Options pour les portefeuilles numériques inclusifs

Concepts pour des formes inclusives de Digital Wallets

Jaume Dubois, janvier 2023, mis à jour en octobre 2026

ID30

Version in English is available here

Introduction

Nous considérons que les justificatifs vérifiables (‘Verifiable Credentials’ en Anglais) constituent un standard puissant pour le futur de l’interopérabilité des systèmes qui facilitera les interactions de manière fiable et décentralisée.

Ils seront faciles à émettre et à vérifier avec un smartphone, le problème restant que tout le monde n'a pas accès à ces appareils ou à la connectivité réseau nécessaire pour les vérifications.

L'objectif de cette étude est de comprendre comment les valoriser tout en limitant l'exclusion d'une partie de la population.

A cet effet, nous avons étudié les différents contextes ainsi que les différentes contraintes des candidats puis abouti à des options possibles pour plus d’inclusivité.

Un premier objectif est que les standards de Digital Wallet les prennent en compte pour permettre des versions inclusives de ceux-ci, un autre serait de construire une solution viable.

Merci à MOSIP, à l'équipe DHI et aux personnes de l’OpenWallet Foundation pour leur temps et leurs idées sur ce sujet.

Combler les lacunes numériques face aux demandeurs

La plupart des solutions développées à des fins d'interactions entre les citoyens et le gouvernement reposent sur l'hypothèse que tous les citoyens sont en mesure d'accéder aux technologies.

Mais dans les pays en développement, c'est loin d'être le cas.

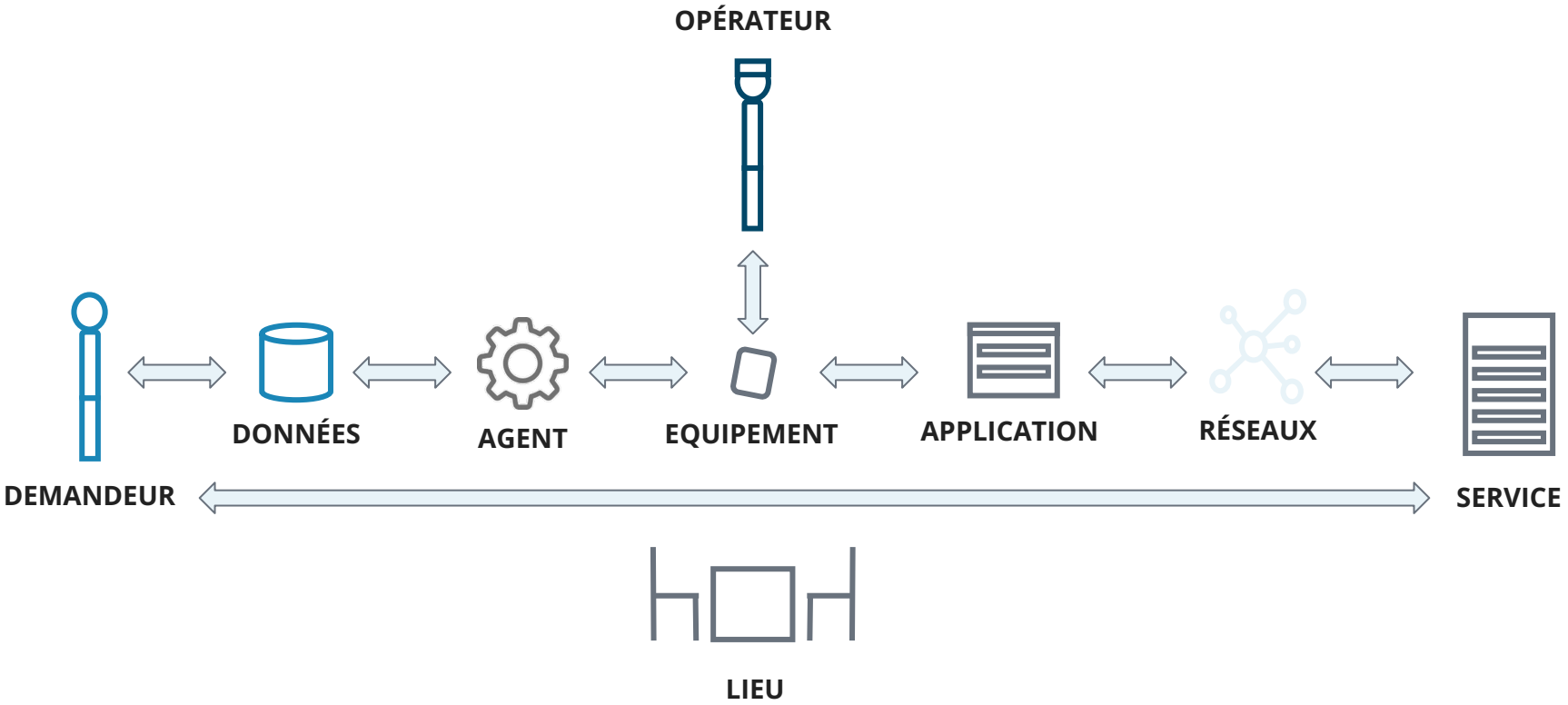
L'idée est de poursuivre la digitalisation et d'identifier un portefeuille de solutions qui permette l'accès aux services de base à l'ensemble des citoyens, des plus vulnérables aux plus équipés technologiquement.

