Request for Proposal

Dignified Identities in Cash Programming (DIGID)

Norwegian Red Cross

June 2019

TABLE OF CONTENTS:

1. Introduction

Due to lack of recognized proof of identity, roughly 1.5 billion individuals (World Bank, 2016)[1] face challenges in accessing or enjoying basic rights and services such as voting, setting up a bank account, registering a business, land ownership, receiving social protection payments, school enrollment, and even humanitarian assistance.

Identity (ID) management remains one of the biggest challenges for humanitarian action. The causes for not having an official proof of identity vary. Some people may have lost documents during a natural disaster or fleeing from conflict. Others have never owned an ID, due to cumbersome procedures, high costs, lack of knowledge on how to register for a National Identity Card (NIC) or lack of feeder documents, such as birth registration. Lack of government identification can make people "invisible" and hamper effective humanitarian assistance.[2] Attempts to address this issue are often ad hoc and siloed within individual aid organizations.

Early experiences in developing digital ID solutions seem to indicate potential for empowering and engaging recipients of aid, facilitating efficient and large-scale cash transfer programming (CTP), and enhancing coordination and collaboration among multiple agencies.

With support from Innovation Norway, four of Norway's largest humanitarian organisations (Norwegian Red Cross, Save the Children Norway, Norwegian Refugee Council, Norwegian Church Aid) have come together to help tackle this challenge. To draft this RFP, we engaged an extensive public discussion on the key problem statements (see Appendix 1 - Detailed Problem Statements) related to dignified identities and particularly with regard to cash transfers in humanitarian contexts, and the potential technical ways to tackle them. The results of this engagement are available online,[3] and in Appendix 2 and 3 - Compiled Q&A from Information Sessions and Slides from Information Sessions.

We invite private companies, social enterprises, and other institutions to submit their proposals aimed at developing a minimum viable product (hereinafter, 'MVP') to be tested by the member institutions participating in this consortium in Kenya with an option to test in one more location depending on the outcome of the initial pilot.

[1] World Bank Group. 2016. Identification for Development. Strategic Framework. http://pubdocs.worldbank.org/en/21571460567481655/April-2016-ID4D-Strategic-RoadmapID4D.pdf

[2] World Disaster Report 2018: Leaving No One Behind https://media.ifrc.org/ifrc/world-disaster-report-2018/

[3] DIGID Documents. https://hiplatform.org/digid/

2. RFP Instructions

2.1. Submission of Proposals:

This RFP is based on the terms and conditions of Norwegian Red Cross' standard procurement procedures. Deadline for submitting a proposal to the RFP is **August 5th, 2019 - 12:00 hrs CEST**.

Vendors are allowed to submit clarifying questions to Norwegian Red Cross through the Mercell portal no later than **July 25th 2019 12:00 hrs CEST**. Please see the section on *Timeline & Milestones*. We will not be able to receive enquiries over the phone or other means except via the Mercell portal. All enquiries received will be collected and addressed through the Mercell portal to all RFP participants. Proposals addressed to different emails or location other than the Mercell portal will not be considered. Proposals submitted after the deadline, or do not comply with the requirements of the tender, or are incomplete will not be considered. The proposal and all correspondence and documents related to the proposal shall be written in plain English. The proposal must be signed and dated by the vendor.

At any time prior to the deadline for submission of proposals, the Norwegian Red Cross may amend the tender documents by issuing Addenda. Any Addendum thus issued shall be part of the tender documents and shall be communicated in writing through the Mercell portal to all Tenderers. Norwegian Red Cross retains the right to cancel the tender process before a contract has been signed in which case the terms and conditions of the contract are guiding.

Norwegian Red Cross reserves the right to ask vendors clarifying questions after the proposal submission deadline. The proposal must remain valid for up to three months after the submission of the proposal. Vendors who have engaged with the Norwegian Red Cross during the market dialogue shall be invited into the Mercell portal via email. The invitation to access the portal is only valid for the DIGID RFP, and cannot be used to access or bid for other tenders. The proposed solution strategy will be assessed against the functional and non-functional requirements team, company, quality of proposal, and the cost model (short and long term). Based on the assessment criteria, selected vendors will be invited into a negotiation phase. After the negotiations are complete, vendors will have the opportunity to submit a revised proposal upon which a final decision will be made.

