Options for inclusive Digital Wallets

Ideas for inclusive public attention
Decentralized forms of wallets

Jaume Dubois, January 2023, updated October 2026



Version en Français disponible ici

Types of applications

Types of application vary with the end objective; the service approach depends on the sensitivity of the use case. The following are examples of public applications.

Registration	On-board a person into the system to access further services. Requires strong identity check, providing evidences and face to face attention or liveness control.
Access control	Verify a person identity before giving physical or digital access. Can use one or more modalities: what I am (biometrics), what I know (PIN, password), what I own (card, token, phone/OTP)
Status control	Verify status of person to maintain access to services. Can start by a liveness or presence control or collecting data on current person situation and re-assessing access to services.
Identity check	For investigation purpose, most often in criminal case. Controlling identity of an individual, very often based on physical document now moving to digital form of ID or use of biometrics.
Digital Signature	To attest agreement on a transaction, on contract, on a subscription or to confirm authenticity of a set of data or a document. Requires a system equipped with a secure element.
Application to program or services	Authenticate and fill-in a form to provide elements and associated evidences for subscribing to a program or a service. Whether as a citizen or as a customer, identification matters: it must be your legal identity for public services, and it must be linked to a trusted means of payment for paid services.
Application for services	Apply for something and get a certificate of it (e.g. diploma, training certificate, medical exam), requiring an identity verification of some kind (any modality is possible starting from ID document visual control)
Goods or cash collection	Being eligible to receive goods or cash, present evidence of this right or of identity if being part of a predefined list of person. Identification also confirms that the good has been delivered to the right person.

Introduction

We consider verifiable credentials to be a future interoperable trusted dataset which will facilitate interactions in a trusted way.

They will be easy to issue and verify with a smartphone, but not everybody has access to such devices or to network connectivity.

The objective of this study is to figure out how to leverage them while limiting the exclusion of part of the population.

For this purpose, we have studied the different contexts together with the different constraints of applicants and concluded with possible options.

One outcome would be to bring in requirements so that digital wallets include more inclusive forms, another one would be to build a viable solution.

Thanks to MOSIP, DHI team and OpenWallet Foundation people for their time and insights around that topic.

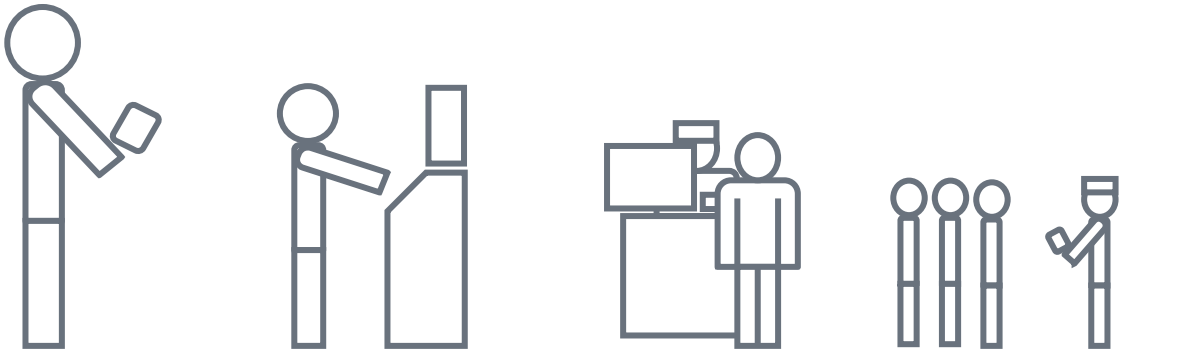
Fill the digital gaps facing applicants

Most solutions developed for citizen interactions with government assume that all citizens can access technology.

In developing countries, this is far from the case.

The idea is to keep digitalization moving forward and to identify a portfolio of solutions ensuring access to services for all citizens, from the most vulnerable to the most tech-enabled.