SITUATION OPTIMALE



SITUATION NORMALE

Mise en scène d'une application



Personnages et composants impliqués



DEMANDEUR

Personne effectuant une demande de service.

C'est une personne physique, elle peut aussi représenter une autre personne ou une organisation



EQUIPEMENT

Matériel impliqué dans l'application

Il peut appartenir au demandeur ou à l'opérateur ou au prestataire de services.

Plusieurs appareils peuvent être nécessaires.

RÉSEAU

Connectivité disponible à l'endroit de l'application.

Cela aura un impact sur l'application en fonction de sa disponibilité et de ses performances.

Ce qui importe : sa disponibilité, sa bande passante et sa latence.



LIEU

L'endroit où se passe l'application.

Il peut se trouver à divers endroits plus ou moins configurés pour l'application.

Le lieu a un impact sur la conception de l'application

← CONTRAINTES LIÉES AU CONTEXTE→



DONNÉES

Stockage des données personnelles du demandeur.

Ce stockage contient des données et des justificatifs du demandeur.

Ils sont cryptés et l'accès est limité au demandeur uniquement.



AGENT

Agent gérant l'accès aux données personnelles

L'agent peut extraire des données personnelles à la demande du demandeur.

Ces données sont adaptées en fonction de l'utilisation finale



APPLICATION

Application utilisée pour le service.

Elle est hébergée sur l'appareil.

Elle est utilisée par l'opérateur ou par le demandeur en libre service.



OPÉRATEUR

Personne qui prend en compte la demande.

Membre du personnel du prestataire, c'est lui qui utilise l'application

Il peut n'y avoir aucun opérateur (libre-service)

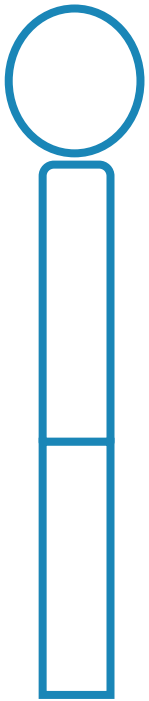
← COMPOSANTS DE LA SOLUTION →

LES DIFFÉRENTES SITUATIONS

Contextes, contraintes et composants de solutions

ID30

Contraintes du Demandeur à prendre en compte



Niveau d’éducation. Sait-il parler la langue officielle ? Sait-il lire ou écrire ?

A-t-il un appareil personnel ? Quel appareil ?

A-t-il accès au réseau ? Quelle bande-passante ?