The submission must include the following information about the vendor:

- Tax certificate for tax and VAT
- Certificate of Registration
- Signed copy of Norwegian Red Cross' procurement policy (Annex 3)
- Copy of vendor's annual report
- Information about vendor's key deliverables relevant to the proposal in past three years
- Confirmation that vendor satisfies the terms and conditions as stated in the Public Salary and Working Condition Policy (08 February, 2008, nr. 112)
- Norwegian Red Cross only accepts electronic invoices (EVF) and a minimum of 45 days to process the invoice.
- Proposal must fill in required sections outlined in the below sections.

2.2. Contents of the Proposal:

The proposal should include the following three parts and should be in the prescribed format.

PART A - Technical (max 20 pages in PDF)

The technical part of the proposal should be in PDF format and should include the following sections:

1. **Executive Summary** (2 pages max). Provide a brief overview of your understanding of the problem, summary of your approach to deliver the solution per the requirements, and financial summary.
2. Description of the proposed **approach, methodology, solution** to meet the requirements and processes described in the *Functional and Non-Functional Requirements* sections. Summarize what is already developed or out-of-the-box in your solution, and which ones will need to be developed or customized. Note to include the completed Appendix 4 Excel file as Annex to your proposal (See Part C Annexes).
3. Illustrate and briefly describe the **Technical Architecture design**. Provide a graphical representation of the technical architecture design identifying the components, how they interact (particularly with external systems such as NGO's internal systems or financial provider's system), and where they are located (on-premise in NGO, public/private cloud, private/public DLT, etc.). Please describe also the data flows particularly with the integration of various systems.
4. Describe the approach for **sustainability and scalability** of your solution assuming successful pilot implementation. Describe how your solution could expand to be used for other programming contexts. Please describe your business model and commercial ways of working with NGO users of your solution in the long term, and potential costs to beneficiaries.

5. Provide a summary of how your solution addresses the **data protection** considerations, ethics, and risks outlined your response. Please ensure to include the completed Appendix 4 Excel file as Annex to your proposal (See Part C Annexes).
6. **Project team**. Describe the members of the project team, roles, and include their CV's. Describe the work location, availability and percent dedication of the proposed team members to our project.
7. **High-level work plan** with breakdown of activities, time schedule, and outputs that are clearly linked to the information in the *Timeline and Milestones* section. Please present as a Gantt chart.

PART B - Financial (max 2 pages in PDF)

The financial part of the proposal shall be structured in the following sections and described in detail what is included in each of the costs and assumptions taken:

1. One-time implementation / setup cost of the full solution based on requirements
    a. Itemize and provide details of the costs (state assumptions)
    b. Describe if a development or staging (pre-production) environment is included with the production environment
2. Recurring monthly costs (e.g. license fee, hosting, support & maintenance, minor enhancements, etc.)
3. Program specific costs (e.g service fees based on transactions or volume of users or their activities where the solution is used)
4. Hardware (specific mobile devices, smartcards, printers, etc.)
5. Training (online training, in person train the trainers, and materials that will be produced)
6. Daily rates for consulting or custom development
7. Travel costs, if any

Note to include the completed Appendix 5 Excel file as Annex to your proposal (See Part C Annexes).

PART C - Annexes

1. Detailed response to the functional and non-functional requirements, and data protection questionnaire. Appendix 4 of this document is an Excel spreadsheet with three tabs: Functional Requirements, Non-functional Requirements, and Data Protection. All tabs should be duly completed and the updated excel spreadsheet should be attached in the proposal. Please do not add any new columns or change the format in the spreadsheet to allow us to easily evaluate the responses.
2. Updated Excel file for cost breakdown. Template can be found in Appendix 5. One tab needs to be duly completed.
3. Terms and Conditions. If you have an existing Terms of Conditions, please include as an Annex.

