their public keys and schemas are stored on different public ledgers and use different verification algorithms. These issues are actively being addressed in different working groups within W3C and the Decentralized Identity Foundation, but, according to Gravity, it will likely take several years to achieve full interoperability.

For the value of digital IDs to be utilized fully by aid recipients, there needs to be interoperability between NGOs as discussed above, but also interoperability between digital ID technology vendors and providers.

39 https://tykn.tech/ Tykn is a Netherlands-based software company developing digital ID solutions based on the Ana Cloud platform built on Sovrin SSI technology.

40 https://www.gravity.earth/. Gravity is a technology company with offices in France and Kenya and one of the first to be granted ID2020's certification mark, indicating they meet ID2020's technical requirements (e.g., usermanaged, privacyprotecting, interoperable) that contribute towards their "good" ID principles.

41 W3C (2021) "Decentralized Identifiers (DIDs) v1.0"

42 W3C (2019). "Verifiable credentials data model 1.0"

Table 2 shows some of the main differences in the Gravity and Tykn implementations, which gives a sense of the complexity required to achieve interoperability.

	Gravity	Tykn
Identifiers *Both rely on a new type of identifiers introduced by the W3C called* *decentralized identifiers (DIDs).*	*Hashed format of public key prefixed by did:tz*	*Encoding of Universally Unique Identifier (UUID) prefixed by did:sov*
Verifiable Data Registry *W3C describes verifiable data registries as a public decentralized ledgers that store public metadata associated with DIDs.*	*Uses Tezos blockchain*	*Based on the Sovrin network, which uses Hyperledger Indy*
Governance & Blockchain	*Tezos Blockchain: public, permissionless Blockchain. It is accessible via a public network* *so anyone can access it (public) and anyone can be a validator node of the chain* *(permissionless)*	*Hyperledger Indy: public, permissioned Blockchain. It is accessible via a public network* *so anyone can access it (public)*
Credential Issuance *Entities issuing data, known as issuers, can attest information on beneficiaries. This data lands in their wallet that they (or their guardian) control.*	*Issuers can directly issue data to the wallet of the beneficiary*	*When issuers issue data, it is the task of the beneficiary to accept or not the credential in their wallet*

Table 2: *Summary of differences between Gravity and Tykn*

The interoperability test between Gravity and Tykn was done as a simulation in a controlled virtual environment. The use case tested looked at how NGO A could issue credentials to a beneficiary, who could then easily share these credentials with NGO B. Interoperability would allow NGOs A and B to use different decentralized identity protocols for issuance and verification, while still allowing a beneficiary to easily share credentials between the two organizations to gain access to different services.

The interoperability test demonstrated that two NGOs can use different decentralized identity platforms to register and deliver assistance to the same set of beneficiaries. This was made possible by associating a beneficiary's different DIDs with each technology provider. This was required because each DID was specific to the two different decentralized identity platforms being used. Allowing for these DIDs to be associated with one another meant that NGOs could use both sets of DIDs and issue credentials to both decentralized identity platforms. This is useful because it allows NGOs to share data with each other and beneficiaries without having to agree on a common identifier (such as a phone number, national ID number or systemgenerated ID number) that is needed to identify a beneficiary between two separate systems.

The interoperability test was promising, as it suggested the possibility for different digital ID providers with different technology stacks to work together. The test, however, was only done as a desktop exercise, triggered by software codes and inputs, with no user interface. It was therefore limited in terms of understanding the end-user experience of interacting with digital credentials. It also involved creating two wallets, since these were still specific to the technology used; the implications of managing multiple wallets are unclear and require further analysis.

Engaging with the wider technology sector and experts in digital ID, particularly those with influence over standards development, is key to ensuring that interoperability for humanitarian use cases is included and addressed in discussions and further development. Also, conducting more technical interoperability tests with other digital ID providers would help identify areas for improvement. The DIGID solution has been developed with a combination of open-source and proprietary components from Gravity. The open-source components and source codes are available for those interested in improving the current solution or exploring how other systems could be interoperable with the DIGID solution.

Engaging with the wider technology sector and experts in digital ID, particularly those with influence over standards development, is key to ensuring that interoperability for humanitarian use cases is included and addressed in discussions and further development.