Quel est son accès aux infrastructures ? (transport, communication)

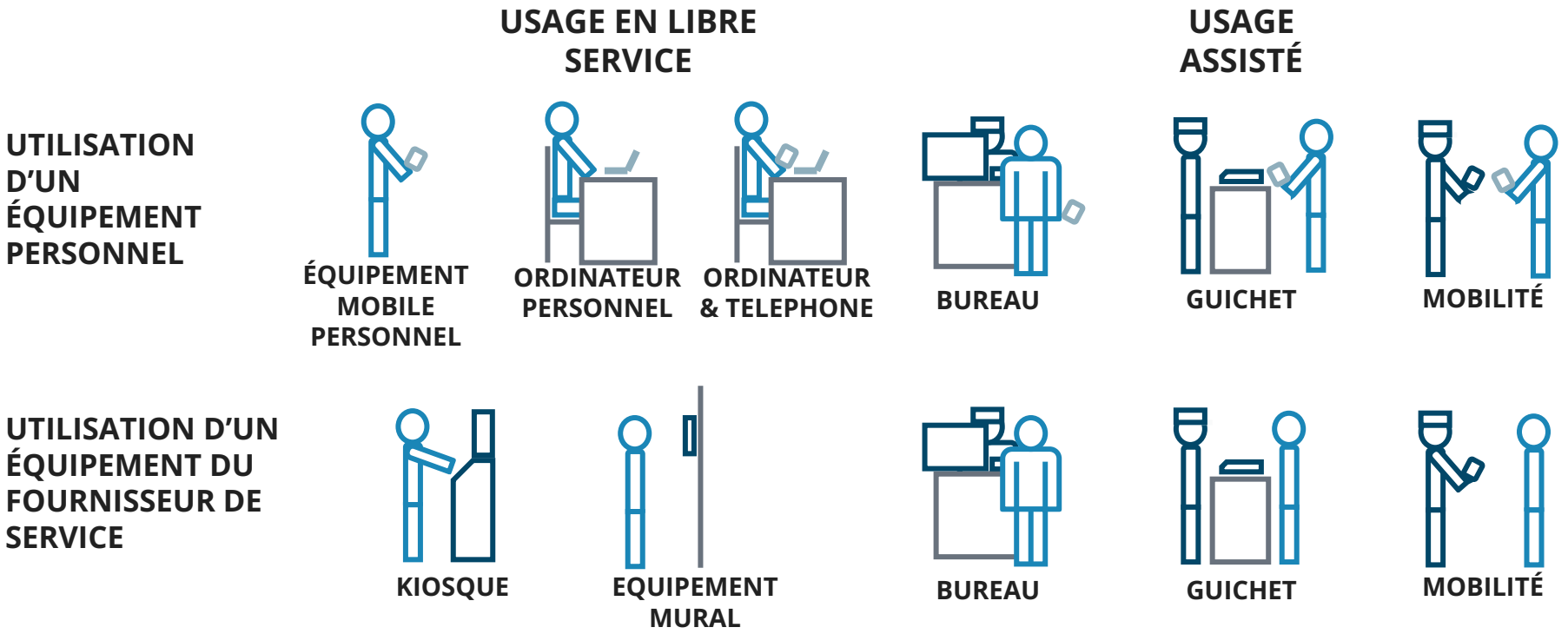
Quel est son accès à l'administration publique ?

A-t-il une forme d'identité? Carte ? Identifiant numérique ?

Comprend-il le processus de demande

Comprend-il la nécessité de cette demande

Le demandeur possède-t-il ou utilise-t-il son propre équipement ?



Disponibilité et qualité du réseau

Selon le lieu, l'accès au réseau de données peut être plus ou moins disponible :

Disponible avec une bande passante élevée et une faible latence (c.-à-d. 5G/fibre)

Disponible avec une bande passante/latence suffisantes (c'est-à-dire 4G/ADSL)

Disponible avec une faible bande passante/une latence suffisante (c'est-à-dire 3G)

Disponible avec une bande passante limitée/une latence élevée (c'est-à-dire 2G)

Instable ou temporairement indisponible (zones rurales)

Pas disponible du tout (régions éloignées)

Le réseau dépendra des infrastructures de communication, de l'accès à l'énergie et de la propriété des appareils.

La conception des solutions doit être adaptée en fonction de cela.

Cas particulier du offline ou lowline

Les contextes déconnectés ou peu connectés sont généralement dus à des barrières techniques telles que l'accès aux infrastructures, l'accès aux appareils, l'instabilité des ressources.

En l'absence de connectivité ou d'équipements possédés par le demandeur, les services doivent être fournis localement et en s’appuyant sur ce à quoi les gens ont déjà accès et savent déjà utiliser.

