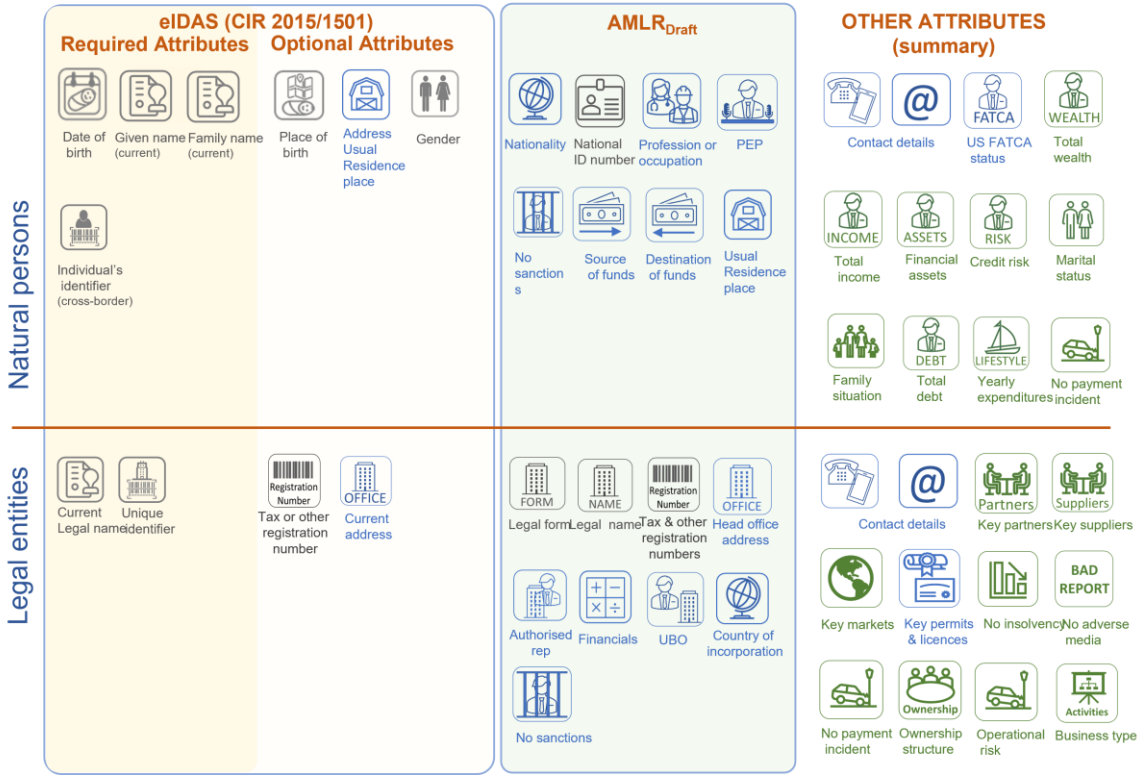
SGM Consulting
In cooperation with
eWALLET NETWORK

The new world of eIDAS 2.0 EDIWs
What it means for relying parties?

Is KYC data portability within reach?



Stéphane Mouy
SGM Consulting

14 October 2021

OIX OPEN IDENTITY EXCHANGE

SGM Consulting
In cooperation with
eWALLET NETWORK

-1-

eIDAS 1
eIDAS 2
&
AMLR

A new landscape on the horizon for CDD Data

eIDAS 1.0 (2014)

Digital Identity schemes
- Discretionary notification process (St[illegible]-controlled)
- Public-s[illegible]us
- High[illegible]vel l[illegible] EU guidelines
- Tech[illegible]ical specs remain nati[illegible]al
- SAML[illegible]ed i[illegible]roperability architecture

RESET

eTrust Services
- E-signature & seals + 3 others
- Fully open to private sector
- Accreditation process
- ETSI standards

eIDAS 2.0 (2022)

Digital Identity schemes
- European Digital Identity Wallets (**EDIWs**) in addition to digital identity schemes
- Public & private-sector use
- Accreditation process
- Common technical specifications
- Fully recognised within EU

eTrust Services
- **e-attested attributes** linked to EDIWs
- e-archiving services
- e-ledgers

AMLR (2022)

Customer Due Diligence (CDD)
- Common Identity attribute requirements (natural & legal persons)
- Regulatory technical standards by future AMLA for simplified and enhanced CDD

- Recognition of EDIWs (on a par with ID documents)

- **CDD Data Portability**
- Common rules for '*third party reliance*'
- Common rules for CDD outsourcing