Image 9: *Verifying digital credentials using a smartphone that scans QR codes. Daadab, 2021.*

4. Recommendations

The lessons learnt the DIGID design, implementation and field piloting are important not only for the Kenya Red Cross Society to continue to improve on their use of the DIGID platform, but also for other organizations looking to develop their own solutions or interested in digital ID technology. The key recommendations for the wider humanitarian sector are as follows. Organizations should:

- Reflect on the following principles, which are the basis for adopting a solution like DIGID: user-owned or user-controlled data; strong focus on data privacy and data protection; interoperability between humanitarian actors to recognize humanitarian IDs.
- Review their technology ecosystem related to affected community identification. Can privacy and protection of affected people's data be improved? Do people have access to their own data, and the option to update data or request data deletion? Indeed, traditional beneficiary databases do not offer the functionality to allow end users to manage and own their data.
- Seek to collaborate and ensure humanitarian digital IDs are recognized. There is potential for organizations to improve coordination and accountability to affected people, reduce costly and duplicative registration processes, and promote the dignity and privacy of individuals.
- Advocate to governments and authorities for humanitarian identities to be recognized as fulfilling KYC requirements (temporary access, shortterm, limited funds). In emergency situations, this could contribute significantly to lifesaving action. Such advocacy will be more effective when groups of humanitarian actors enact it together.
- Engage with the private sector and technologists and educate them about use cases and challenges in humanitarian action. This will allow technology to be better shaped to the unique context humanitarians face.

5. Conclusions

The Kenya Red Cross Society is committed to upholding the dignity of the people it serves as it pursues its mission of preventing and alleviating human suffering. Identifying people in need of assistance is at the core of programmes and operations, as well as organizational accountability. The concern here is not only about the efficiency and effectiveness of a single organization, but also about empowering people with their own personal data and working with other organizations to ensure the identities of the most vulnerable are recognized to quickly provide assistance, while ensuring privacy and data are safeguarded.

The DIGID field pilot was the first step in realizing this greater vision of providing dignity through humanitarianissued digital IDs, especially for those who have no other forms of ID. With the pilots in Mathare and Turkana, targeted communities affected by COVID-19 and who did not have official IDs not only received cash assistance directly, but they also had an opportunity to see how to manage or access their own data. Also, a wider dialogue with regards to identities was convened with stakeholders such as local government officials, community leaders, and other organizations.

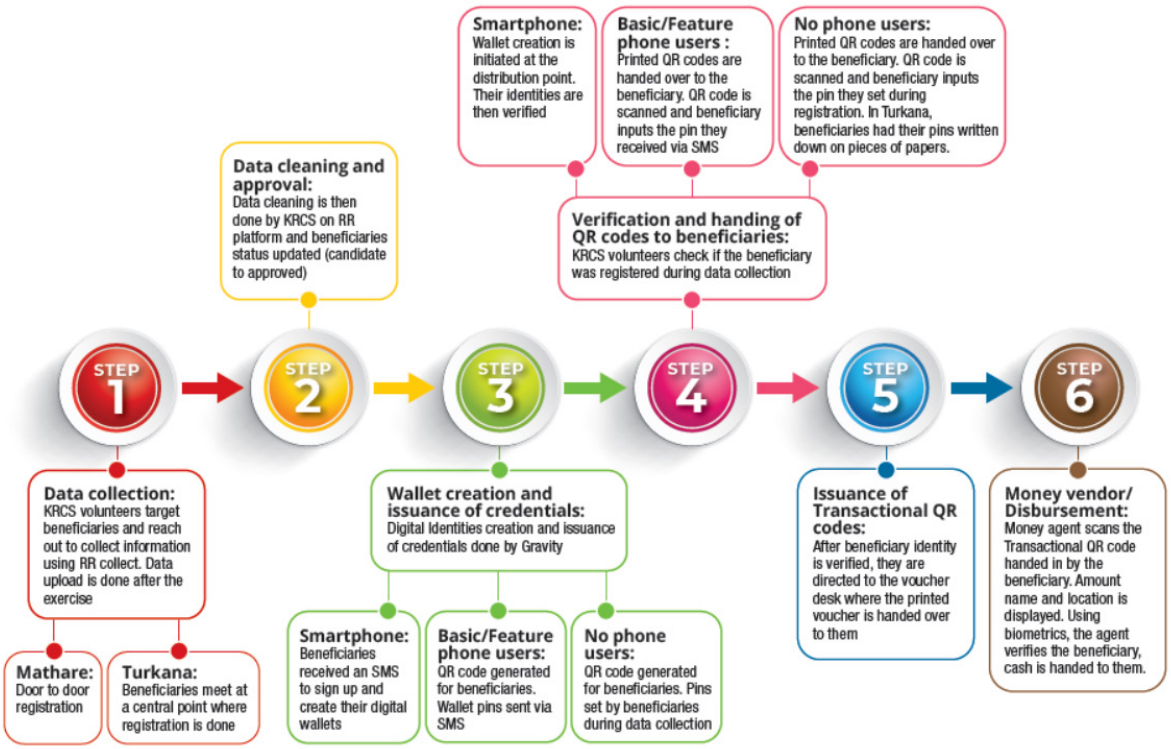
This dialogue, in combination with the practical lessons from the field pilots, are key to ensuring digital IDs issued by humanitarian organizations are useful for both organizations and individuals themselves, and that opportunities and risks, particularly to individuals, are evaluated as part of adhering to the do-no-harm principle. Trust was a central factor in communities' acceptance of the digital ID solution proposed by KRCS. It is therefore critical to ensure data related to identification are safeguarded and protected by KRCS and other humanitarian organizations.