Par exemple s'ils n'ont pas d’équipement, il serait néanmoins possible de leur fournir un équipement de stockage sécurisé (carte à puce ou clé USB sécurisée) afin qu'ils puissent conserver leurs données avec eux.

Également, à des fins d'économie, les données pourraient être imprimées sur une carte avec une signature numérique attestant de leur authenticité.

CAS D'UTILISATION

ID30

Types d'applications

Les types d'application varient en fonction de l'objectif final, l'approche des services dépendra de la sensibilité du cas d'utilisation. Voici des exemples d'applications publiques.

Inscription	Enrôler une personne dans le système pour accéder à des services. Cela nécessite un contrôle d'identité robuste, fournissant des preuves et une attention face à face ou une détection du vivant.
Contrôle d'accès	Vérifier l'identité d'une personne avant de donner un accès physique ou numérique. Peut utiliser une ou plusieurs modalités : 'ce que je suis' (données biométriques), 'ce que je sais' (PIN, mot de passe), 'ce que je possède' (carte, clef USB, téléphone/OTP)
Contrôle de statut	Vérifier le statut de la personne pour maintenir l'accès aux services. Peut commencer par une détection du vivant ou de la présence ou la collecte de données sur la situation actuelle de la personne et la réévaluation de l'accès aux services.
Contrôle d'identité	À des fins d'enquête, le plus souvent dans une affaire pénale. Le contrôle de l'identité d'un individu, très souvent basé sur un document physique, évolue désormais vers une forme numérique d'identification ou l'utilisation de la biométrie.
Signature numérique	Pour attester d'un accord sur une transaction, sur un contrat, sur un abonnement ou pour confirmer l'authenticité d'un ensemble de données ou d'un document. Nécessite un système équipé d'un élément sécurisé.
Enregistrement dans des programmes ou demandes de services	S'authentifier et remplir un formulaire pour fournir les éléments et justificatifs associés à la souscription à un programme ou à un service. Que ce soit en tant que citoyen ou en tant que client, l'identification est clé. Il est important d'utiliser son identité légale pour les services publics, il faut aussi la lier à un moyen de paiement fiable pour les services payants.
Demande de prestations	Faire une demande et obtenir un justificatif (par exemple, diplôme, certificat de formation, examen médical, ..), cela nécessite qu'une vérification d'identité soit effectuée d'une manière ou d'une autre (automatiques ou manuelles)
Encaissement de marchandises ou d'espèces	Être éligible à recevoir un bénéfice, présenter un justificatif de ce droit, ou décliner son identité pour vérification dans une liste prédéfinie de personnes. Effectuer une identification sert également de preuve que le bénéfice a été remis à la bonne personne.

