SGM CONSULTING
Digital transition expertise for financial services

FRANCE PAYMENTS FORUM
PAY' TECH DAY

Identités numériques et paiements

« Grand dérangement »
ou
rendez-vous manqué?

Stéphane MOUY
16 février 2023

SGM CONSULTING
Digital transition expertise for financial services

IDENTITÉ NUMÉRIQUE & PAIEMENTS

Messages clés

1. Identité numérique et paiements : un rapprochement au potentiel considérable et… disruptif

   Le statu quo est une mauvaise option

2. l'identité numérique sera sur wallet et décentralisée – mais, pour être pertinente, devra être en phase avec l'écosystème des paiements

   « Vaste programme ! » (citation historique)

3. Deux grandes variantes possibles des wallets eID pour les paiements
   - Complément identitaire d'une application bancaire
   - Mécanisme autonome d'autorisation de paiement

4. « *The jury is still out* » sur les fonctionnalités de paiement des wallets eIDAS 2 suite au vote du Parlement européen et à la publication de la 1ère version du *Architecture & Reference Framework* (ARF) – février 2023

   Wait & see…

FRANCE PAYMENTS FORUM
PAY' TECH DAY

SGM CONSULTING
Digital transition expertise for financial services

IDENTITÉ NUMÉRIQUE & PAIEMENTS

Identité & paiements sur wallets

Une rencontre disruptive

FRANCE PAYMENTS FORUM
PAY' TECH DAY

L'identité numérique est d'abord un outil de…

… lutte contre l'usurpation d'identité et la fraude documentaire
… gestion maitrisée des données personnelles
… et bien sûr, de sécurisation des interactions digitales et des paiements

L'identité numérique est prioritairement déployée sur smartphones au travers d'applications spécifiques (wallets d'identité)

Mais la rencontre des attributs d'identité et de paiement sur wallets annonce aussi une évolution majeure des parcours clients

- En élargissant les cas d'usage des wallets
- En allant au-delà du rôle conservation numérique des cartes de paiement (solutions X-Pay)
- En permettant une présentation combinée d'attributs d'identité, de statut et de paiement

A terme, c'est la maîtrise de la relation client qui est en jeu, avec à la clé, des parcours disruptifs pour les fournisseurs de solutions de paiement

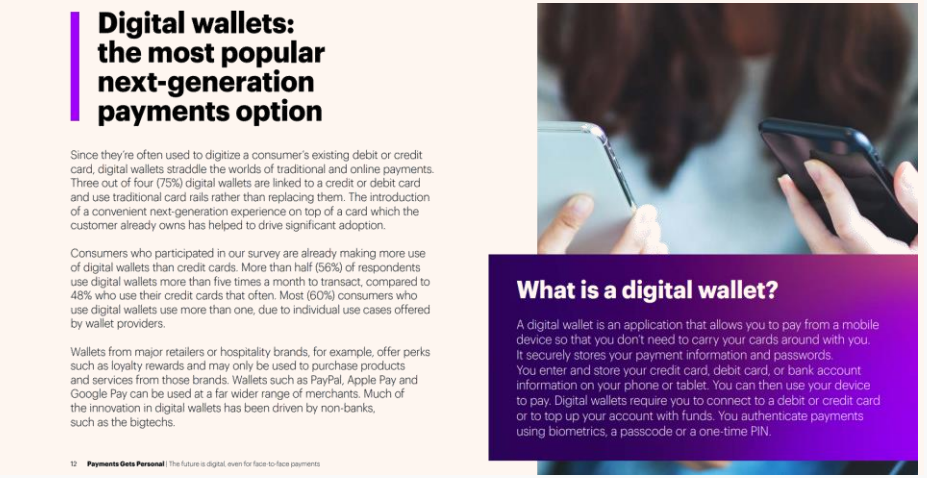
Ce qui n'a pas échappé à l'Observatoire de la Sécurité des Moyens de Paiement (Rapport 2021)

Ce qui n'a pas échappé aux GAFAM/BATX

- Apple déploie une solution d'identité numérique sur wallet aux USA (mobile Driving Licence)
- Google crée un écosystème autour de son wallet
- Mastercard se positionne sur l'identité numérique

Etude Accenture *PAYMENTS GETS PERSONAL* 2022 12

"Accenture believes there is significant revenue at risk for banks that are slow on the uptake when it comes to investing in next-generation payments options. Our analysis suggests that disruptions in payments mean that 4.6% ($89 billion) of banks' payment revenues between 2022 and 2025 are at risk."