During the piloting process, issues and challenges were identified related to technology, governance and policies, and reflecting on and addressing these will be important as more use of the digital ID technology is envisaged. Based on this experience, KRCS is planning to develop policies and a framework for digital IDs.

KRCS also plans to pursue further advocacy with the Kenyan government and FSPs, such as MPesa, to have digital IDs recognized as fulfilling KYC requirements so that affected people with no official IDs and made vulnerable by crises and disasters can nonetheless receive cash assistance. KRCS intends to continue to work with other units and programmes within its organization to identify opportunities to use digital ID in providing other essential services besides cash, and to explore their use in other sectors, such as volunteering, migration and health. KRCS is part of wider humanitarian sector coordination and collaboration bodies such as the Kenya Cash Working Group. Continuing dialogue with other humanitarian organizations on the acceptability of such digital IDs, particularly to receive cash assistance, is also foreseen.

6. Appendices

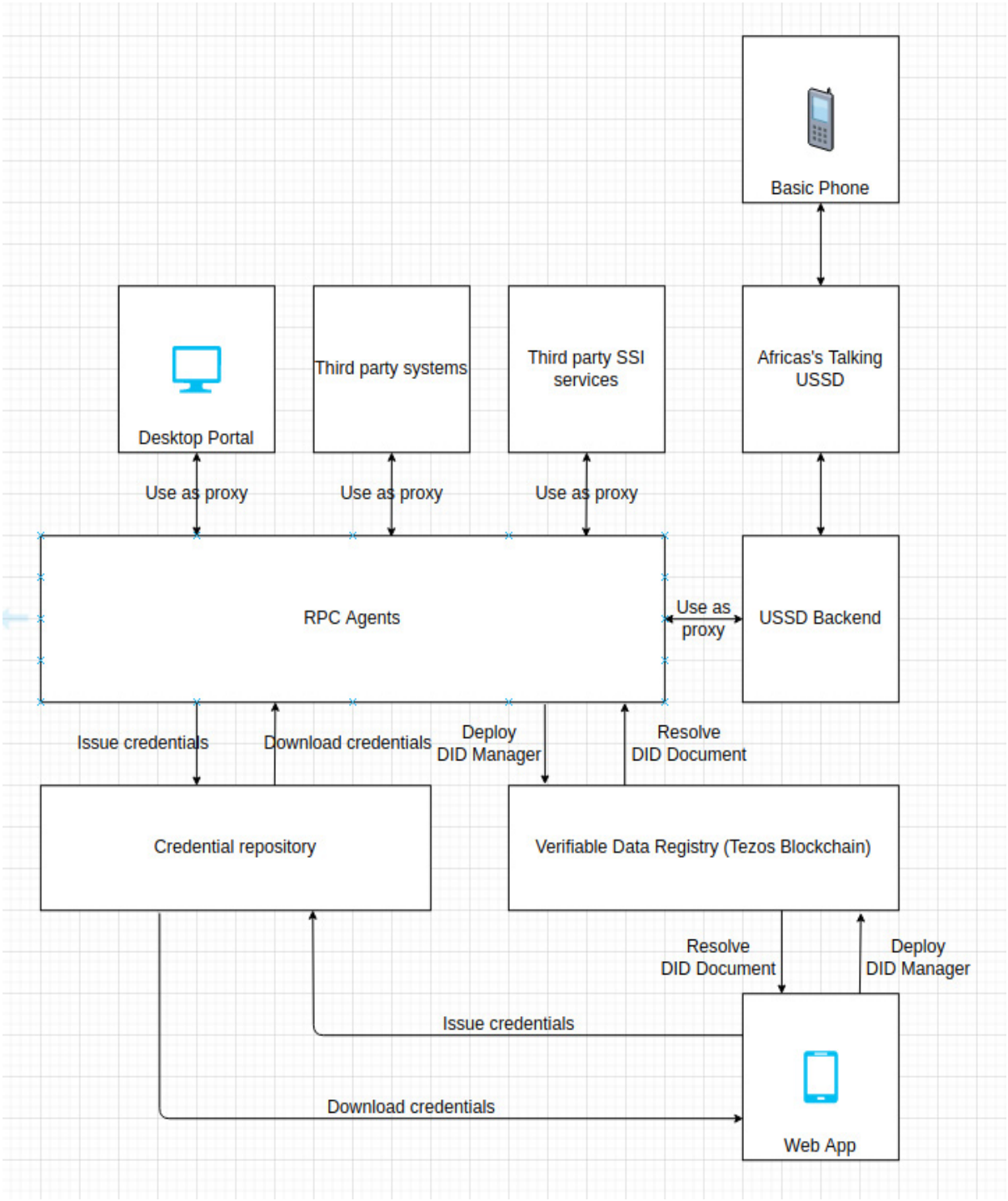
Appendix 1: Detailed DIGID process flow



Appendix 2: Digital credentials created in the pilot

- Geographical location
  - County
  - Sub-county
  - Ward
  - Location
  - Sub-location
  - Village
- Name of local area chief
- Name of local area assistant chief
- Name of household head
- Type of ID (if there is one)
- ID number (e.g., National ID number or left blank if person does not have an official ID)
- Type of phone (e.g., smartphone, basic/feature, or no phone)
- Phone number (left blank if person has no phone)
- In case of an alternate phone contact, name of that person
- Type of phone
- Gender of household head
- Marital status of household head
- Age (in completed years) of household head
- Do you give consent for your photo to be taken?
- Photo of household head
- How many members (including household head) are in the household by age and gender
- Vulnerability
  - Are there household members living with disabilities?
  - Type of disability in the household?
  - Number of people living with disability by gender
  - Number of pregnant household members
  - Number of lactating household members
  - Do any members of the household live with chronic illness?
  - Number of people living with chronic illness
- Remarks or comments from KRCS
- GPS coordinates