3. Timeline and Milestones

Date	Action
28 June 2019	RFP published in Mercell portal
4 July 2019	Deadline for vendors to ask clarifying questions
5 August 2019	Deadline to submit a proposal through Mercell
September 2019	Milestone 1 - design sprints with vendor and key project/pilot stakeholders
October 2019	Milestone 2 - controlled test and continued development
January 2020	Milestone 3 - Field test in Kenya
April 2020	TBC Milestone 4 - Field test location 2

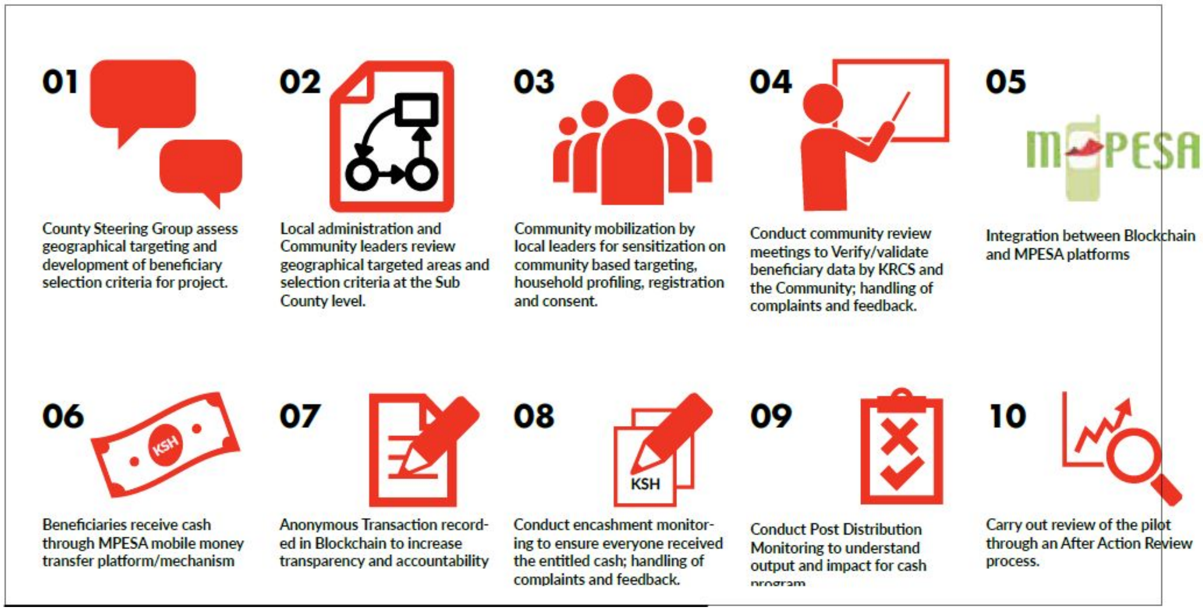
4. Pilot Context - Kenya

Kenya is one of the countries where all four members of the DIGID consortium operate and provide various forms of humanitarian assistance, in some cases in the same areas. In recent years, the country has been affected by severe drought and flooding. Kenya also hosts close to 500,000 refugees, including over 257,000 from Somalia and 115,000 from South Sudan (ACAPS). The repatriation of refugees from Kenya to Somali is ongoing.

The Kenya Red Cross Society (KRCS) is the largest humanitarian organization in Kenya, with presence across the country with 64 branches and sub branches supporting a network of 134,000 volunteers. KRCS has wide acceptance across the country with capacity to operate in areas considered hard to reach based on geographical isolation and limitations in humanitarian access. The society is designated as the first line of response in all sudden onset disasters by the Government and the Kenya Humanitarian Partnership Team (KHPT). It has an auxiliary role to both National and County Governments in Kenya. KRCS plays a key role in providing emergency services in health, WASH, camp management, protection, recovery and reconstruction. In partnership with the national and county governments, KRCS has been providing assistance to the affected through evacuation, search and rescue, distribution of non-food items provision of emergency health services, access to safe water and sanitation as well as cash disbursement to key affected populations. Kenya Red Cross Society estimates

25% of their beneficiary caseload do not have issued government ID's (World Disasters Report, 2018).

KRCS has a strong capacity for providing humanitarian cash assistance. During the Drought response between 2016-2018, over 70% of the assistance was provided through cash. Thanks to the widely used MPESA mobile money network and through partnerships with other financial service providers (FSP) such as local banks and network of money agents. On May 2018, KRCS in partnership with the International Federation of Red Cross and Red Crescent Societies (IFRC) has conducted a pilot on Blockchain and cash transfer using MPESA, which highlighted the needs and opportunities for digital ID's of affected communities. The figure below shows the general steps that KRCS usually takes in their cash transfer programming (CTP); the blockchain however was only used during the pilot.