Significant impact for the Financial Sector

OIX OPEN IDENTITY EXCHANGE

SGM Consulting
In cooperation with
eWALLET NETWORK

-2-

eIDAS 2 defines broad EDIW specifications

But more is to come with the

MUST HAVE	Must be accredited – complies with common specifications	Common specifications co-constructed with eIDAS Expert Group
	Must be issued or 'approved' by a Member-State	Digital equivalent of national ID cards & passports
	Must offer ***High*** Level of Assurance	For remote ID-proofing - will likely imply using biometric-based ID-proofing processes (CIR 2015/15002 & ETSI 119 461)
	Must put EDIW users in full control of EDIWs	(who can disagree with this?)
	Must be accepted for identity-proofing by relying parties offering **financial** and other key services as well as '*very large online platforms*' (GAFAM + BATX)	Private-sector focus. Cannot be refused by key private and public service providers Relying parties will need to be authenticated
	Must accept eAAs (electronically attested attributes)	Range of attributes goes beyond core ID attributes (extends to status, qualifications, **financial data**, etc)
	Must be free of charge for users	(but not necessarily for other participants)
	Must create Qualified Electronic Signatures/seals	**CRITICAL REQUIREMENTS**
	Must work offline as well as online	
	Must support Strong Customer Authentication requirements (inc. for payment authorisation)	**WITH STRUCTURAL IMPLICATIONS**
NICE (OR VERY NICE) TO HAVE	**Strengthen privacy**	… but will need to communicate the 'Unique identifier' whenever required (when?)
	Allow several identity profiles	Use for private/professional context
	Support CBDCs	

High LoA Identity + **Offline & SCA/payment initiation** functionalities + **Signing/countersigning** viewed as key steps for CBDC deployment

OIX OPEN IDENTITY EXCHANGE

SGM Consulting
In cooperation with
eWALLET NETWORK

-3-

What to make out of this?

- (Very) ambitious proposal + tight implementation timeframe

- The EDIW – a near universal digital credential

All key service providers required to accept EDIWs
  - Core ID attributes
  - 'e-attested attributes' (issued by eIDAS TSPs but available on EDIWs)

- A structural impact on the financial sector (AML/CFT 'obliged entities')

1. Data providing side : Financial institutions can provide electronically attested attributes on EDIWs (IBAN, account information, etc)
   - Not certain whether this implies TSP status

2. For CDD processes : EDIWs clear substitutes for ID documents
   - EDIWs avoid *Third party reliance* constraints (FATF recommendation 17)
   - Key tool for CDD Data portability/reusability but economic model + liability allocation provisions need addressing

3. EDIWs will authorize payments online and offline
   - Structural impact on PSD2 SCA processes
   - 'Redirection' no longer needed (inconsistent with offline mode)

OIX OPEN IDENTITY EXCHANGE

SGM Consulting
In cooperation with
eWALLET NETWORK

-4-

eIDAS 2.0

SSI and privacy considerations

• Is eIDAS 2.0 embracing SSI solutions?

No obvious answer – full picture not available yet

On the one hand

- EDIWs meant to offer full/sole control over data to users - EDIWs are in effect self-custody solutions for ID and other attributes
- No obvious discrepancy with SSI principles

On the other hand

- EDIWs to be issued or 'recognised' by member States; and
- Existing federated eID solutions still valid with eIDAS 2.0

Also having distributed ledger solutions work offline appears to be a challenge (is there a solution?)

• Privacy considerations

EDIWs should enhance privacy

- Stated as a key goal of eIDAS 2.0
- Wallet issuers are prohibited from monitoring wallet usage (+ stringent data segregation requirements apply to TSPs for e-attested attributes)
- But '*Unique & persistent identifier*' is stated as a key ID attribute for EDIWs

However, solutions are available to prevent EDIW tracking and still meet eIDAS 2.0 requirements