Appendix 3: DIGID Technical architecture



Component	Description	Status
Backend layer		
Core package	The Gravity core package is a JavaScript implementation of the W3C decentralized identity and verifiable credential standards. This allows the creation of very low-level, components including W3C verifiable credentials, verifiable presentations and DIDs, and provides cryptographic encryption and signature algorithms.	Open source
Remote Procedure Call (RPC) Agent	The agent is a server which can be used outside the DIGID ecosystem. It could be set up on customer infrastructure or used by a guardian. This server exposes an advanced programmable interface reachable via the public network (https requests). Each party able to host such an agent is then able to remotely, in a secure and close environment, perform high level operations, including wallet creation, encrypted credential issuance and sharing, credential management and account recovery.	Open source
Credential repository	Beneficiaries' credentials are stored on a decentralized credential repository. The credentials, which are encrypted by the issuers for the subjects, are split up and stored across different nodes. Multiple trusted entities can participate in storage. It is necessary to have secure cloud storage, since the solution does rely on web applications instead of native applications, and guardianship also requires secure cloud storage.	Proprietary (Gravity)
Software development kit (SDK)	The SDK is a library developed by Gravity, running on the background of the progressive web-based application (PWA) or the Gravity agent. It uses the core package to create lowlevel objects and orchestrates the communications between the other services, such as the PWA, the RPC agent, Verifiable Data Registry (Tezos Blockchain) and the Credential Repository. It is also responsible for managing the keys used for the decentralization authentication process.	Proprietary (Gravity)
Frontend Layer		
Unstructured Supplementary Service Data (USSD) application	Basicphone users will interact with the solution via a USSD menu interface, which relies on a PIN for authentication. Basicphone users will therefore be able to perform consent & share, update & delete, view & verify operations as per requirements.	Open source
Progressive web-based application	The application is accessible via smartphone and web browser. Smartphone users can encrypt and sign credentials and consents directly on their phone. The application retrieves the received credentials from the Gravity credential repository. It receives presentation requests directly from relaying parties, resulting in the credential being shared on to the requester's RPC agent.	Proprietary (Gravity)
Portal	An existing beneficiary management system can leverage the Gravity core package to build, sign, and encrypt credentials and send them directly to a beneficiary's wallet. However, in some cases this kind of integration might not be possible due to technical limitations. Therefore, such a portal needs to have direct connection with a remote RPC Agent.	Open source

Table 3: *Summary of differences between Gravity and Tykn*

The DIGID platform relies on a decentralized identity ecosystem. That ecosystem is built on top of two decentralized storages:

- **Verifiable data registry** that stores public information, and
- **Credential repository** that stores the private credentials.

For this information to be downloaded from the verifiable data registry, public assets must be recorded on an underlying system or network of some kind. Blockchain technology has been chosen for multiple reasons, as follows:

- **Authentication:** Blockchain technology relies on transactions that are cryptographically signed, which means that operational senders on the registry can be natively verified, ensuring only authorized entities can perform those operations.
- **No central control:** The decentralized identity standard recommends the use of public, decentralized registries. This is to avoid vendor lock-in, singlepointfailure and censorship, while giving entities the opportunity to control and manage their own identities without needing external authorities. Public blockchains provide mainnet instances that fulfil the requirements with thousands of independent nodes, making attacks to take over the registry impossible.
- **Security:** Blockchain is powered by cryptography at a very deep level, namely elliptic curve cryptography. This algebraic approach results in fast, robust algorithms that guarantee the safety of cryptographic keys. Additionally, redundancy across the multitude of nodes makes blockchain fault tolerant. Even if some nodes go out of service, the peer-to-peer mechanism is still running and those nodes will get synchronized when they are up again, preventing any loss of data.

Personal data storage and the blockchain

A combination of different types of public keys, along with a link to the decentralized credential repository, are stored on the blockchain[43]. No directly personally identifiable information, such as names or addresses, are stored on the blockchain.[44]

How the technical architecture has been contextualized for Kenya

It is important to note that the DIGID platform is modular and, therefore, adaptable to different regional and organizational contexts. Since the field testing was to be conducted in Kenya with the Kenya Red Cross Society, certain elements of the technical architecture and flows were customized to this context.

Specifically, the integration with RedRose to allow for credential issuance directly from the RedRose system was done to demonstrate that the DIGID platform can be seamlessly integrated with an NGO's existing data and beneficiary management systems. Integrating with data and beneficiary management systems other than RedRose is therefore possible in case an NGO chooses to do so.

Additionally, the choice of USSD as an interface for guarded (i.e., non-self-sovereign) beneficiaries was due to its widespread use and familiarity in Kenya, given mobile money services' reliance on it. NGOs may also opt for another interface, such as interactive voice response, or other interfaces suited to beneficiaries' preferences.

Last, a dedicated cloud storage was deployed in Kenya for the duration of the field testing to avoid international data transfers in compliance with the Kenya Data Protection Act of 2019. NGOs may choose to use cloud storage in Kenya or in another jurisdiction of their choice. This may depend on the NGO's internal data protection and information security policies, as well as the local regulation in the country of operation.

43 Gravity (2021). *DIGID Project Technical Specifications*

44 According to the KRCS DIGID DPIA, the public keys stored on a distributed ledger (in this case Tezos blockchain), are considered personal data.

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