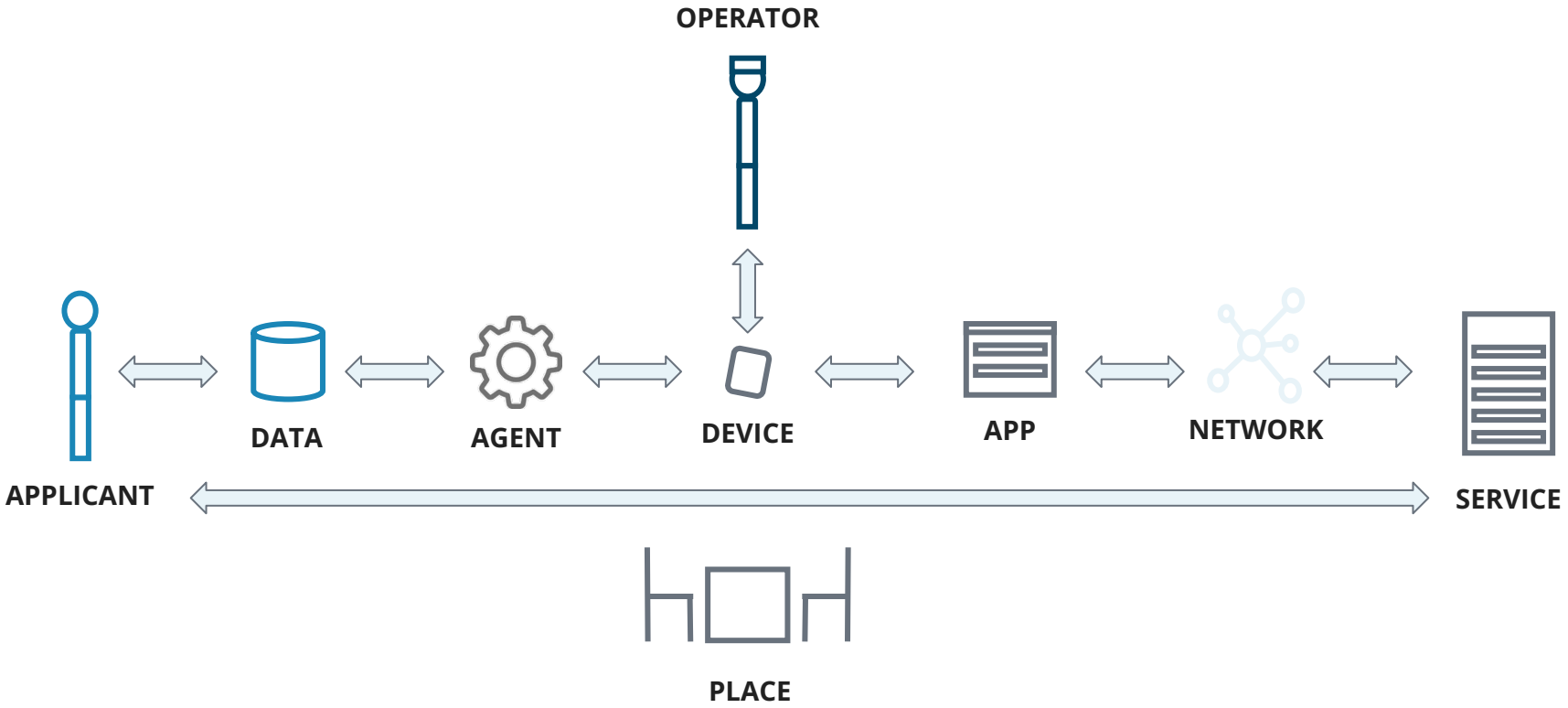
IDEAL SITUATION



REAL SITUATION

ID30

Setting the scene of an application



Characters involved in the scene

← CONTEXTS CONSTRAINTS →

← SOLUTIONS COMPONENTS →



APPLICANT

Willing to apply for a service.

A person, possibly representing another person or an organization



DEVICE

Equipment involved in the application

It can belong to applicant or to the operator or to the service provider.

Multiple devices may be required.

NETWORK

Connectivity available at the place of the application.

It affects the application depending on its availability and performance.

What matters is availability, bandwidth and latency.



PLACE

The place where the application happens.

It can be in various places which are more or less configured for the application.

Place impacts application design



DATA

Storage of personal data of the applicant.

This storage contains data and claims of the applicant.

They are encrypted and access is limited to applicant only.



AGENT

Agent managing access to personal data

The agent can extract personal data on the applicant's request.

The data are formatted according to the end use



APP

Application used for the service.

It's hosted on the device.

It is used by the operator or by the applicant for self-service.



OPERATOR

Assists the applicant with the application.