01 County Steering Group assess geographical targeting and development of beneficiary selection criteria for project.

02 Local administration and Community leaders review geographical targeted areas and selection criteria at the Sub County level.

03 Community mobilization by local leaders for sensitization on community based targeting, household profiling, registration and consent.

04 Conduct community review meetings to Verify/validate beneficiary data by KRCS and the Community; handling of complaints and feedback.

05 Integration between Blockchain and MPESA platforms

06 Beneficiaries receive cash through MPESA mobile money transfer platform/mechanism

07 Anonymous Transaction recorded in Blockchain to increase transparency and accountability

08 Conduct encashment monitoring to ensure everyone received the entitled cash; handling of complaints and feedback.

09 Conduct Post Distribution Monitoring to understand output and impact for cash program

10 Carry out review of the pilot through an After Action Review process.

Figure 1: Steps involved in KRCS' cash transfer programming

Initial analysis has been conducted early this year to identify the key challenges related to identities. Figure 2 below is a high-level journey map based on a scenario of providing cash assistance to beneficiaries affected by natural disaster in rural areas. Figure 3, highlights the key challenges related to ID's for the various stakeholders involved in a cash program including the affected communities, the humanitarian organization, FSP's, and donors.

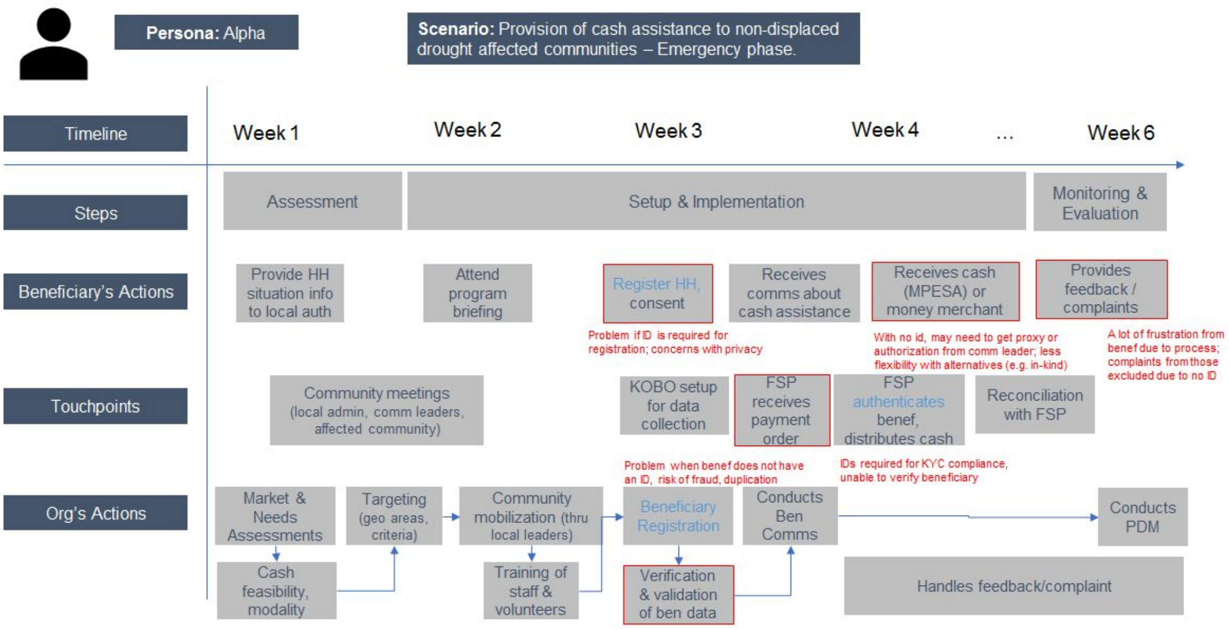

Persona: Alpha
Scenario: Provision of cash assistance to non-displaced drought affected communities – Emergency phase.
Timeline
Week 1
Week 2
Week 3
Week 4
...
Week 6
Steps
Assessment
Setup & Implementation
Monitoring & Evaluation
Beneficiary's Actions
Provide HH situation info to local auth
Attend program briefing
