FRANCE
PAYMENTS
FORUM

eIDAS 2.0 EUROPEAN DIGITAL IDENTITY WALLETS (EUDIWs)

WHEN PORTABLE IDENTITY MEETS PAYMENTS…

Great things can happen!

SGM CONSULTING
Digital transition
expertise for
financial services

Stéphane Mouy
SGM Consulting

eIDAS 2.0

WHEN PORTABLE IDENTITY MEETS PAYMENTS

I – THE eIDAS 2.0 PARADIGM FOR EUDIWs

II – LOOKING BEYOND PAYMENT-ENABLING EUDIWs – CBDCs

III – UNDER CONSTRUCTION : THE e-SIGN PAYMENT-AUTHORIZING EUDIW

FRANCE PAYMENTS FORUM

Stéphane Mouy
SGM Consulting

eIDAS 2.0

WHEN PORTABLE IDENTITY MEETS PAYMENTS

I – THE eIDAS 2.0 PARADIGM FOR EUDIWs

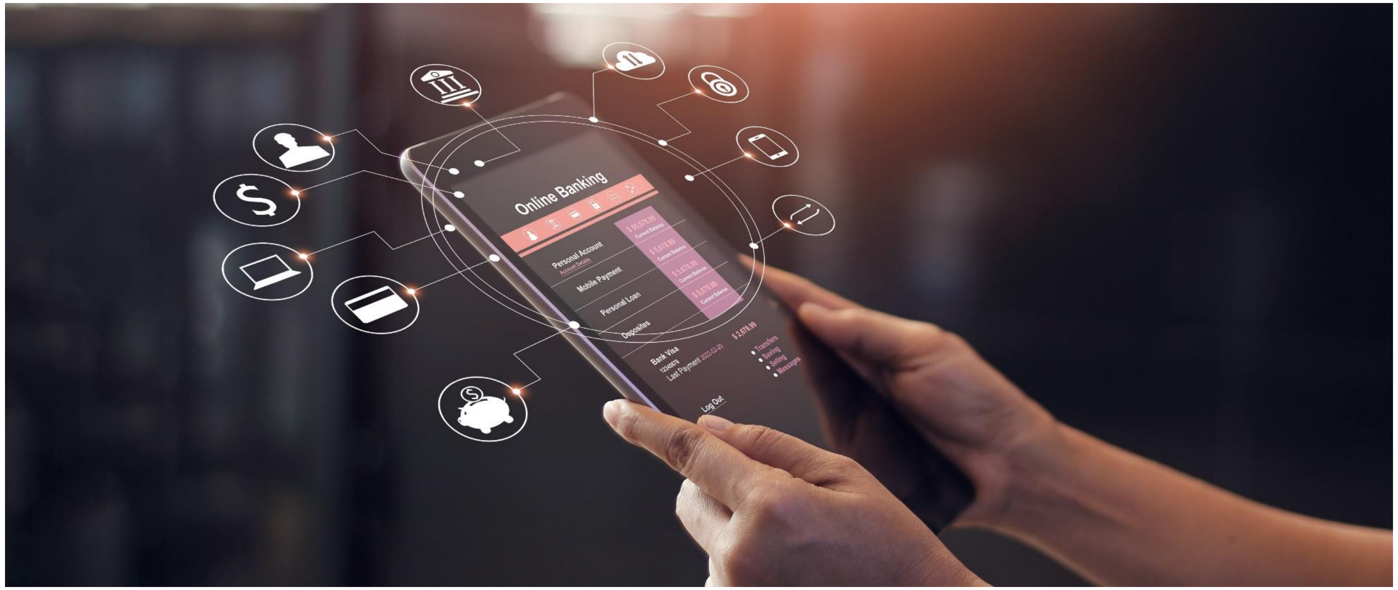
II – LOOKING BEYOND PAYMENT-ENABLING EUDIWs – CBDCs

