Set-Up Guide:
DIGID Platform

June, 2021

Supported by:

Table of Contents

Introduction

The Dignified Identities (DIGID) in cash programing project aims to address the issue of lack of official or recognized identity for recipients of humanitarian cash assistance.

As part of the project, an open source digital identity platform, i.e. the DIGID Platform, was built based on decentralized identity technology that is inclusive and easily integratable by different humanitarian organisations. It was first tested in a controlled environment, followed by field testing within the framework of a cash transfer programme in Nairobi and Turkana in Kenya in April 2021.

This document serves as a guide on setting up and using the DIGID Platform for NGOs and other organisations interested in adopting it for their own cash programing operations.

It consists of 3 Sections as follows:

- **Section 1: DIGID Platform Overview**, in which the platform's main functions, users, features and flows are explained,
- **Section 2: Technical Architecture,** which details the DIGID Platform's technical ecosystem and components, along with data privacy and protection standards, and
- **Section 3: Considerations for Deployment**, which provides different options regarding the technical set up and management of the platform for NGOs (and other organisations) that wish to adapt the DIGID Platform to their respective contexts.

I. DIGID Platform Overview

1.1 Functionalities

The DIGID Platform can be used to:

1. Create digital identity wallet

Beneficiaries can create their own digital identity wallets by signing up via a Progressive Web App (App from here onwards) if they have a smartphone, or via a USSD Menu if they have a basic/feature phone. In case a beneficiary doesn't have a phone, an NGO can create a beneficiary's digital identity on their behalf.

2. Issue credentials related to beneficiary identity and other attributes

NGOs and other organisations can upload relevant beneficiary data to the DIGID Platform. This data is encrypted and digitally signed to create a credential. The digital signature helps verify the authenticity and origin of the data accompanying it.

3. Request credentials

Organisations such as Financial Service Providers (FSPs), other NGOs and organisations delivering assistance and services can use the platform to request beneficiaries' credentials to authenticate them.

4. Share credentials (authentication)

Beneficiaries can share credentials that have been requested by an organisation by giving their consent and authenticating themselves via a PIN or other means including biometrics.

5. Manage digital identity

Beneficiaries can view their own credentials to see the data that an NGO has collected about them. They can also request updates to outdated and/or erroneous credentials and permanently delete them. Beneficiaries can also recover their digital identity and corresponding credentials in case they lose or forget the means to access it.

1.2 Users

The DIGID Platform is designed to suit the needs of several different types of users (see DIGID User Consultation Report for more information). Currently, the platform serves 3 main user types (see Table 1: Users of the DIGID Platform below) specific to the cash programing scenario.

However, in future, other organisations may also leverage the platform to provide services beyond cash programing and humanitarian assistance.

Table 1: Users of the DIGID Platform

User Type	Actions	Notes
Beneficiary (Smartphone, Basic Phone, No Phone)*	• Create digital identity • Manage digital identity • Share data/Authenticate using digital identity	Beneficiaries with smartphones can create their own digital identity by signing up to the platform themselves.
NGO/ Humanitarian organisation	• Issue credentials • Request credentials • Create and manage digital identity on behalf of beneficiary	NGOs serve as issuers of data which is requested by organisations such as FSPs. However, they can also request credentials. For example NGO A can request credentials issued by NGO B.
Financial Service Provider (FSP)	• Request credentials	Both money vendors and mobile money/digital cash providers can use the DIGID Platform, making it suitable for different scenarios.

	• Issue credentials	FSPs are currently envisioned as requesting data to authenticate beneficiaries for cash disbursement. However, they may also issue credentials, for example confirming cash disbursement to a certain beneficiary.

** Currently, self-sovereign beneficiaries who have signed up to the DIGID Platform as a smartphone beneficiary are **not able to switch** to using the platform as guarded beneficiaries (i.e. those with basic/feature phones and no phones), and vice versa.*

1.3 Interfaces

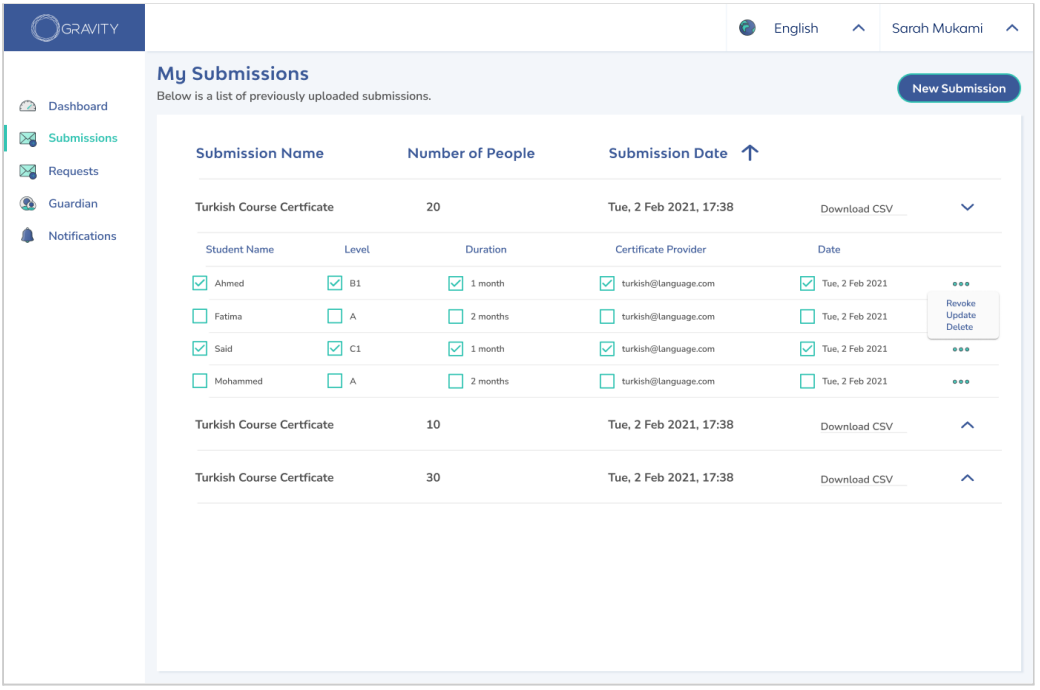
The DIGID Platform is accessible via different interfaces tailored to meet the needs and requirements of various user types.