Register HH, consent
Receives comms about cash assistance
Receives cash (MPESA) or money merchant
Provides feedback / complaints
Problem if ID is required for registration; concerns with privacy
With no id, may need to get proxy or authorization from comm leader; less flexibility with alternatives (e.g. in-kind)
A lot of frustration from benef due to process; complaints from those excluded due to no ID
Touchpoints
Community meetings (local admin, comm leaders, affected community)
KOBO setup for data collection
FSP receives payment order
FSP authenticates benef, distributes cash
Reconciliation with FSP
Problem when benef does not have an ID, risk of fraud, duplication
IDs required for KYC compliance, unable to verify beneficiary
Org's Actions
Market & Needs Assessments
Cash feasibility, modality
Targeting (geo areas, criteria)
Community mobilization (thru local leaders)
Training of staff & volunteers
Beneficiary Registration
Verification & validation of ben data
Conducts Ben Comms
Conducts PDM
Handles feedback/complaint

Figure 2: User Journey Map showing the actors, process, and steps for a cash transfer programming.

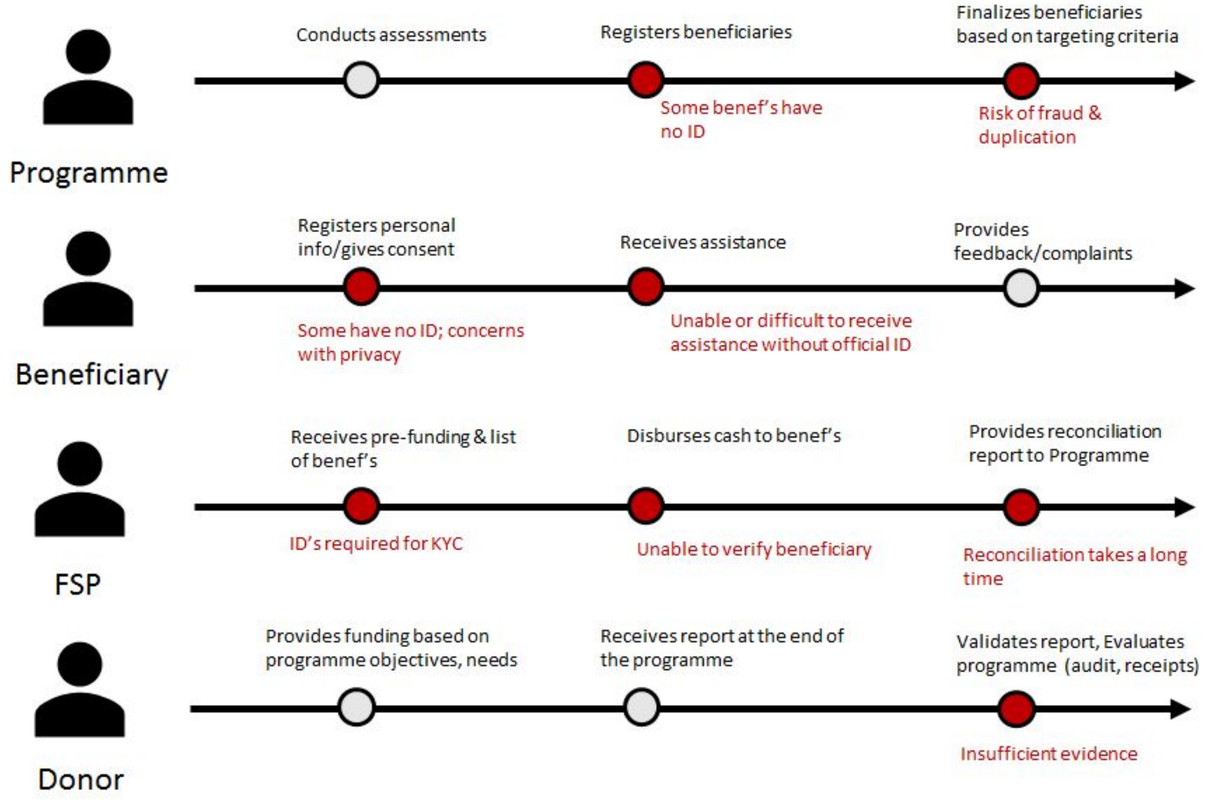

Programme
Conducts assessments
Registers beneficiaries
Finalizes beneficiaries based on targeting criteria
Some benef's have no ID
Risk of fraud & duplication
Beneficiary
Registers personal info/gives consent
Receives assistance
Provides feedback/complaints
Some have no ID; concerns with privacy
Unable or difficult to receive assistance without official ID
FSP
Receives pre-funding & list of benef's
Disburses cash to benef's
Provides reconciliation report to Programme
ID's required for KYC
Unable to verify beneficiary
Reconciliation takes a long time
Donor
Provides funding based on programme objectives, needs
Receives report at the end of the programme
Validates report, Evaluates programme (audit, receipts)
Insufficient evidence