III – UNDER CONSTRUCTION : THE e-SIGN PAYMENT-AUTHORIZING EUDIW

FRANCE PAYMENTS FORUM

Stéphane Mouy
SGM Consulting

WITH EUDIWs, eIDAS 2.0 HERALDS THE CONVERGENCE OF HIGH QUALITY IDENTITY, STATUS AND PAYMENT ATTRIBUTES, A STEP WITH TRANSFORMATIONAL IMPLICATIONS FOR EU PAYMENT SERVICE PROVIDERS



Attribute-based

User centricity

Multiple use cases

Private-sector focus

High LoA

*“The **vast majority of the needs of electronic identity and remote authentication remain with the private sector**, in particular in areas like **banking…**”* (eIDAS.2 Explanatory memorandum)

eIDAS 1, eIDAS 2 & AMLR

A new landscape on the horizon for CDD Data

FRANCE PAYMENTS FORUM

Stéphane Mouy
SGM Consulting

eIDAS 1.0 (2014)

Digital Identity schemes

- Discretionary notification process (State-controlled)
- Public-sector focus
- High level LoA EU guidelines
- Technical specs remain national
- SAML-based interoperability architecture

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

EUDIW

Key specs.

Toolbox approach

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** **WITH STRUCTURAL IMPLICATIONS**
	Must work offline as well as online	
	Must support Strong Customer Authentication requirements (inc. for payment authorisation)	
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