Portal

Description: An interface made for organizations (NGOs, FSPs and others) to submit and request data about users. It also comes with a set of features which help organizations manage the users they are guardians of.

Users: NGO, FSP and any other organization issuing and requesting credentials.

Accessibility: The Portal can be accessed through a web browser on a desktop/laptop with an internet connection.



A snapshot of the Portal for organizations issuing credentials

System Requirements: The Portal is accessible via the following web browsers: Chromium (Chrome, Edge Insider), Firefox, Safari 10+, IE11/Safari 9.

Alternative: Organizations can also choose to use a Beneficiary Management Systems (BMS) that they are already using or another third party interface to issue and request credentials. This would require an integration with the DIGID Platform. See Section 3: Considerations for Deployment for more details.

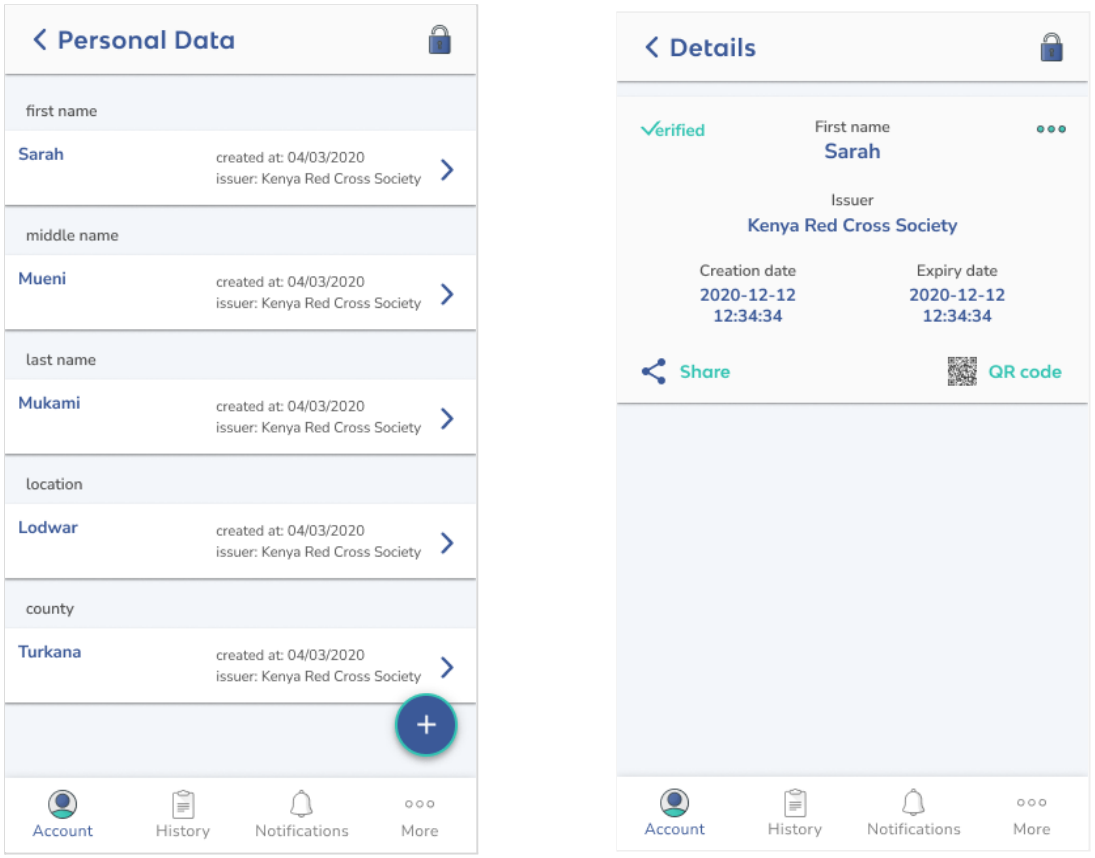
This was the case for the DIGID project with the Kenya Red Cross Society, during which the RedRose BMS was used for credential issuance. This adaptability allows for adoption of the DIGID Platform without disruptions in NGO's existing beneficiary management systems and processes.