Digital wallets: the most popular next-generation payments option

Since they're often used to digitize a consumer's existing debit or credit card, digital wallets straddle the worlds of traditional and online payments. Three out of four (75%) digital wallets are linked to a credit or debit card and use traditional card rails rather than replacing them. The introduction of a convenient next-generation experience on top of a card which the customer already owns has helped to drive significant adoption.

Consumers who participated in our survey are already making more use of digital wallets than credit cards. More than half (56%) of respondents use digital wallets more than five times a month to transact, compared to 48% who use their credit cards that often. Most (60%) consumers who use digital wallets use more than one, due to individual use cases offered by wallet providers.

Wallets from major retailers or hospitality brands, for example, offer perks such as loyalty rewards and may only be used to purchase products and services from those brands. Wallets such as PayPal, Apple Pay and Google Pay can be used at a far wider range of merchants. Much of the innovation in digital wallets has been driven by non-banks, such as the bigtechs.

12 **Payments Gets Personal** | The future is digital, even for face-to-face payments

What is a digital wallet?

A digital wallet is an application that allows you to pay from a mobile device so that you don't need to carry your cards around with you. It securely stores your payment information and passwords. You enter and store your credit card, debit card, or bank account information on your phone or tablet. You can then use your device to pay. Digital wallets require you to connect to a debit or credit card or to top up your account with funds. You authenticate payments using biometrics, a passcode or a one-time PIN.

SGM CONSULTING
Digital transition expertise for financial services

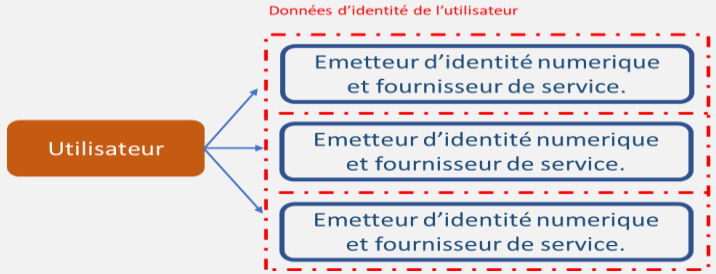
IDENTITÉ NUMÉRIQUE & PAIEMENTS

Avec les wallets eID…

… Des schémas décentralisés de gestion des identités (1/2)

FRANCE PAYMENTS FORUM
PAY' TECH DAY

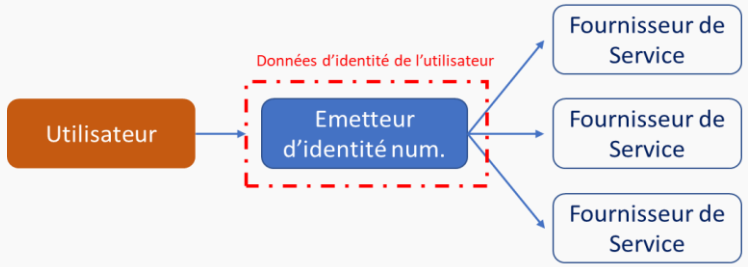
Génération I
Gestion bilatérale



- Chaque fournisseur de services gère l'authentification de chaque utilisateur
- Pas d'interopérabilité

Solution classique d'accès aux services bancaires

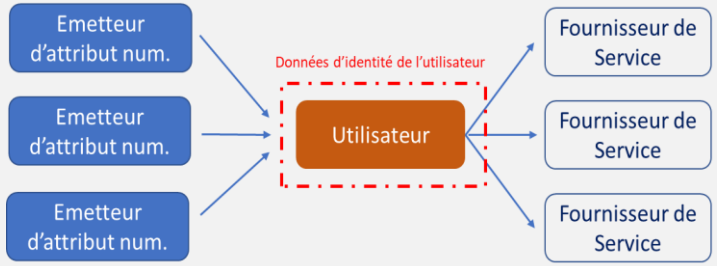
Génération II
Gestion fédérée



- L'émetteur d'identité numérique gère l'authentification de chaque utilisateur et la propage auprès de fournisseurs de services (utilisateurs d'identité numérique)
- Interopérabilité mais schéma centralisé