Staff member of the service provider who uses the app

There may be no operator (self-service)

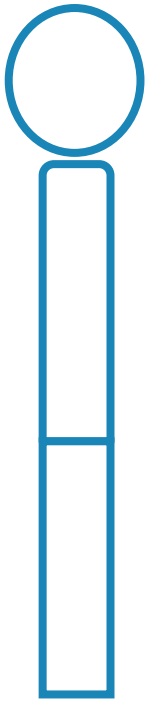
ID30

THE DIFFERENT SITUATIONS

Contexts, constraints and solutions components

ID30

Constraints inherited from the Applicant



Literacy. Can speak the official language? Can read/write?

Has a personal device? Which device?

Has network access? Which data network generation?

Has access to transport and communication infrastructure?

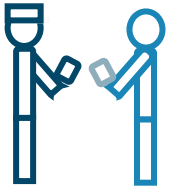
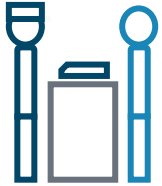
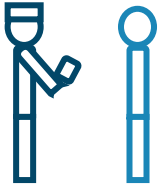
Has access to public administration? How far?

Has a **form of identity**. Card? Digital ID?

Understand the process of application

Understand the need for the application

Does the applicant have or use their own device?

	SELF-SERVICE			ATTENDED		
USE OF PERSONAL DEVICE	 PERSONAL MOBILE DEVICE	 PERSONAL COMPUTER	 COMPUTER & PHONE	 OFFICE	 COUNTER/GATE	 MOBILE
USE OF SERVICE DEVICE	 KIOSKS	 WALL- MOUNTED	 OFFICE	 COUNTER/GATE	 MOBILE	

ID30

Availability and quality of network

Depending on the place, **access to data network** may be more or less available:

- Available with **high bandwidth low latency** (e.g. 5G/Fiber)
- Available with **fair bandwidth/latency** (e.g. 4G/ADSL)
- Available with **low bandwidth/fair latency** (e.g. 3G)
- Available with **limited bandwidth/high latency** (e.g. 2G)
- **Unstable** or **temporarily unavailable** (rural areas)
- **Never available** at all (remote areas)

Network will depend on **communication infrastructures**, **access to energy** and **ownership of devices**.

The application approach needs to be adapted accordingly.

Specific case of offline or lowline

Offline or lowline contexts are generally due to technical barriers such as access to **infrastructures**, access to **devices**, unstable **resources**.

Without connectivity or devices in the applicant's hands, services need to be delivered locally and using **what people have** and **can use**.

For example, if they have no device, it would be possible to deliver them a **secured token** (card with chip or secured USB stick) so they can **keep their data with them**.

Ultimately, to save costs, data could be **printed on a card** together with a **digital signature** attesting their authenticity.