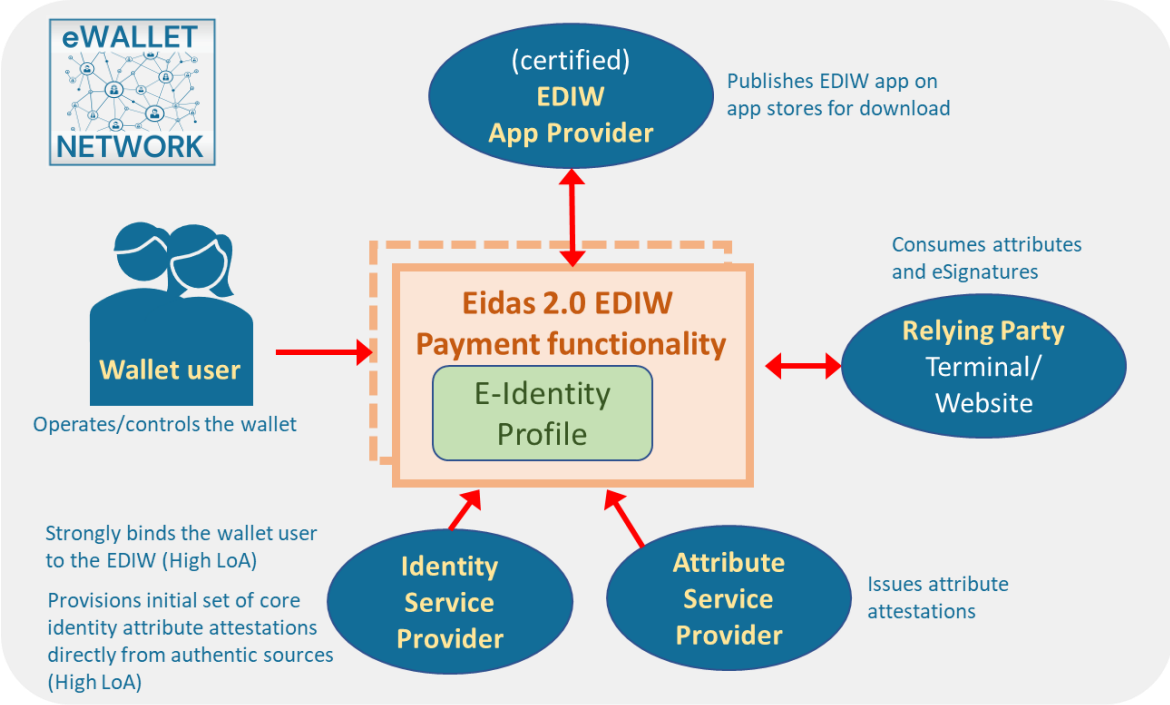
OIX OPEN IDENTITY EXCHANGE

SGM Consulting
In cooperation with

-5-

Implementing an e-sign EDIW design for payment and attribute exchanges

- The eWallet Network has worked on an EDIW design with offline payment initiation functionality - and PSD2-compliant strong customer authentication



An open architecture supporting multiple interfaces and participants

With seamless interoperability across multiple sectors and borders

- The EDIW is in essence a SDO (signed data object) tool allowing:
  - Secure **offline** interactions between EDIWs and relying parties - with full signature verification
  - **Countersigning** of payments for legal certainty (full audit trail)
- Other exchanges are treated in the same way (can be viewed as 'no-amount' payments)
  - used for communication of ID attributes and other attributes

OPEN IDENTITY EXCHANGE

SGM Consulting
In cooperation with
eWALLET NETWORK

-6-

EDIW FOR PAYMENTS & ATTRIBUTE EXCHANGES (identity & other attributes) – APP STRUCTURE