Schéma France Connect (évolution du schéma : il y a plusieurs émetteurs d'identité numérique)

Génération III
Gestion décentralisée



- L'utilisateur contrôle la gestion de ses données (attributs) d'identité, sans intervention des émetteurs d'attributs d'identité numérique
- Interopérabilité et respect de la vie privée

Wallets eIDAS 2

Nota : n'implique pas l'utilisation de technologies de répertoires distribués (blockchain)

SGM CONSULTING
Digital transition expertise for financial services

IDENTITÉ NUMÉRIQUE & PAIEMENTS

Avec les wallets eID…

… Des schémas décentralisés de gestion des identités (2/2)

FRANCE PAYMENTS FORUM
PAY' TECH DAY

- **Un sujet lié aux usages hors ligne des wallets d'identité numérique… (communication directe entre le smartphone et la partie sans accès à internet)**

… favorisé par les exigences de privacy (non traçabilité des usages)
… et pertinent pour les travaux en cours sur les Monnaies Numériques de Banque Centrale

- **Mais comment assurer une conservation sécurisée de clé privées sur les smartphones compatible avec un niveau de garantie élevé?**

3 Options envisageables passant par l'utilisation
- D'un **token externe** (par exemple une carte eID);
- D'un **Trusted execution environment (TEE)** offrant une solution virtualisée d'exécution des CPU
- D'un **Secure element (embedded SE)**;

- Un enjeu pour la **certification des smartphones** 'compatibles Eidas 2 High LoA' et utilisables comme **Dispositifs de Création de Signature Qualifiée**, permettant l'utilisation de signatures électroniques qualifiées en usage hors ligne comme en ligne

- Le mode hors ligne est discriminant vis-à-vis des technologies et standards utilisés. Il est par exemple mal supporté par les DLT (blockchain)

- **Niveau de garantie élevé : implique de résister à des attaques à potentiel élevé**
- Les mécanismes de preuve impliquent d'avoir accès à des clés cryptographiques privées – également requises pour le deuxième facteur d'authentification

- Processus envisagé dans le cadre des procédures de certification des wallets eIDAS 2
- Mais implique une coopération des fabricants de smartphones et de systèmes d'exploitation sur mobiles – ce qui prendra du temps !

SGM CONSULTING
Digital transition expertise for financial services

IDENTITÉ NUMÉRIQUE & PAIEMENTS

… en phase avec l'écosystème du paiement?

Un cahier des charges conséquent…

FRANCE PAYMENTS FORUM
PAY' TECH DAY

Assurer la sécurité juridique des paiements

Permettre également une utilisation en mode P2P

Conformité à la règlementation (DSP2)
- Mise en œuvre de l'authentification forte
- Mise en œuvre du lien dynamique
- Permet une implication des TPP (PISP)

Gérer les virements de compte à compte (A2A – y-compris les paiements instantanés) et les paiements par carte

Compatibilité avec l'infrastructure monétique des points de vente

Un wallet d'identité numérique avec fonctionnalité de paiement s'inscrit dans un écosystème complexe…

D'où un cahier des charges exigeant

- Authentification réciproque des parties – '***Zero trust by default***'
- Engagement pris par le payeur et le bénéficiaire juridiquement reconnu (irrévocabilité du paiement), d'où un dossier de preuve exploitable en justice

- Compatibilité avec les normes EMV CoE?