USE CASES

ID30

OPTIONS

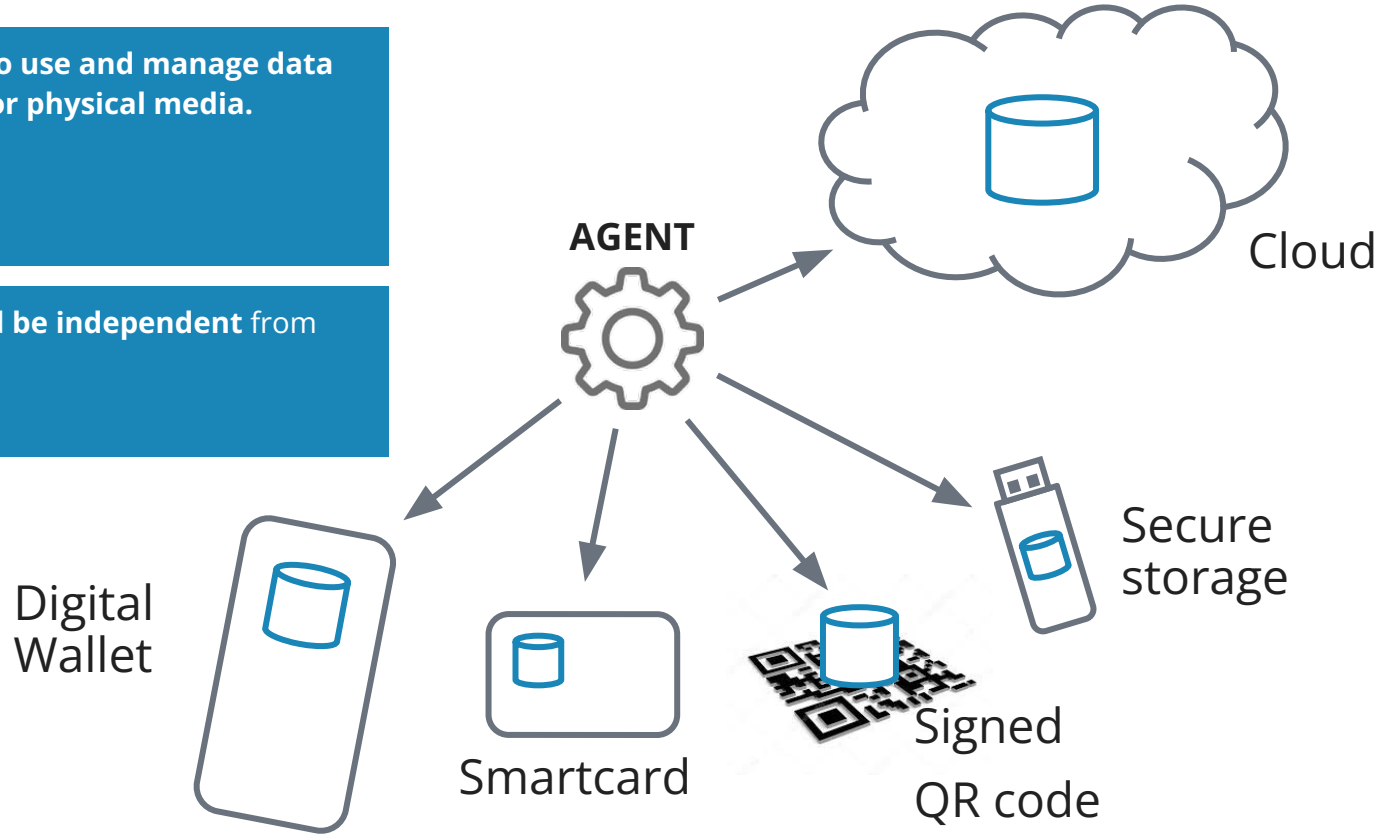
How to combine solution components
to address the different situations

ID30

Agent(s) and location of data

Agents must be able to use and manage data from multiple digital or physical media.

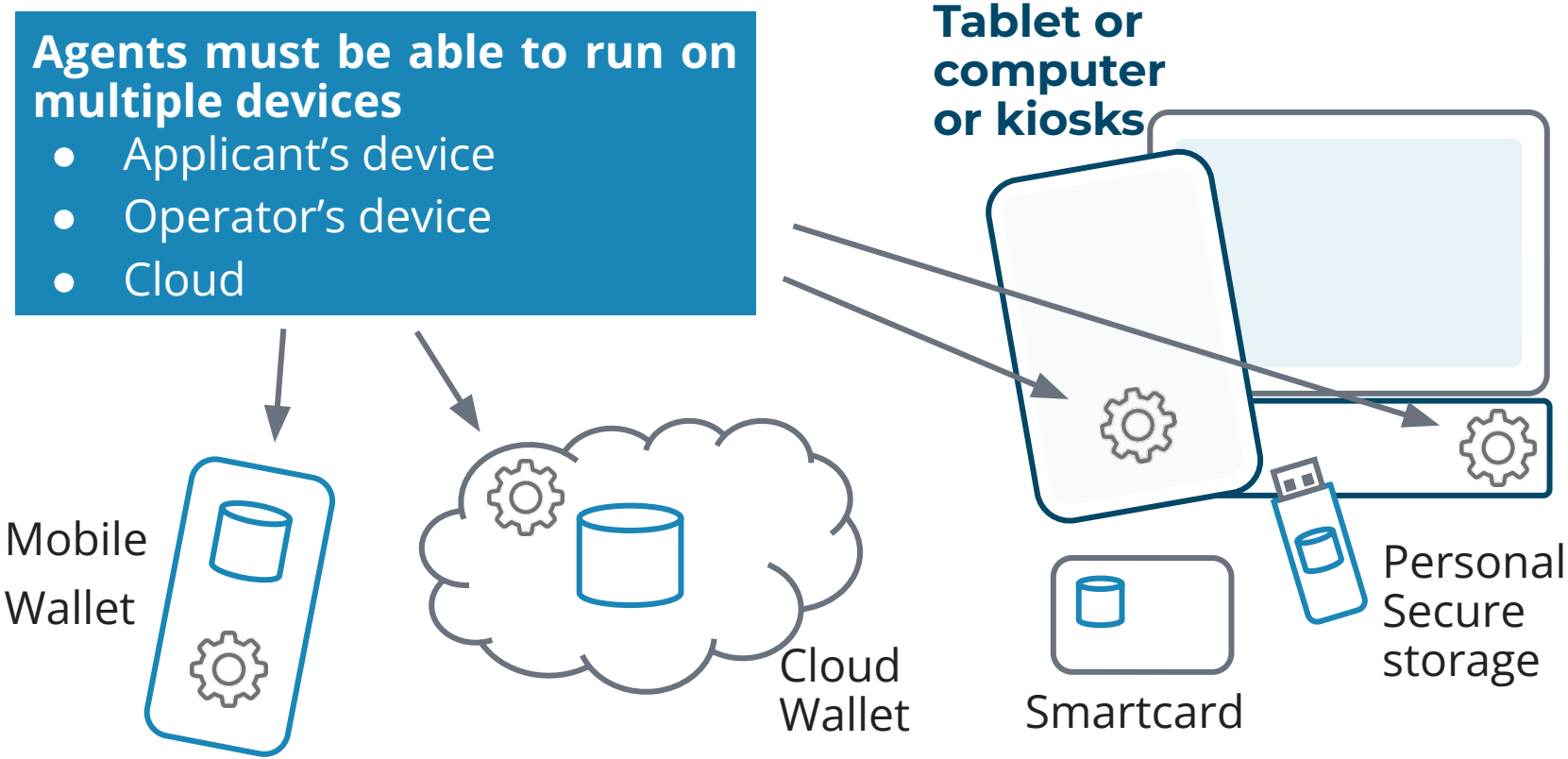
Agents location should **be independent** from **data location.**