OPTIONS DE WALLETS

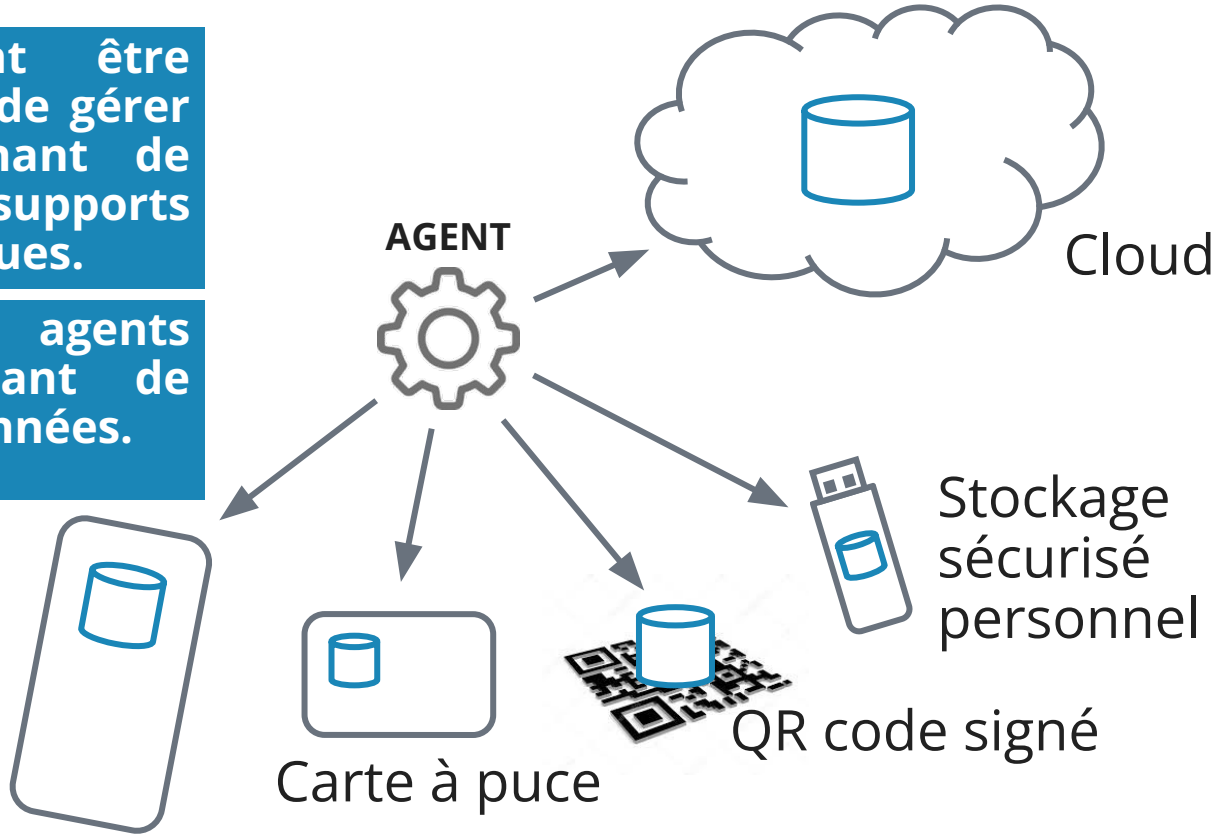
Quelles configurations de composants pour plus d’inclusion dans les différentes situations

ID30

Agent(s) et emplacement des données

Les agents doivent être capables d'utiliser et de gérer des données provenant de plusieurs supports numériques ou physiques.

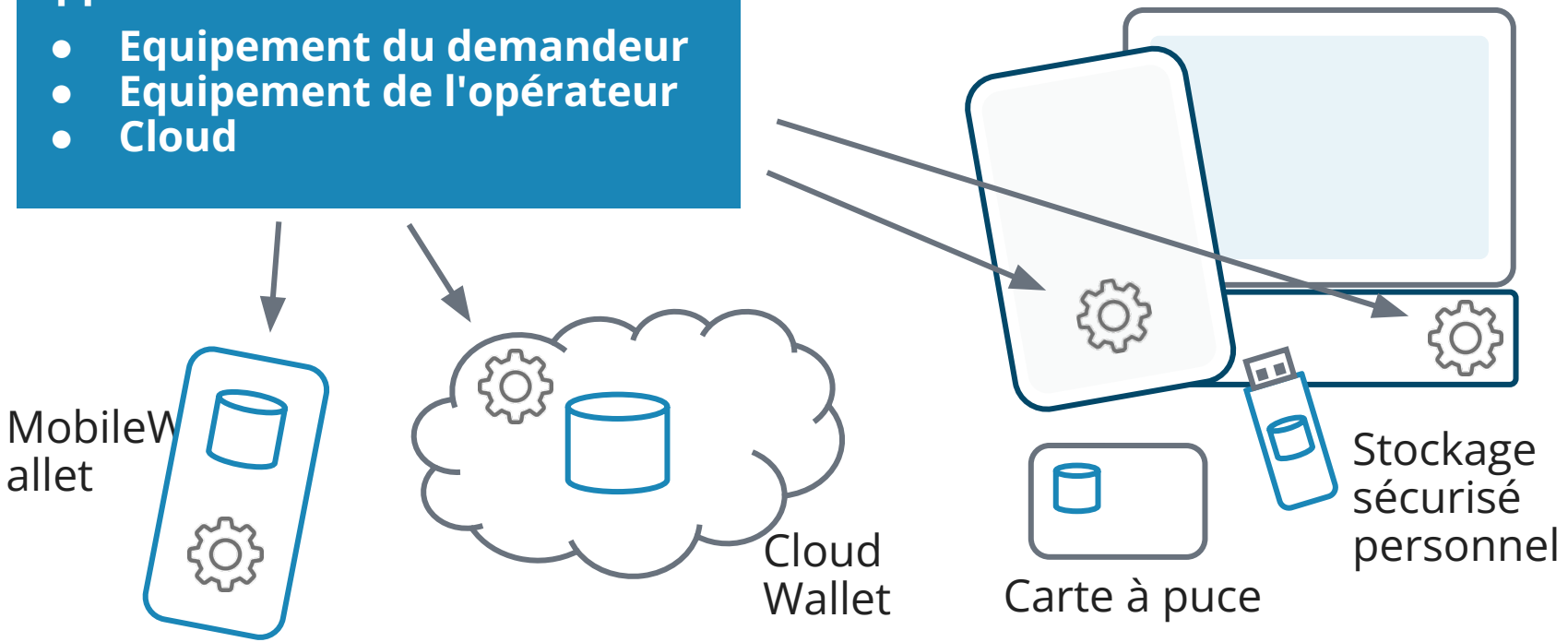
L'emplacement des agents doit être indépendant de l'emplacement des données.