Progressive Web Application ("App")

Description: An interface used by beneficiaries of assistance that have smartphones to create their digital identity, share credentials/authenticate and manage their digital identity (update, dispute and delete credentials). NGOs and FSPs can also use the PWA to scan and read QR codes containing digital identity credentials.

Users: Beneficiaries with smartphones, NGO field staff

Accessibility: The App currently requires mobile data/internet connectivity to use, but offline mode will be available shortly (see Appendix: Product Roadmap).



A beneficiary's view of their digital identity credentials on the App

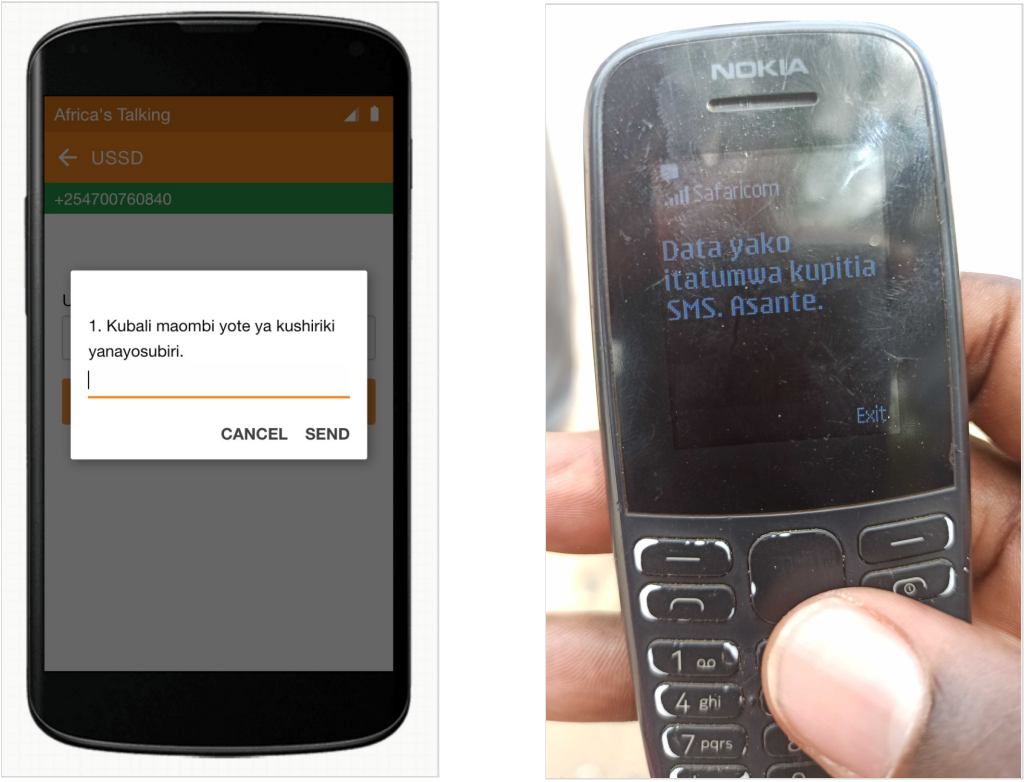
System requirements: The App is accessible on the following mobile browser versions: Android Browser +2.1, Blackberry +7, Chrome +23, Chrome for Android +32, Firefox +18, Firefox for Android +25, Firefox OS +1.0, Opera 15 (Opera 10.5+ with localStorage), Opera Mobile 11, Phonegap/Apache Cordova 1.2.0, Safari 3.1 (includes Mobile Safari).

USSD Menu

Description: A USSD interface accessible by dialing a dedicated shortcode. Beneficiaries with a basic phone can use this USSD interface to view, request, share and manage their digital identity credentials. Beneficiaries are required to authenticate using a 4 digit PIN to use the USSD menu and interact with their DIGID digital identity.

Users: Beneficiaries of assistance with a basic/feature phone

Accessibility: The USSD menu is accessible by dialing a shortcode on a basic/feature phone. It requires mobile/cellular network coverage to be used.



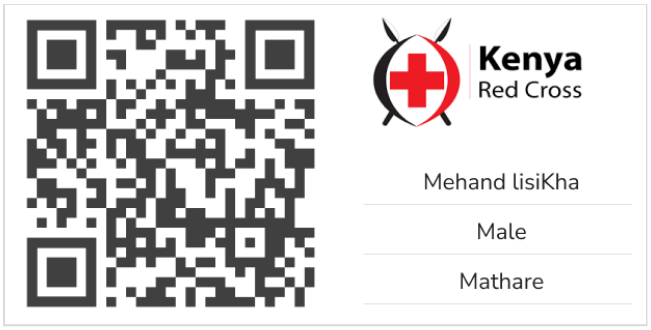
Sharing credentials through the DIGID USSD menu

QR Code Cards

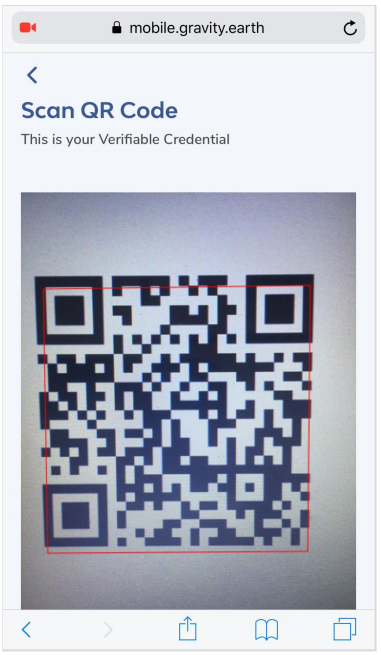
Description: A QR code which contains a link to the beneficiary's digital identity credentials. It is generated on the Portal by the guardian organization, printed and then distributed to beneficiaries without a device. Organizations that wish to request data from such beneficiaries can scan this QR code using the App to view beneficiaries' digital identity credentials.