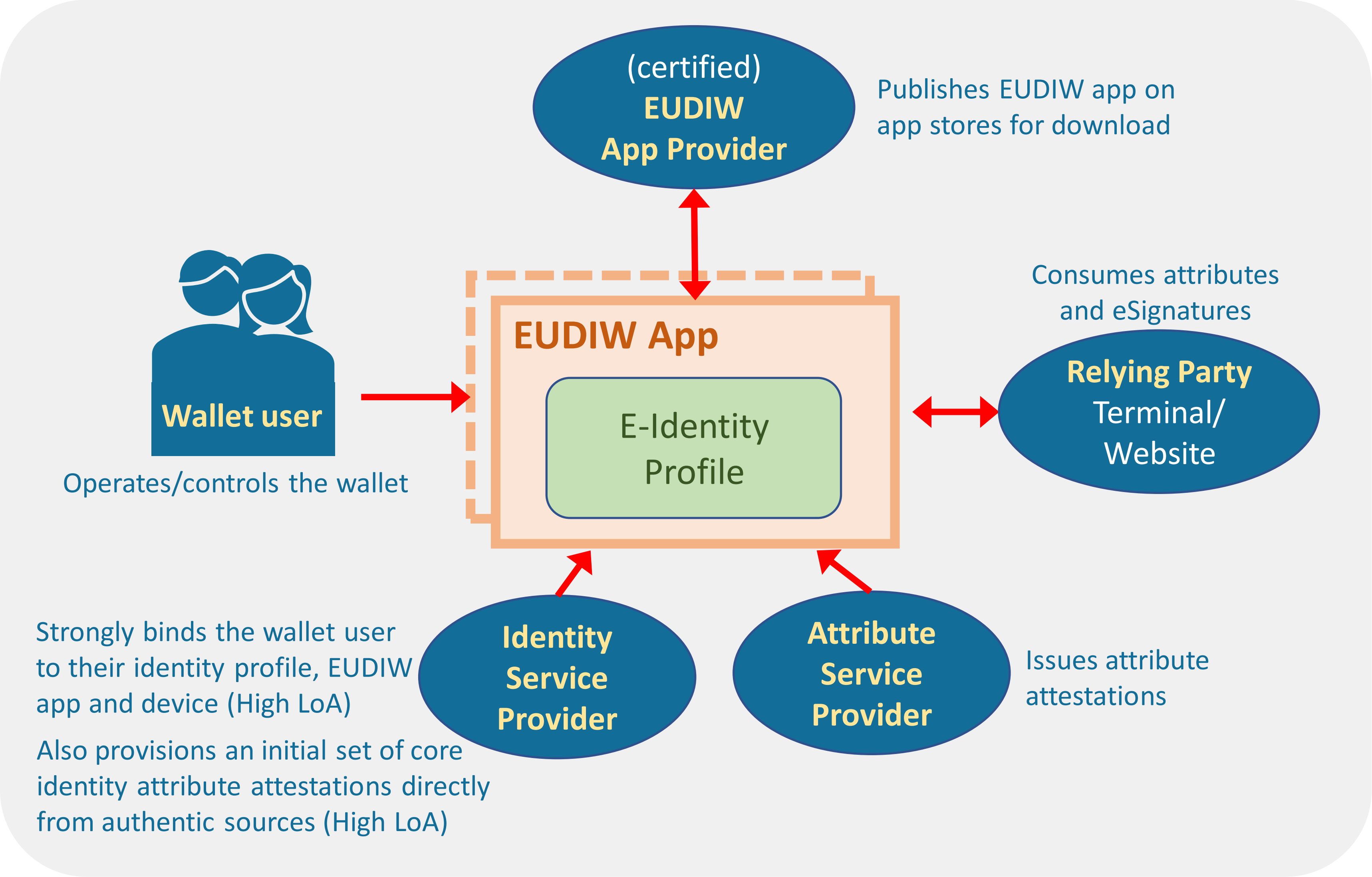
FRANCE PAYMENTS FORUM

Stéphane Mouy
SGM Consulting

The European Digital Identity Wallets (EUDIWs) ecosystem

EUDIWs : 5 Main Actors

All actors operate autonomously within the trust framework



(certified) **EUDIW App Provider**

Publishes EUDIW app on app stores for download

Wallet user

Operates/controls the wallet

EUDIW App

E-Identity Profile

Relying Party Terminal/ Website

Consumes attributes and eSignatures

Identity Service Provider

Strongly binds the wallet user to their identity profile, EUDIW app and device (High LoA)

Also provisions an initial set of core identity attribute attestations directly from authentic sources (High LoA)

Attribute Service Provider

Issues attribute attestations

Stéphane Mouy
SGM Consulting

eIDAS 2.0 (very) preliminary Assessment

Impact on financial sector

FRANCE PAYMENTS FORUM

Stéphane Mouy
SGM Consulting

- (Very) ambitious proposal + tight implementation timeframe

- The EDIW – a near universal digital credential

All key service providers required to accept EDIWs – including 'obliged entities' (banks)

- ➢ 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)

The case for eIDAS 2.0 EUDIWs with payment functionality

FRANCE PAYMENTS FORUM

The overall eIDAS 2.0 paradigm is to move to a user-controlled identity-based ecosystem