Figure 3: Key challenges related to ID's for the various stakeholders

5. Functional Requirements

As described in *Section 4. Pilot Context* above, the cash transfer programming process involves the collection of beneficiaries' personal information by NGO's to plan the distribution, ensure targeting requirements are met, and to authenticate beneficiaries when redeeming their cash assistance. A payroll order is provided to a contracted FSP, which includes a subset of the beneficiary data to fulfil KYC requirements. Data is typically stored in internal data management systems or excel spreadsheets.

We envision an innovative solution that helps establish a digital version of identity-related credentials for beneficiaries, which they could use to avail humanitarian assistance including cash. Ideally, we envision beneficiaries having full autonomy and control over their data (self sovereign[4]). Furthermore, we envision such solution to allow interoperability with other NGO's to access and use such digital credentials, provided the beneficiaries give their consent.

Based on our learnings from the Information Sessions, the Concept Note bilateral meetings with vendors, and the preliminary consultation we conducted in Kenya, we understand that there are constraints to allowing full ownership and management of digital credentials by the beneficiaries themselves. Such constraints include the literacy level and access to technology that would enable this. It is foreseen that literacy levels and access to technology will improve over the coming years[5]. However, in the short term, we will need a solution that caters to today's reality, where our target population is the most vulnerable with low levels of literacy, and where we operate is in challenging environments where connectivity and power access are poor. We see that in the short term, a guardianship or custodianship model will be necessary, where beneficiaries entrust their personal data to be maintained by NGO's on beneficiaries' behalf.

In your proposal, we are keen to understand how your company or institution could help us build a solution that takes into account our future, ultimate vision of having more user-controlled and managed digital credentials, but where the current development will be focused on the minimum viable product (MVP) reflected in our Functional Requirements in Appendix 4 to address our needs today. Please also address the sustainability and scalability of your proposed solution.

Please see and complete Appendix 4: Functional Requirements and indicate how your solution addresses these requirements and if new development or customization is needed. Please include the updated Excel file in your proposal submission. We have indicated in the functional requirements, which ones are must-have for the pilot (thus referring to the MVP) and which ones are nice-to-have, to be considered as part of our ultimate vision or future implementation.

[4] http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

[5] https://www.gsma.com/r/mobileeconomy/

6. Non-Functional Requirements

The non-functional requirements in Appendix 4 are meant to ensure the solution will work in the operating environment we expect for our pilot location(s) and ensure a robust and flexible architecture that would address the evolving technologies and functionalities related to digital identities.

Please see and complete Appendix 4: Non-functional requirements and indicate how your solution addresses these requirements. Please include the updated Excel file in your proposal submission.

Some information to consider in your solution:

Operating environment:
Certain processes may need to be conducted in offline or low-connectivity areas where power supply may also be limited. Such processes include beneficiary registration, where currently KRCS is using Kobo/ODK mobile data collection to collect beneficiary data in the field. At the end of the registration, volunteers and staff have to establish a connection to the internet through mobile hotspots or by taking the mobile devices to a location that has internet access to upload the data. Distribution of cash assistance may also happen in offline or low-connectivity environments (e.g. where mobile money is not feasible). Or sometimes, the beneficiaries may live in areas with no network connection but may travel to an area with network to use their phone.

It is possible to bring a satellite phone or portable internet in areas where connectivity is absolutely necessary during a field visit, but costs will need to be considered for sustainability and scalability. Power generators are sometimes brought in areas where electricity is necessary as well, but also for short periods of time.

Access to mobile phones & Literacy:
Not all beneficiaries have mobile phones. Some rely on family members, neighbors, or friends to have access to phones. To own a mobile phone and mobile money MPESA account, an official ID is necessary.

Those who have access to phones tend to have good literacy levels, even just to be able to send simple text messages. Those who are not literate rely again on family members or neighbors.