Accessibility: Beneficiaries do not need to have any type of device to use these QR codes. Mobile data/internet connectivity is currently required to scan and read the QR codes. The possibility to do this offline will be available shortly (see Appendix: Product Roadmap).

Users: Beneficiaries without a device.



Digital identity QR code



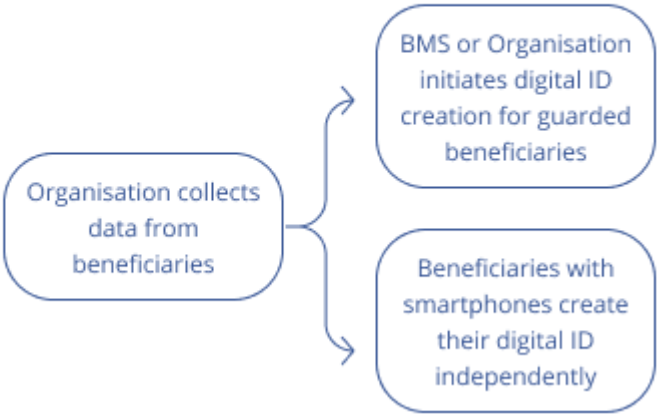
QR code scanner on the App

1.4 Sample DIGID Platform process flows

The DIGID Platform can be used across different cash programing contexts, for example in terms of different modalities of cash distribution: mobile money, money vendor or even in kind distribution. **The following section thus provides an example of how the DIGID Platform can be used in the scenario for cash distribution with a money vendor**. This was the case for the field testing in Kenya with the Kenya Red Cross Society.

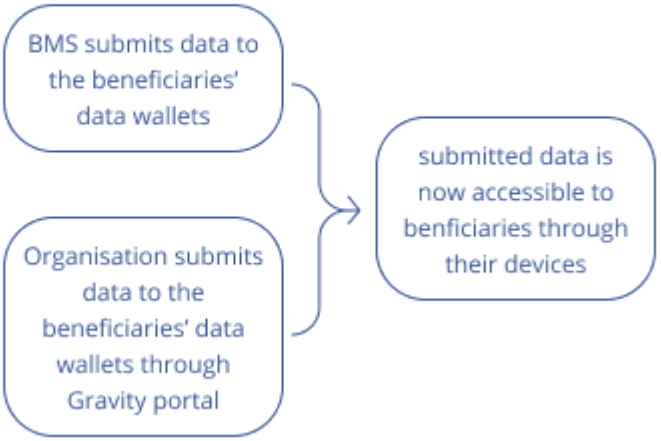
Digital ID Creation

The creation of the digital identity is either initiated by a BMS integrated with the DIGID platform or through the portal. Beneficiaries with smartphones can create their own digital identity by signing up to the App.



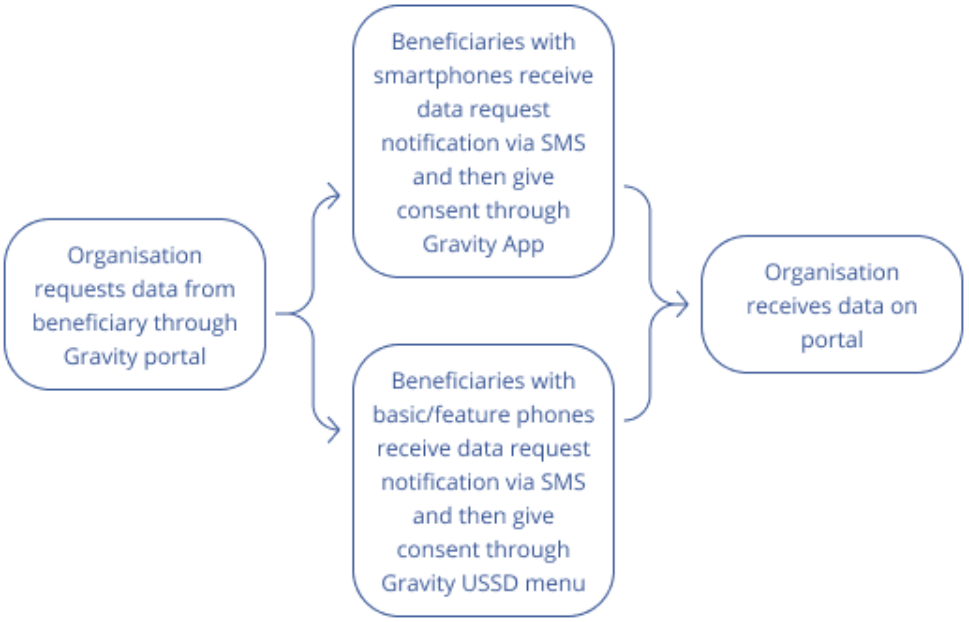
Credential Issuance

Credentials are issued either via the BMS or the portal. After submission the data can be accessed by the beneficiaries through their devices. Beneficiaries with smartphones view their data by logging into the App. Beneficiaries with basic or feature phones can request to view their data through the USSD menu and receive a summary of the credentials via SMS.