Localisation des agents

Les agents doivent pouvoir s'exécuter sur plusieurs appareils:

- **Equipement du demandeur**
- **Equipement de l'opérateur**
- **Cloud**



Options pour les zones de faible configuration

Un ensemble de solutions low-tech doit être activé spécifiquement pour les zones à faible niveau d'infrastructures.

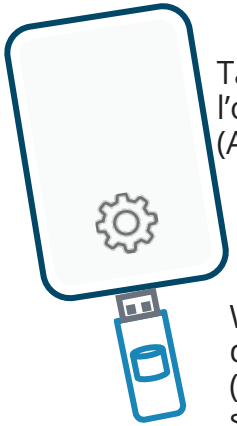
Pas d'équipements !
Pas de réseau !





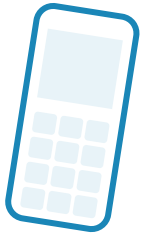
Pas d'agent

OU

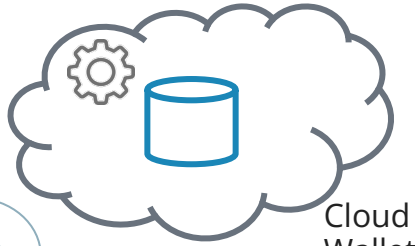


Tablette de l'opérateur (Agent)

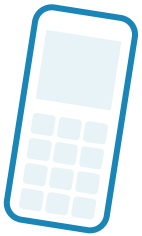
Wallet du demandeur (stockage sécurisé)