Payments are a key part of most wallet ecosystems

Payment-enabling EUDIWs will provide convenience and value to end users

Will strengthen security and sovereignty

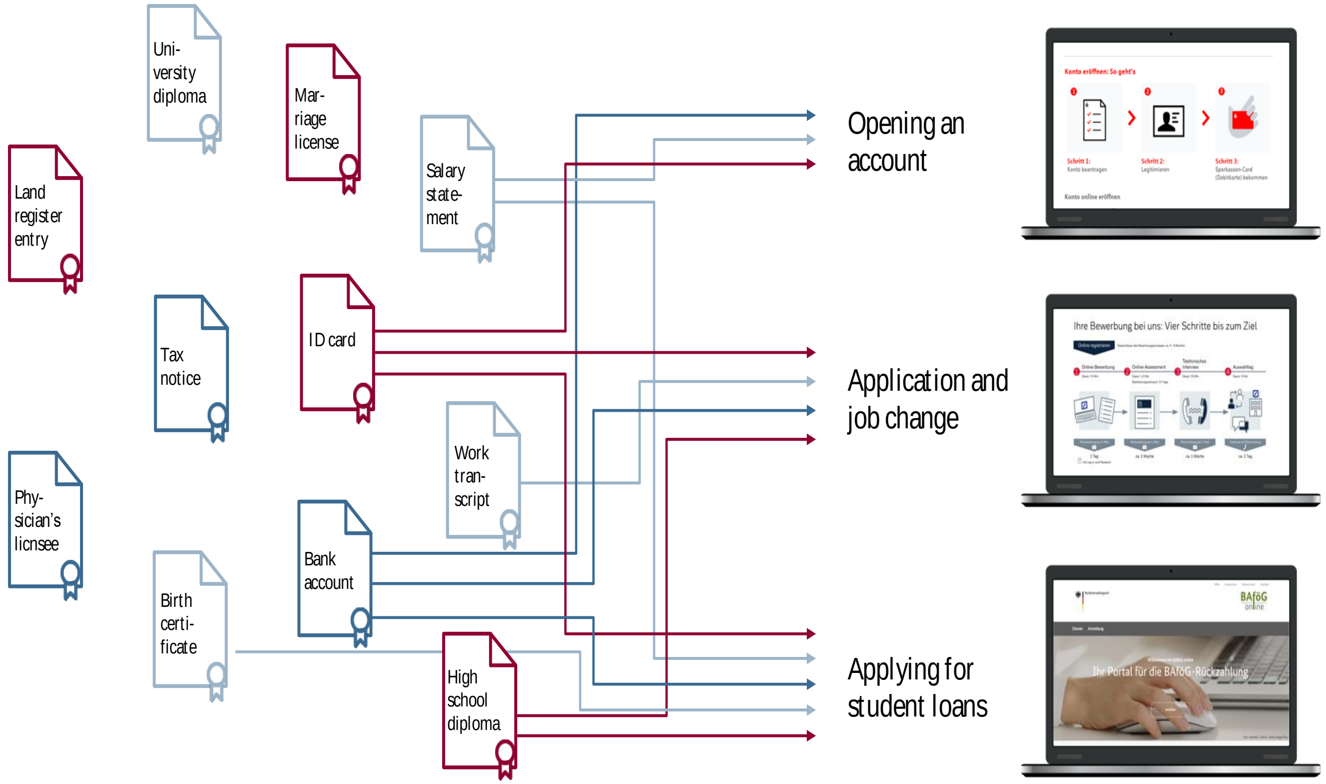
Support for the retail payment strategy and the digital finance initiatives

Will provide support for the digital euro

But overall, there is a recognition that many interactions need to mix financial and other attributes, such as, notably, ID and status attributes.

- Civil & family status
- Professional status
- Licences or eligibility status

This opens the way to new value-added services offered by financial institutions



eIDAS 2.0

WHEN PORTABLE IDENTITY MEETS PAYMENTS

I – THE eIDAS 2.0 PARADIGM FOR EUDIWs

II – LOOKING BEYOND PAYMENT-ENABLING EUDIWs – CBDCs

III – UNDER CONSTRUCTION : THE e-SIGN PAYMENT-AUTHORIZING EUDIW

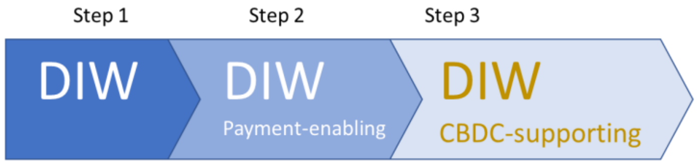
FRANCE PAYMENTS FORUM

Stéphane Mouy
SGM Consulting

Attribute exchanges that are verifiable offline can help 'cash like' CBDC transactions meet AML requirements Whilst maintaining user privacy

FRANCE PAYMENTS FORUM

On the retail side, digital Identity wallets are needed for Central Bank Digital Currencies with EUDIWs generally recognized as suitable tools



Step 1 — DIW

Step 2 — DIW Payment-enabling

Step 3 — DIW CBDC-supporting

eIDAS 2.0-compliant DIW
'Financial grade' (AML/CFT) + SCA

DESIGN CHOICES FOR DIGITAL IDENTITY WALLETS IMPLY MAKING TRADE-OFFS BETWEEN OBJECTIVES BROADLY FALLING INTO THREE CATEGORIES