Sharing credentials (authentication) remotely

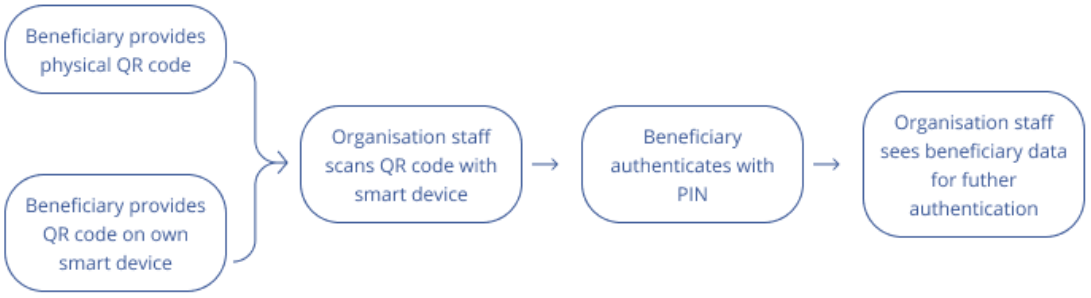
Remote sharing of credentials is initiated by the organisation that can request specific credentials from beneficiaries using the portal. Beneficiaries with smartphones receive an SMS with the data request notification and are redirected to the App where they can give consent with one click. Beneficiaires with basic or feature phones also receive a data request notification via SMS and then navigate to the USSD menu to give consent. Once consent to the data request has been given the organisation can view the requested data points on the portal.



Sharing credentials (authentication) in person

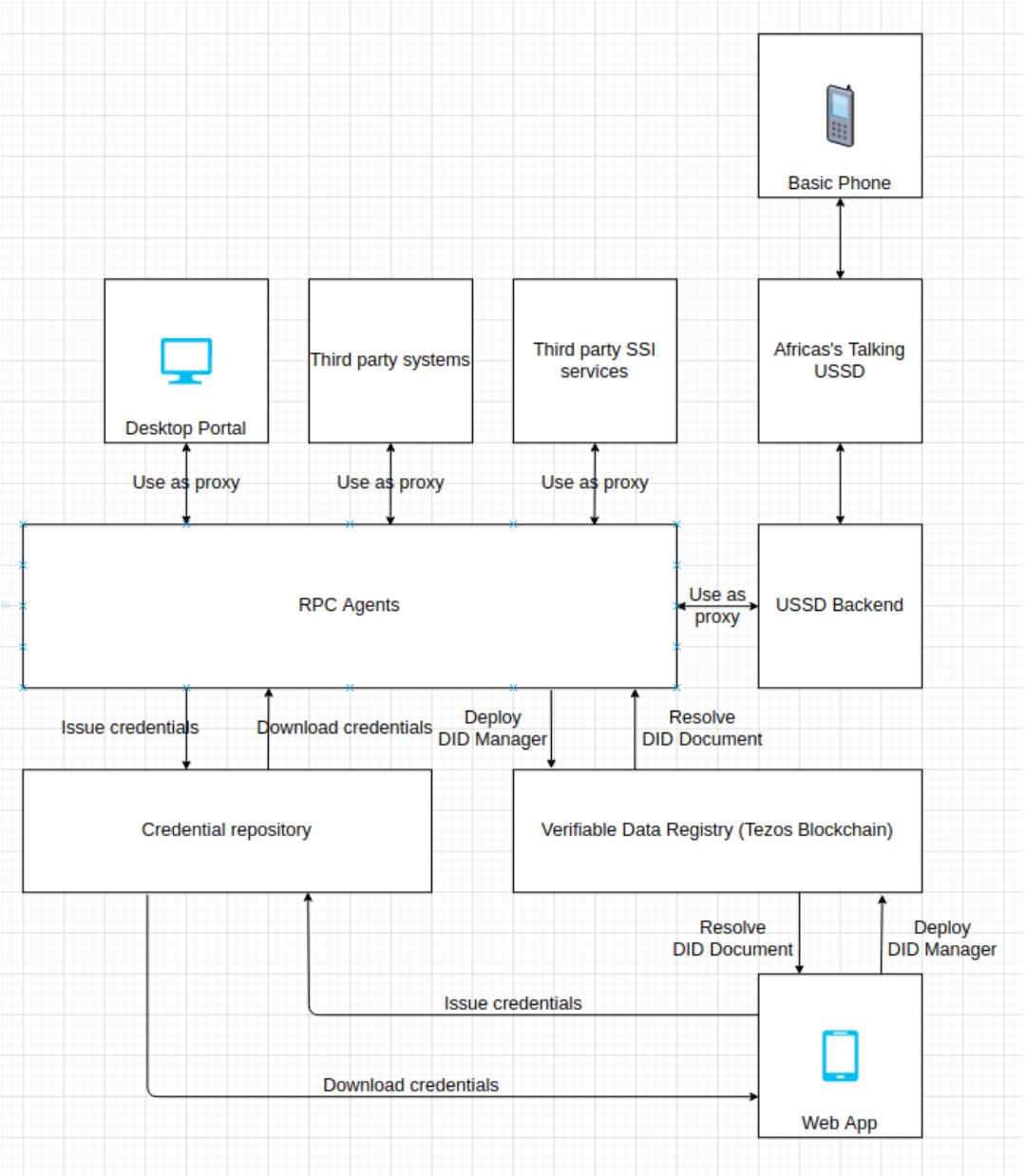
Sharing credentials in person is useful in the field during programme activities where beneficiary data is required and to authenticate the beneficiary. The organisation must have generated physical QR codes for beneficiaries with basic/feature phones or no phones prior to the activity. Beneficiaries with smartphones can generate their QR code on their own smart device.