Location of agents

Agents must be able to run on multiple devices

- Applicant's device
- Operator's device
- Cloud



Options for low setup areas

A **set of low-tech solutions** needs to be enabled specifically for **low-setup areas**.

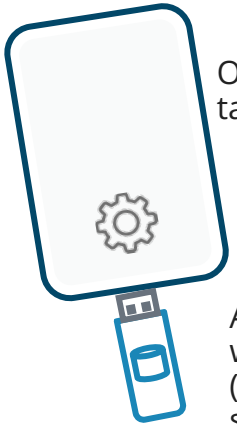


No device!
No network!



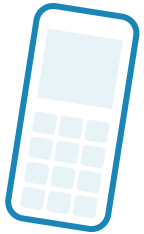
No agent

OR

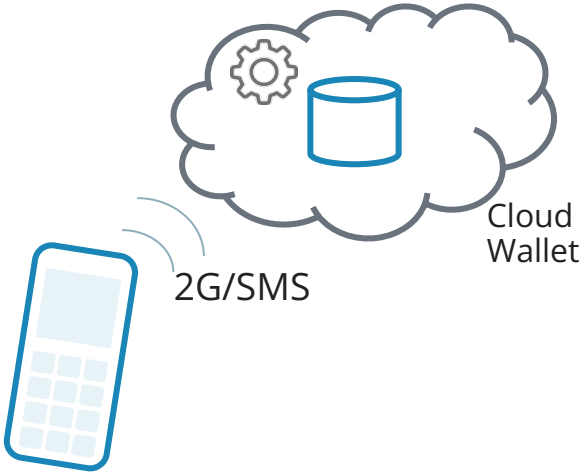


Operator's tablet (Agent)

Applicant wallet (Secure storage)