Privacy

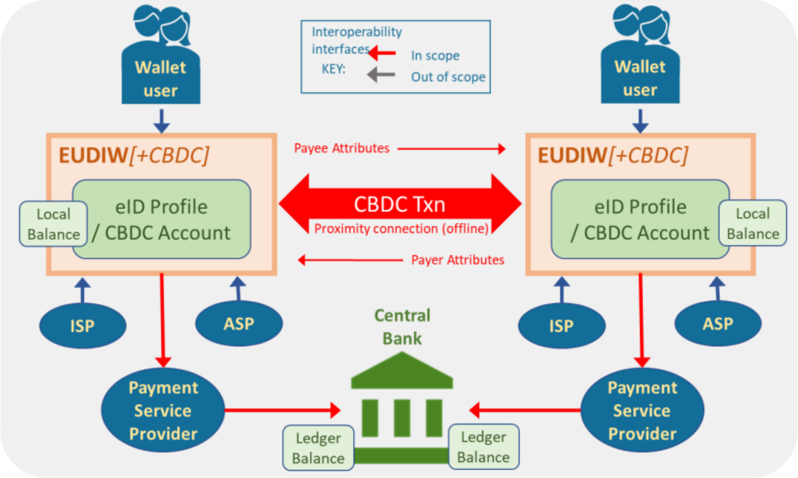
- data minimisation,
- no central monitoring or usage tracking

User experience & interoperability

- Multiple use cases
- **Combine identity, status and other attributes** (including banking) for value-added digital interactions
- **Offline & online** connectivity

Public interest policies (Fraud prevention – AML/CFT)

- High LoA attributes
- e-attested attributes securely linked to mobile phone of wallet user
- Strong Customer Authentication



The ECB has launched the digital euro project in June 2021 but little information has been given on the retail side and key questions remain.

Digital Identity Wallets are a critical step towards CBDCs…

… but offline functionality (proximity connection) is essential

FRANCE PAYMENTS FORUM

Stéphane Mouy
SGM Consulting

Retail CBDCs are already here… (in China)

A tangible reality in China – A widely distributed e-yuan solution now competing with AliPay (Ant Financial) and WeChat Pay (Tencent) but also a key tool for the internationalisation of the Renminbi

The toughest challenge : emulating cash transactions

Key requirements : Legal irrevocability, settlement finality and (at least some) privacy
Offline also key for UX and interoperability

But CBDC exchanges necessarily imply AML/CFT checks and those cannot be meaningfully implemented without some level of identity assurance offered by digital identity wallets.

There is therefore a clear linkage between CBDCs and Digital Identity Wallets – see House of Lords CBDC report (January 2022)

The offline mode brings key benefits but has major implications

- Usage flexibility (internet connectivity often an issue at POS/POI)
- Competes with GAFAM-pay solutions and supports all payment rails (A2
  and card-based)

- Proximity connection protocol (BLE, NFC, QR code) must be specified for EUDIWs
- Difficult to support with blockchain/DLTs
- Today not supported by W3C *Verifiable Credentials* specs