The beneficiary displays the physical or digital QR code so the organisation staff is able to scan it with a smart device. Next, the beneficiary is prompted to type in their PIN on the organisation's smart device. After successful authentication the organisation staff is able to view the beneficiary data on the organisation's smart device.



II. Technical Architecture and Deployment

2.1 High Level Technical Architecture



High level architecture of the DIGID Platform

2.2 Roles

Users have different roles designated to them within the DIGID Platform. Each role corresponds to specific actions which can be performed. It is important to note that an entity can have multiple roles if needed and depending on the context. For example, an NGO can be both an issuer and a verifier depending on the purpose they want to fulfil.

Table 2: Roles within the DIGID ecosystem

Role	Definition	Example *(by DIGID User Type in Table 1)*
Issuer	An entity that asserts claims about one or more subjects, creating a verifiable credential from these claims, and transmitting the verifiable credential to a holder.	NGO
Guardian	For self-sovereign identity (SSI) to be truly inclusive, individuals who do not have digital access, or the appropriate capacity for access, will need another person or organisation to serve as their digital guardian (an entity). The guardian is responsible for helping the beneficiary to create and manage their digital identity wallet.	NGO
Verifier	An entity which receives one or more verifiable credentials, optionally inside a verifiable presentation, for processing.	Financial Service Provider
Data subject	An entity about which claims are made. Example subjects include human beings, animals and things. In many cases the holder of a verifiable credential is the subject, but in certain cases it is not. For example, a parent (the holder) might hold the verifiable credentials of a child (the subject).	Beneficiary

For more information regarding the above roles and their definitions, please consult the Gravity Glossary.

2.3 Ecosystem Components

Table 3: Components of the DIGID Ecosystem

Component	Description	Status
Backend Layer		
Core Package	The Gravity Core Package is a javascript implementation of the W3C DecentralizedIdentity and VerifiableCredential standards. This allows the creation of very low level components including W3C VerifiableCredentials, VerifiablePresentations and DID Documents, and provides cryptographic encryption and signature algorithms.	Open Source
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 API reachable via the public network (https requests). Each party able to host such	Open source

	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.	
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
Software Development Kit (SDK)	The SDK is a library developed by Gravity, running on the background of the PWA or the Gravity agent. It uses the core package in order to create low level 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
Frontend Layer		
USSD Application	Basic phone users will interact with the solution via a USSD menu interface which relies on a PIN code for authentication. Basic phone users will therefore be able to perform consent & share, update & delete, view & verify operations as per requirements.	Open Source
Progressive WebApp (PWA)	The App is accessible via smartphone and web browser. Smartphone users have the ability to encrypt and sign credentials and consents directly on their phone. The App retrieves the received credentials from the Gravity credential repository. It receives presentation requests directly from relying parties, resulting in the credential being shared on to the requester's RPC Agent.	Proprietary
Portal	An existing BMS 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

2.4 Technical deployment through the RPC Agent

Organizations willing to take a role of issuer, guardian or verifier on the DIGID platform must have access to an RPC Agent. Such an Agent is contained on a Docker

image and can either be automatically deployed on a remote machine or manually installed by the said organization as detailed below:

Option 1: Automatic deployment

The easiest option for an organization to be part of the DIGID ecosystem is to get an RPC Agent automatically deployed by Gravity on a remote host it controls. This deployment is possible thanks to an IT automation tool that uses SSH to access any remote hosts, and injects Python scripts in order to execute complex operations on it. For this to work it is necessary to have on the remote host:

- **A running SSH server:** The access modalities and credentials of the SSH server must be communicated with Gravity. Organizations not willing to share this information or even expose an SSH server must use the "Manual installation" option described below.
- **A Python interpreter:** Supported versions are v2 (must be v2.5+) and v3 (must be v3.6+).

Option 2: Manual installation

It is also possible for organizations to manually download and install an instance of RPC Agent without having to expose an SSH server. In this scenario, organizations need to be sure Docker is present on the machine in order to run it.

In both cases, the installed Agent is only capable of receiving requests coming from the local network and doesn't come neither with an SSL nor a Cross-Origin configuration. This is then the responsibility of the organization to make its Agent publicly available via a firewall or a reverse proxy, as well as setting up the desired configurations regarding SSL, Cross-Origin or request filtering.

For both option, technical support can be requested at : contact@gravity.earth

2.5 Data Privacy & Protection

The DIGID project relies on a decentralized identity ecosystem. That ecosystem is built on top of 2 decentralized storages:

- **Verifiable Data Registry** that stores public information,
- **Credential Repository** that stores the private credentials.