Feature phone 2G network



Cloud Wallet

2G/SMS

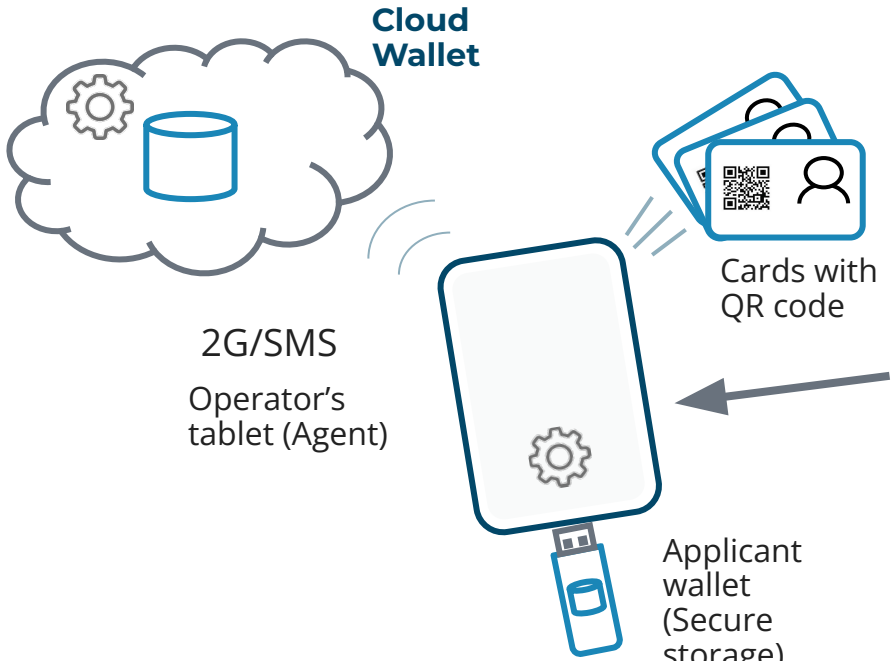
ID30

A versatile solution for low-setup countries

We should use a single solution that adapts to different contexts

One solution for the different low-setup cases (no device or low connectivity)

Once identified, this solution should be redesigned from the standpoint of each context.



A cost-effective ANDROID TABLET would do the job in multiple cases.

It should have:

- **Camera**
- **USB slot**
- **SIM slot**

That tablet would **belong to the operator** of the **services provider**.

A professional **can afford** a **device** and a **data subscription**.

ID30

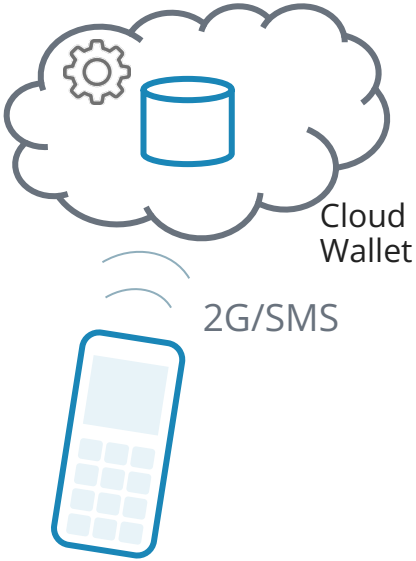
Implications for Digital Wallets solutions

OPTION 1

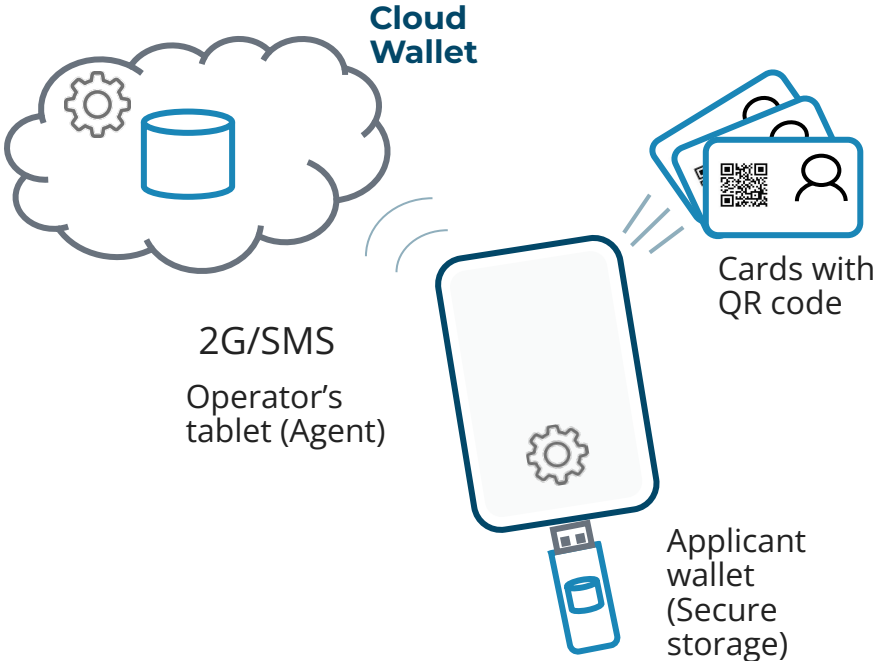
Mobile Wallet



OPTION 2



OPTION 3



ID30

Call to action

If you have reached this slide

… and if you are willing to contribute to at least one element of this solution

… and if you would like to make it happen

Please let us know: contact@id30.org