We do not assume people in our target communities to have smartphones. We do assume that a majority of them are able to use feature phones and can interact using Unstructured

Supplementary Service Data (USSD) used to send text between a mobile phone and an application program in the network.

Payment Mechanisms:
Mobile money through MPESA is one of the common ways in which KRCS provides cash assistance. Those without a mobile phone have to designate a proxy or a person with a mobile phone and MPESA account, to receive their cash assistance on their behalf.

Where mobile money is not possible, KRCS will contract money vendors to go to a predetermined location near the affected communities and distribute cash directly to beneficiaries. Here, there's no need to have a mobile phone, however sometimes it is a challenge to authenticate the individuals either because they have no official ID, their ID's are not legible because it is damaged or too old to read, or it is difficult to check the person against their paper ID's. In this case, KRCS have used biometrics to help with the authentication of the beneficiaries.

Internal systems:
KRCS uses ODK/Kobo to collect and store beneficiary registration and survey data. They also use different data management solutions such as RedRose[6] to manage beneficiary and distribution data for programming purposes. For payment mechanism, there's an integration with Safaricom's MPESA mobile money services. The solution should consider how to integrate with these various internal systems, which store and process beneficiary data. Such systems could also vary depending on the NGO. For example, an NGO may use LMMS or Salesforce or even a custom developed application for data management.

Security:
Data security is critical to ensure the protection of data we collect from our beneficiaries as well as data we process to provide, track, and monitor humanitarian assistance. End-to-end security of data should be considered from the moment they are collected using mobile phones to upload and storage on servers and data rendered in applications. We would like to understand the vendor's approach to ensure end-to-end security of data including the use of encryption and other privacy enhancing methods particularly when dealing with beneficiary personal information and transactions.

Support and Maintenance:
Support and Maintenance is critical for any IT system particularly for new technologies being rolled out. We would like to understand what models will be available for both the pilot and future deployments and what are the Service Level Agreement (SLA) considerations.

Interoperability and Standards:

[6] http://redrosecps.com/.

We assume different humanitarian organizations may opt for different digital ID solutions but are able to read, recognize, and use digital credentials issued by another humanitarian organization. This level of interoperability is what we would expect for the solution to provide versus a siloed approach that caters to a specific organization. We see that this is possible with agreed standards. We would like to understand how your solution takes interoperability and standards. For the pilot we assume the DIGID partner organizations deploy the same solution and be able to see how to interact with the digital credentials issued for their beneficiaries.

ID2020:

We acknowledge the work of ID2020[7] on how a *Good Identity* should be designed: "A good identity should be portable, persistent, private and personally controlled". ID2020 published a technical requirements to be considered for Good Identity: https://id2020.org/uploads/files/ID2020-TAC-Requirements-v1.01.pdf. We would like to understand how much of the vendor solution meets or addresses those technical requirements. We have taken an excerpt of key requirements from the ID2020 Technical Requirements in our non-functional requirements. At minimum, we'd like to understand how your solution addresses those specific requirements.

7. Data Protection

As referred to in the User Journey map, the collection of personal information is part of the setup and implementation process of a cash transfer program. Such information is used to authenticate beneficiaries when claiming cash assistance. FSP's also use this information to comply with KYC requirements and other regulations. Protecting all collected personal information is paramount in our response. The following are key questions related to data protection and data security. Please complete Appendix 4: Data Protection questionnaire tab and include it in your proposal submission.

8. Cost

We would like to understand the cost factors to develop the MVP based on our functional and non-functional requirements for the pilot, as well as the cost considerations for future deployments keeping in mind the financial sustainability and scalability of the solution. Please complete Appendix 5 and include it in your proposal submission.

[7] https://id2020.org/

10. Appendices

- Appendix 1 - Detailed Problem Statement
- Appendix 2 - Consolidated Q&A from DIGID Information Sessions
- Appendix 3 - Slides from DIGID Information Sessions
- Appendix 4 - Excel spreadsheet with Functional & Non-functional Requirements & Data Protection questionnaire: TO BE COMPLETED BY VENDOR and included in the proposal as Excel file.
- Appendix 5 - Excel spreadsheet with costing breakdown. TO BE COMPLETED BY VENDOR and included in the proposal as Excel file.