Verifiable Data Registry (Tezos Blockchain)

In order 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 listed below.

Authentication

Blockchain technology relies on transactions that are cryptographically signed. It involves that operations senders on the registry can be natively authentified, ensuring only allowed entities can perform those operations.

No central control

The Decentralized Identity standard recommends the use of public and decentralized registries. This is to avoid vendor-lock, single point of failure and censorship while giving entities the opportunity to control and manage their own identities without needing external authorities. Public blockchains provide mainnet instances that fulfill the requirements with thousands of independent nodes, making attacks to take over the registry (51% attacks) impossible.

Security

Blockchain is powered by cryptography at a very deep level, namely elliptic curve cryptography. This algebraic approach results in fast and 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 synchronised when they are up again, preventing any loss of data.

Note on personal data storage and the blockchain

The following data is stored on the blockchain:

- **Authentication public key:** Used by remote parties verify a signature with an "authentication" purpose (in W3C terms), most frequently used during the sharing of credentials,
- **AssertionMethod public key:** Also for use by remote parties to verify signatures with an "assertionMethod" purpose (in W3C terms), usually used during credential issuance,
- **KeyAgreement public key:** Used by remote parties to compute the shared secret necessary for end to end encryption,
- **Link to the credential repository:** A link to a dedicated space on the credential repository which allows issuers to know where to send credentials post encryption, and
- **TZIP-16:** Standard that helps attach off-chain metadata to the DID manager, allowing for the inclusion of metadata views.

This means that no personal data/personally identifiable information is stored on the blockchain, upholding beneficiaries' Right to be Forgotten and safeguarding their privacy.

Credential Repository

The credential repository is a decentralized storage vault that stores beneficiaries' credentials. The credential repository offers a high degree of protection for beneficiaries' data through:

Authentication

Nodes on the repository come with a cryptographic authentication mechanism using the same verification keys stored on-chain. This way, the authentication to access this vault storage is as strong as the native Blockchain authentication.

Encryption

The repository only deals with encrypted data. This is the role of the issuer (resp. data subject) software to perform data encryption (resp. decryption), resulting in an end-to-end encryption.

In addition to that, the underlying technology itself comes with a native encryption layer so even a malicious nodes of the repository can't read the data stored

Redundant Array of Independent Disks (RAID)

The internal storing mechanism, namely RAID, splits the encrypted data across the multiple nodes and ensures redundancy. This way, even in the unlikely case of several nodes getting attacked, damaged or lost, users' information remains safe. Lastly, a reparation protocol is executable in order to reconstitute data.

This splitting algorithm along with the native encryption guarantees that nodes part of the credential repository only possess a few pieces of encrypted information and therefore are unable to read the data itself.

Location of data

In order to store sensitive data from the beneficiaries, the **Credential Repository should ideally avoid** international transfers (as recommended by the DIGID Data Protection Impact Assessment). To do so, a private cloud decentralized storage is used and its belonging nodes were set up exclusively in Kenya for the DIGID project, in compliance with the Kenya Data Protection Regulation. **In future, organizations may continue to use the storage nodes in Kenya or decide to have one in their country of operation.**

Because of the underlying technology being public Blockchain, the **Verifiable Data Registry** has storage nodes across the world and therefore international transfers can not be avoided. However, this does not concern personal data as mentioned above in the section "Note on personal data storage and the blockchain".

III. Considerations for deployment

3. 1 How does the DIGID Platform interact with existing Beneficiary Management Systems (BMS) ?

One of the principal objectives of the DIGID project has been to decouple identity management from beneficiary management systems. For this reason the DIGID Platform has been developed in a manner which complements beneficiary management systems and processes rather than disrupting them. NGOs can therefore choose how they want their existing BMS to interact with the DIGID Platform:

Option 1: Integrate existing BMS with DIGID Platform

This was the case for the DIGID field testing in Kenya, where an integration between RedRose and Gravity took place. Data collection for the cash transfer program was

conducted through RedRose. Once data had been cleaned and additional checks on beneficiary eligibility made, digital identity wallet creation and credential issuance was triggered.

This option implies using the BMS as a frontend for digital identity wallet creation and credential issuance, rather than the Portal. Organizations that prefer using only one interface to manage cash programing and digital identity processes may choose this approach.

Option 2: Keep BMS and DIGID Platform separate

Organizations that would like to keep the BMS and DIGID Platform distinct, or do not want to integrate or do not have a BMS can use the DIGID Portal as the main interface. Organizations may input beneficiary data to the DIGID Portal or upload a CSV file to issue credentials. The Portal can also be used to request credentials and perform digital identity management functions such as revoking and updating credentials, account recovery for guarded beneficiaries and generating QR codes.

3.2 What does an organization need to do to ensure the technical deployment of the DIGID Platform ?

The decentralized identity ecosystem accepts multiple organizations as issuers. Those organizations may or may not need a third party such as RedRose as a data provider.

Each organization would have to host an instance of the Agent from where they have to issue credentials about their beneficiaries. Such an Agent is contained on a Docker image and can either be automatically deployed on a remote machine or manually installed by the said organization as detailed in 2.4 Deploying the RPC Agent.

Optionally a data provider such as a BMS like RedRose needs to initialize the credentials with the said data on the Agent of the NGO. In that context, the associated NGO needs to trigger the issuance of the credentials previously initiated by the data provider.