eWALLET NETWORK

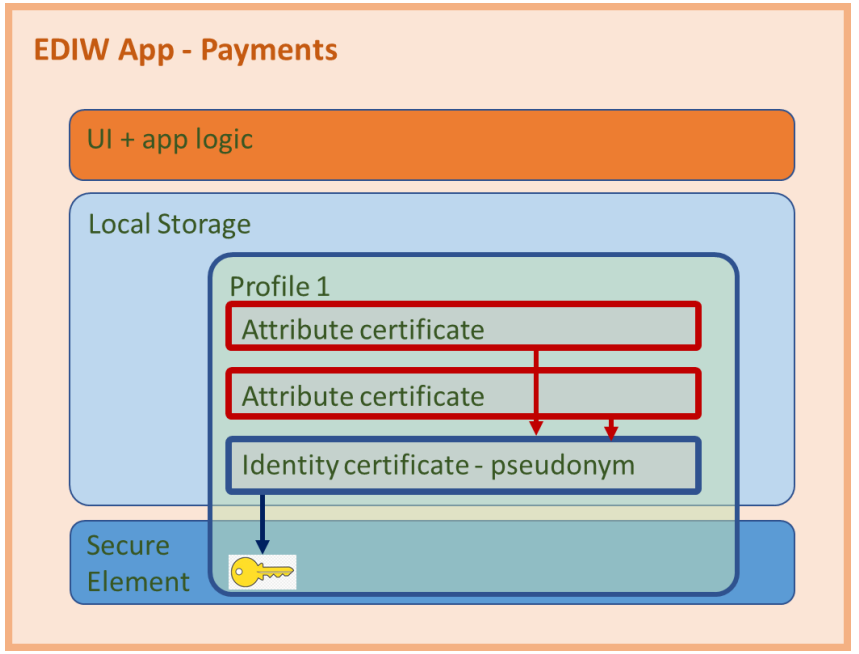
eWallet Network proposal

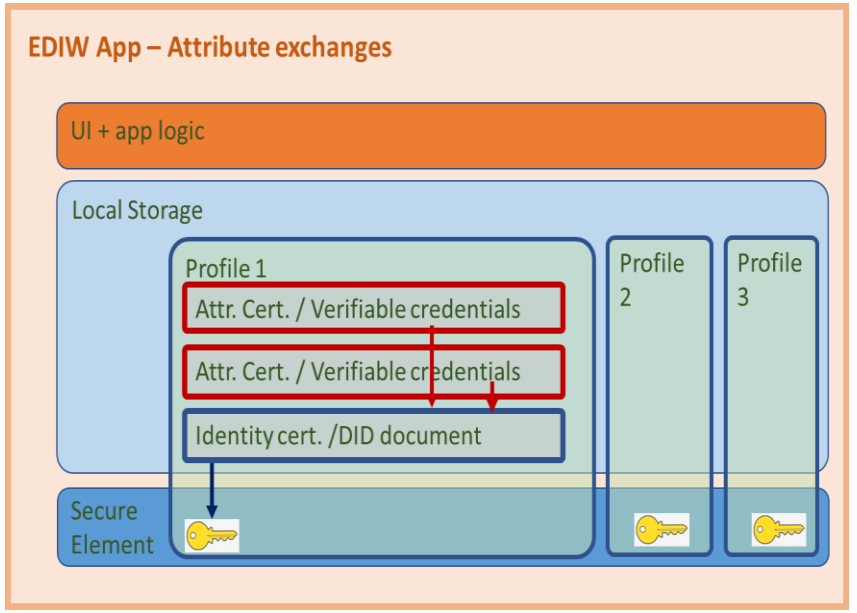
Storage of personal attributes

- **(Q)SCD to store the private key of a (Q)cert – ”identity certificate”**
- **Storage of additional attribute certificates - “attribute certificates”**

This can be extended to multiple profiles

- Multi-profile (but this is also useful for payments) – e.g. for professional and private use
- Provided by MSs / authorized by MSs (High LoA requirement)
- Attr. certificates / verifiable credentials? ID certificates / DID documents ?





OPEN IDENTITY EXCHANGE

SGM Consulting
In cooperation with
eWALLET NETWORK

-7-

A PROTOTYPE WALLET BASED ON EXISTING NON-PROPRIETARY STANDARDS

Attribute description based on W3C Verified Credential (VC) JSON structures and schemas

Real-world chain of trust based on digital certificates

Digital certificates based upon :

- X.509 specifications; ETSI 319 411-2 requirements for qualified certificates
- The EIDW proof based upon eIDAS qualified signatures, ETSI XAdES and ASiC

Communications based upon :

- HTTPS, NFC, BLE, QR code
- Elliptic Curve Diffie-Hellman for message end-to-end encryption

Work remains to be done on wallet message interchange standards

To be considered as part of the toolbox approach (eIDAS Expert Group)

In particular, attribute exchange message formats & protocols need standardising

ETSI also involved

OIX OPEN IDENTITY EXCHANGE

SGM Consulting
In cooperation with
eWALLET NETWORK

-6-

TO CONCLUDE

e-sign EDIW payment demo
link

KYC portability EU report
link

OIX OPEN IDENTITY EXCHANGE

Work still in progress : this is not the end of the story…

But thank you for your attention

SGM CONSULTING

Stéphane Mouy - President

Digital transition expertise for financial services

SGM Consulting Services
25 rue Lavoiser
75008 Paris
France
RCS Paris 852 543 420

Phone : +33 188 325 650
https://sgmconsultingservices.com

sgmouy@sgmconsultingservices.com

Special thanks to Michael Adams

Quali-Sign
Specialists in mobile apps for eID and Strong Customer Authentication

Alderley Edge
Cheshire
UK

michael_adams@quali-sign.com