Avec à la clé une expérience client 'seamless'

… un modèle économique stabilisé pour les intervenants (ASPSP, PISP, Emetteur de wallet, bénéficiaires (*relying parties*))

et, pour finir, des règles de responsabilité claires et partagées

SGM CONSULTING
Digital transition expertise for financial services

IDENTITÉ NUMÉRIQUE & PAIEMENTS

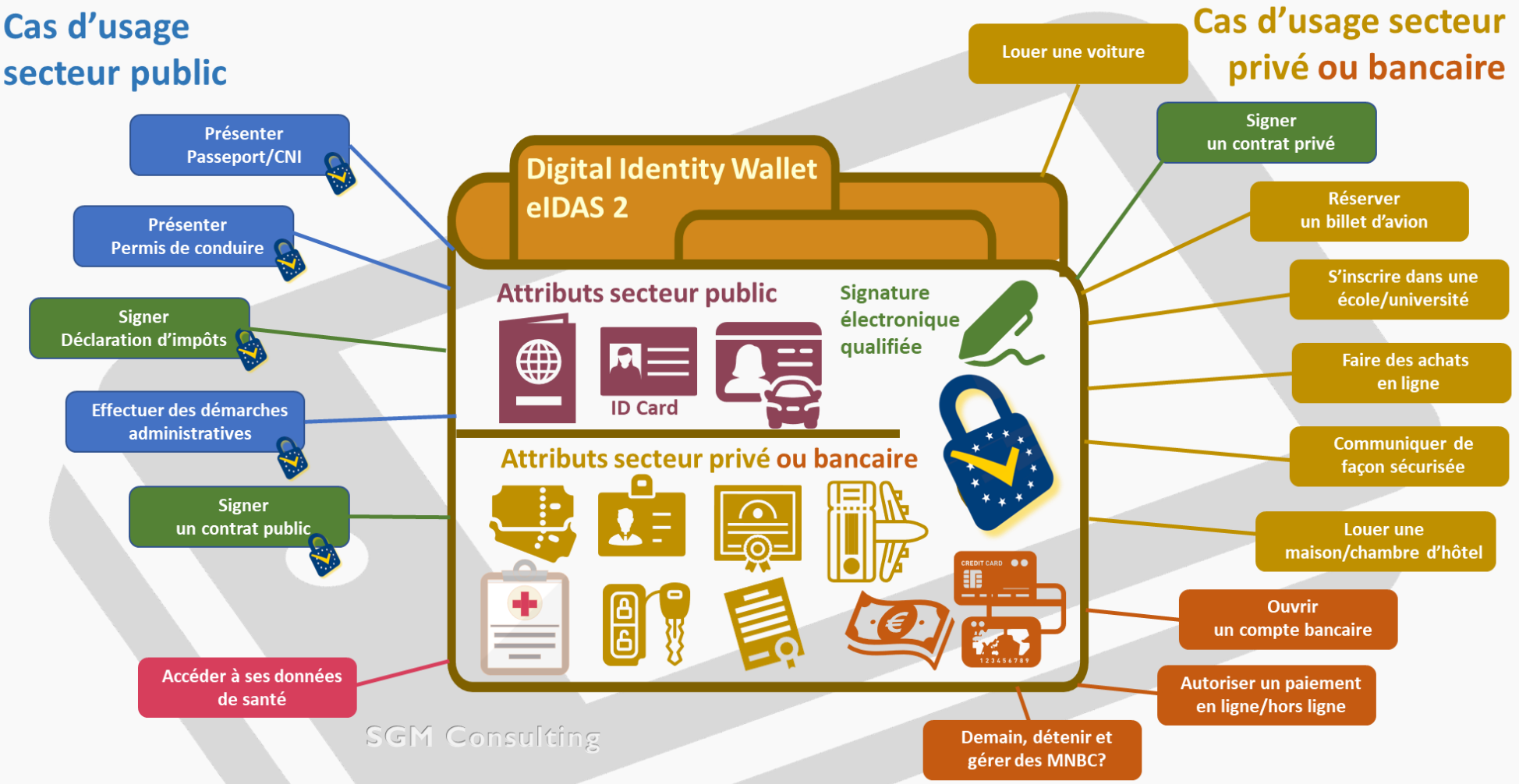
Wallet eIDAS 2

Un véritable couteau suisse des usages numériques

Et pour les paiements?