Agents hosted by NGOs also serve as a Guardian for beneficiaries relying on guardianship. NGOs are in charge of creating digital wallets for their guarded beneficiaries.

3.3 What mechanisms for beneficiary authentication are possible with the DIGID Platform ?

For the DIGID project in Kenya, beneficiaries authenticated themselves with a 4 digit PIN to receive cash disbursements. The choice of PIN as the authentication mechanism was due to various reasons, such as its **ease of use for beneficiaries (see DIGID User Consultation Report) and interoperability with NGOs not using biometrics.**

However, other authentication mechanisms such as biometrics can also be introduced for increased levels of security. Organizations should decide on the authentication mechanism based on their relative advantages and disadvantages to a

particular context depending on the level of security required, beneficiary literacy levels and connectivity requirements.

Interactive Voice Response (IVR) which allows users to authenticate using their voice will also be introduced to the platform following feedback from the user consultations and field testing in Kenya.

Table 4: Authentication mechanisms for the DIGID Platform

	Ease of use	Low connectivity	Security	Literacy	Other
PIN	A simple combination of 4 digits is easy to remember and type, but low literacy can cause problems.	Entering a PIN is possible as long as the phone comes with a text messaging functionality, meaning it is suited for beneficiaries basic/feature phones.	Without extra security features, cracking a PIN is only a matter of time. Beneficiaries that struggle to set/recall a PIN may have to write it down somewhere in which case it is important to keep the PIN safe.	Beneficiaires with low literacy may struggle to set a PIN and remember it.	Modifiability: Can be reset in case it is forgotten or compromised.
Voice (IVR)	Easy for beneficiaries since it relies on processes they are already used to such as calling.	Possible on basic/feature phones and without internet connectivity.	Higher level of security compared to PIN.	Suitable for low literacy contexts.	Not ideal in a noisy environment, or in case of voice loss which may prevent authentication.

Other means of authentication, whether biometric or other such as pattern-based, are also under consideration and may be integrated to the DIGID Platform depending on the needs of both organizations and beneficiaries.

3.4 How are staff access and rights to the DIGID Platform managed ?

Since the DIGID Platform allows organizations access to sensitive beneficiary data through the Portal, it is important to consider the different permissions and rights that organizations' staff will be given. **Designating staff access and authorization to the platform should be determined by individual organizational policy and the purpose for which different staff members may need access to the Portal depending on their role.**

Currently, a technical feature for staff rights management has not been implemented. In the absence of such a feature, organizations should clearly outline and agree on which staff members should be able to log in to the Portal and perform which functions.

In the coming months, a feature to designate staff access and rights to the Portal will become available (see Appendix: Product Roadmap). This will **involve authenticating staff members to access the Portal** so that a staff member is able to perform only those functions allowed by an administrator.

This authentication layer uses a Directory System Agent (DSA) under the hood in order to atomically and natively restrict low level operations, such as user creation, deletion or right management, to user agents by using Access Control Lists (ACLs). **In addition to that, users are assigned business groups to limit access to high level functionalities such as:**

- Creating digital identity wallets for Guarded beneficiaries,
- Issuing credentials,
- Requesting credentials, and
- Managing digital identity in terms of revoking and updating credentials, and account recovery.

Appendix

1. Product Roadmap

The following features will be made available on the DIGID Platform in the upcoming months.

Feature	Description
Authentication via Interactive Voice Response	Beneficiaries will be able to authenticate themselves with their voice. This will be especially useful for guarded beneficiaries with a basic/feature phone, particularly in contexts with low literacy in which beneficiaries have difficulties managing a 4 digit PIN.
App (PWA) offline mode	This will allow certain actions to be run without mobile data/internet connectivity, such as scanning beneficiary QR codes.
Authentication API	This will allow authenticating staff members to access the Portal so that a staff member is able to perform only those functions allowed by an administrator. This authentication layer uses a Directory System Agent (DSA) under the hood in order to atomically and natively restrict low level operations, such as user creation, deletion or right management, to user agents by using Access Control Lists (ACLs).
Admin. Dashboard	A dashboard accessible through the Portal which allows an organization's System administrator to gather metrics regarding identities created by the NGO. E.g. number of new beneficiary digital IDs created, deleted, updated.

2. Further documentation

Kenya User Consultation Report (December 2020)

Executive Summary on DIGID project

Gravity Glossary

Gravity Digital ID API Documentation

3. About Gravity

Gravity's digital identity solutions empower individuals at the bottom of the pyramid to build trusted digital identities that are private, portable and persistent. Gravity's cloud platform allows individuals and small businesses ("beneficiaries") who lack legal forms of identity to bring together verifiable data about themselves into a digital wallet. With this secure digital wallet, Gravity users can safely share this data with

organisations to access key services including humanitarian aid, financing and educational resources to accelerate their path towards financial inclusion.

Gravity is a trusted, human-centered company with a dedicated and diverse team based in Nairobi, Kenya and Paris, France. We believe that having a diverse staff based directly in the communities we work with is key to ensuring that our digital identity solutions meet the needs of the individuals and organizations we support.

Contact

For a demo or to learn more about the DIGID Platform and how it can be set up and customised to your needs, **please visit www.gravity.earth or directly reach out to us at contact@gravity.earth.**