Téléphone GSM
Réseau 2G



Cloud Wallet



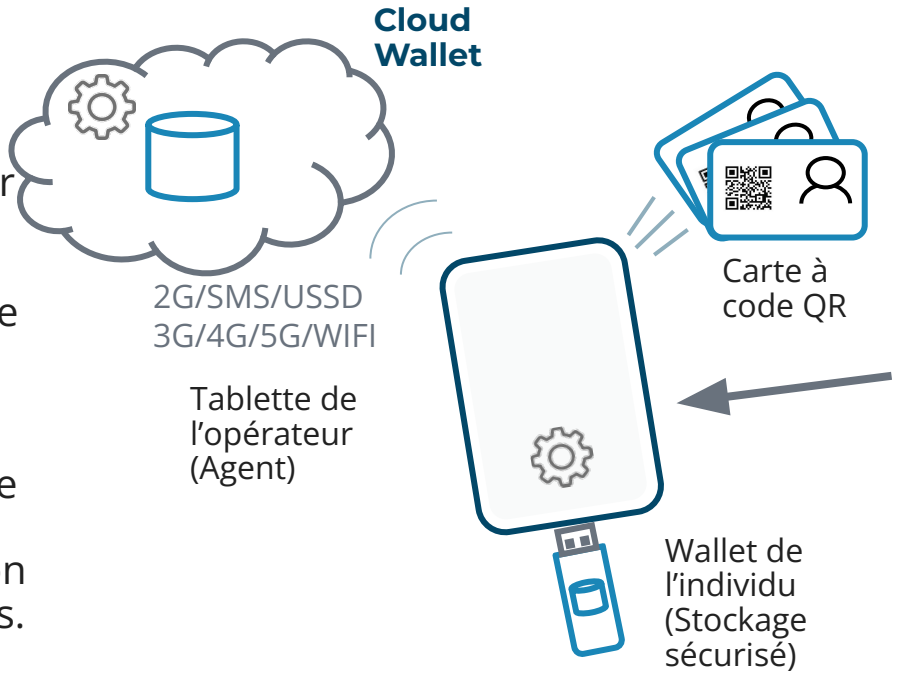
2G/SMS

Une solution polyvalente pour les pays à faible développement numérique

Il faut, dans la mesure du possible, maintenir une seule solution

Il faut une solution pour permettre une utilisation dans les zones reculées (absence de smartphones ou de connections)

Une fois identifiée, cette solution devra ensuite être adaptée en fonction des différents contextes.



Une TABLETTE ANDROID abordable peut gérer plusieurs cas.

Il faut:
Une caméra
Un Port USB
Un emplacement SIM

Cette tablette est celle de l'opérateur du fournisseur de services.

En effet, un professionnel peut se permettre d'acheter un appareil et un abonnement de données.

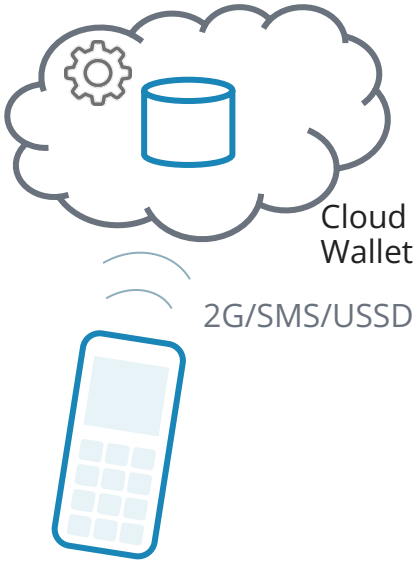
Options inclusives de Digital Wallet

OPTION 1

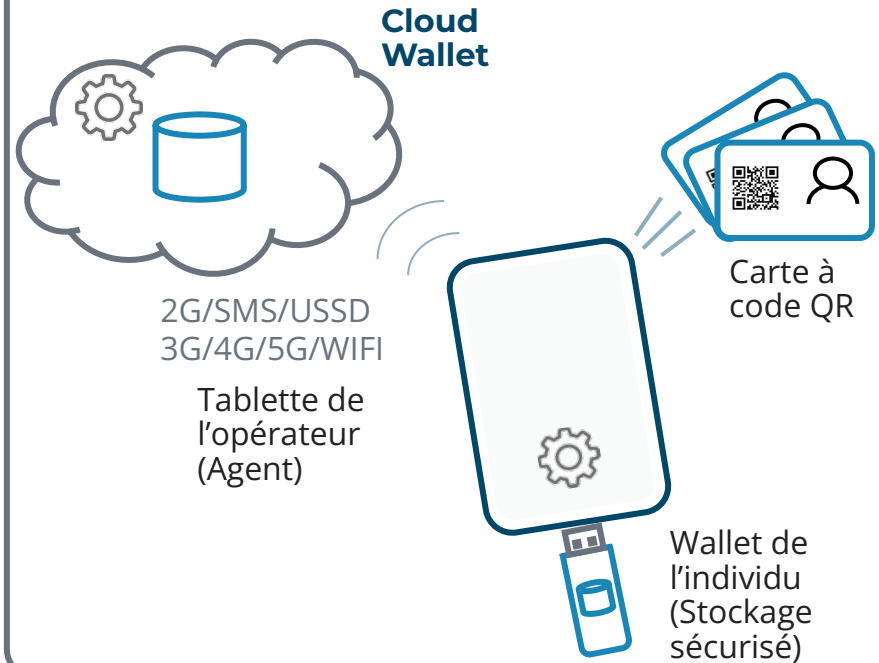
Wallet Mobile



OPTION 2



OPTION 3



ID30

MERCI !

Plus d’information : contact@id30.org

ID30