FRANCE PAYMENTS FORUM
PAY' TECH DAY

Une application sur smartphone validée par les pouvoirs publics…
Offrant un niveau de garantie élevé et… avec un très large spectre d'utilisation



SGM CONSULTING
Digital transition expertise for financial services

IDENTITÉ NUMÉRIQUE & PAIEMENTS

Wallets eIDAS 2

Points saillants du projet au 09 février 2023

- Communication de données d'identité (PII) et de données électroniquement attestées (eAA) en ligne et hors ligne
- Usages publics et privés (y-compris P2P)
- Niveau de garantie (LoA) élevé
  - Pas critiquable en soi mais… niveau d'exigences très contraignant
  - Problème pour les services de confiance (rédaction de l'article 24 1a))
  - Implique une certification des *Secure Elements* des smartphones au niveau EAL 4+
- Exigences de Privacy
- Fonctionnalité de signature électronique qualifiée
- Obligation d'enregistrement des bénéficiaires (R*elying Parties)* fournissant des biens et services
  - Quelle justification si les particuliers sont eux-mêmes exemptés?
- Et bien sûr… l'article 12b2 sur l'authentification forte et les paiements

*Where private relying parties providing services are **required by national or Union law, to use strong user authentication for online identification**, including in the areas of transport, energy, **banking and financial services**, social security, health, drinking water, postal services, digital infrastructure, telecommunications or education in particular with regard to the recognition of educational and professional qualifications, **private relying parties shall also offer and accept the use of European Digital Identity Wallets and notified electronic identification means with assurance level 'high'** issued in compliance with this Regulation for identification and authentication.*

FRANCE PAYMENTS FORUM
PAY' TECH DAY

SGM CONSULTING
Digital transition expertise for financial services

IDENTITÉ NUMÉRIQUE & PAIEMENTS

Wallets eIDAS 2

Deux options possibles pour les wallets d'identité numérique

FRANCE PAYMENTS FORUM
PAY' TECH DAY

Entrée en relation à distance – gestion du KYC

- Point généralement admis, logique au regard du niveau de garantie élevé offert par les wallets eIDAS 2

Gestion de l'authentification dans les paiements

- l'ambition du projet eIDAS est clairement de permettre l'utilisation des wallets eIDAS comme moyen d'initiation de paiement (voir Considérant 31) et d'imposer son acceptation par les prestataires de services de paiement

- Le sujet fait aujourd'hui débat
- La rédaction du texte – article 12b2 - est ambigüe et autorise, à notre avis, plusieurs interprétations

Au plan technique, deux aspects paraissent déterminants

- L'utilisation d'un mécanisme interne au wallet garantissant une authentification forte (identité numérique niveau substantiel ou élevé, signature électronique qualifiée); et

- La capacité du wallet à gérer de façon autonome l'exigence de lien dynamique résultant de la DSP2 (opérations de paiement électronique à distance – article 97.2)

- Le respect des règles d'authentification forte doit idéalement se déduire de la simple constatation de l'utilisation d'un mécanisme ou procédé garantissant l'utilisation de ces règles – par exemple une signature électronique qualifiée
- De plus, la signature électronique qualifiée gère l'exigence de lien dynamique et supporte des interactions en ligne et hors ligne

Ces éléments permettent d'anticiper deux modes d'utilisation des wallets eIDAS 2 dans les paiements

- Un wallet eIDAS 2 dépendant d'une interaction (application) bancaire pour réaliser l'opération de paiement, mais avec le risque que le schéma soit alors '*ASPSP-centric*' et exclut de fait les TPP (y-compris les PISP) et ne fonctionne pas en mode hors ligne;

- Un wallet pleinement autonome pour la mise en place de l'authentification DSP2, réalisant une authentification 'fully embedded'

- Ces considérations militent pour l'utilisation de signatures électroniques dans les interactions de paiement, d'autant plus que les wallets eIDAS 2 embarqueront une fonctionnalité de signature électronique qualifiée
- Mais de nombreuses contraintes opérationnelles demeurent, notamment l'absence de compatibilité avec les spécifications EMV Co des terminaux de paiement

SGM CONSULTING
Digital transition expertise for financial services

IDENTITÉ NUMÉRIQUE & PAIEMENTS

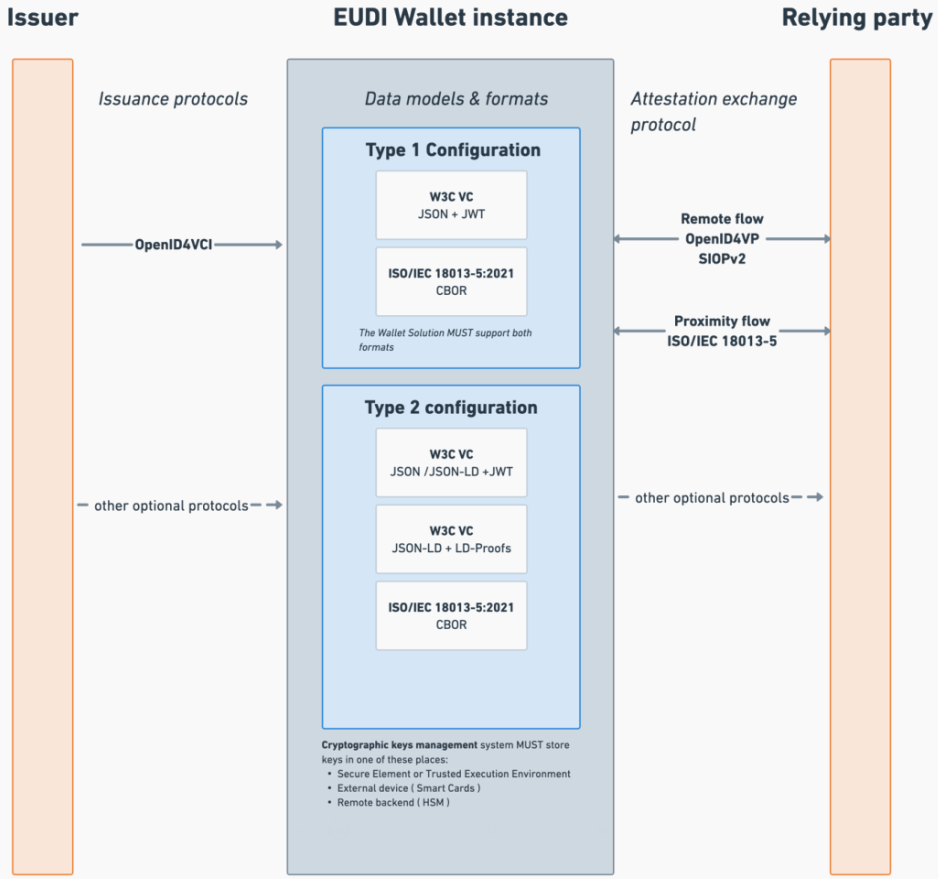
Wallets eIDAS 2

Présentation du document ARF Architecture & Reference Framework 10 février 2023

FRANCE PAYMENTS FORUM
PAY' TECH DAY

- Précise les spécifications des wallets d'identité numérique ainsi que les rôles attendus de chaque participant à l'écosystème des wallets eIDAS 2
- A prendre en compte par le consortium chargé de la production des wallets et les consortia déployant les *Large Scale Pilots*
- Une approche évolutive et 'work in progress' - certains sujets seront traités dans un second temps
- Deux configurations envisagées dont une prioritaire, centrée sur les PIDs
- Des spécifications techniques combinant plusieurs standards technologiques
- ISO/IEC 18013-5 mobile driving licence et ses dérivés (ISO/IEC 23220-4 (projet))
- W3C Verifiable Credentials Data Model 1.1.
- OPENID4VP & SIOPv2 (OpenID Connect)
- Certains aspects restent en attente de clarification et seront développés dans les prochaines versions du document ARF

- Netcompany-Intrasoft + Scytales
- NOBID (LSP Payments)
- EWC (LSP Travel + Payment)



(Document ARF – extrait)

SGM CONSULTING
Digital transition expertise for financial services

FRANCE PAYMENTS FORUM
PAY' TECH DAY

Merci pour votre attention

Stéphane MOUY
sgmouy@sgmconsultingservices.com