An example of
offline/online interaction

eIDAS 2.0

WHEN PORTABLE IDENTITY MEETS PAYMENTS

I – THE eIDAS 2.0 PARADIGM FOR EUDIWs

II – LOOKING BEYOND PAYMENT-ENABLING EUDIWs – CBDCs

III – UNDER CONSTRUCTION : THE e-SIGN PAYMENT-AUTHORIZING EUDIW

FRANCE PAYMENTS FORUM

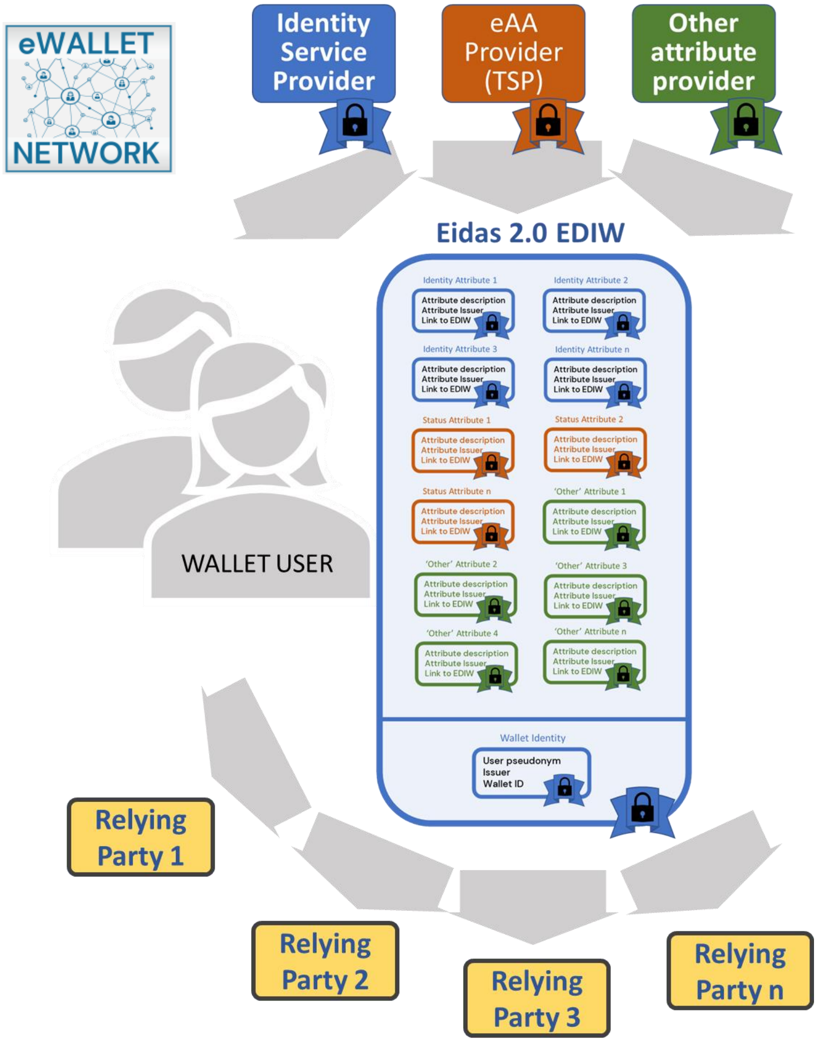
Stéphane Mouy
SGM Consulting

The eWallet Network has worked on a EUDIW design with payment authorisation functionality – and PSD2-compliant strong customer authentication

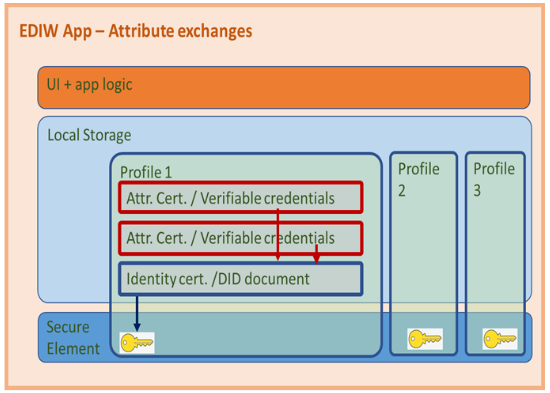
FRANCE PAYMENTS FORUM

Stéphane Mouy
SGM Consulting

Payment-enabling EUDIW – Overview



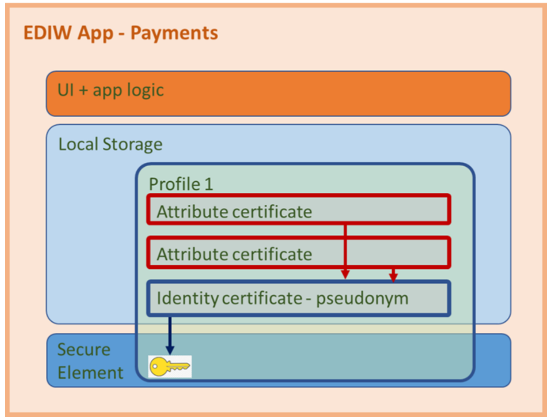
Each attribute (identity attribute, status attribute or other attribute) sectors and borders is evidenced by an **ETSI 319 411-2 qualified certificate** pointing to the wallet identity certificate, which itself is securely linked to the mobile phone of the user



EDIW App – Attribute exchanges
UI + app logic
Local Storage
Profile 1
Attr. Cert. / Verifiable credentials
Attr. Cert. / Verifiable credentials
Identity cert. /DID document
Profile 2
Profile 3
Secure Element

Storage of personal attributes

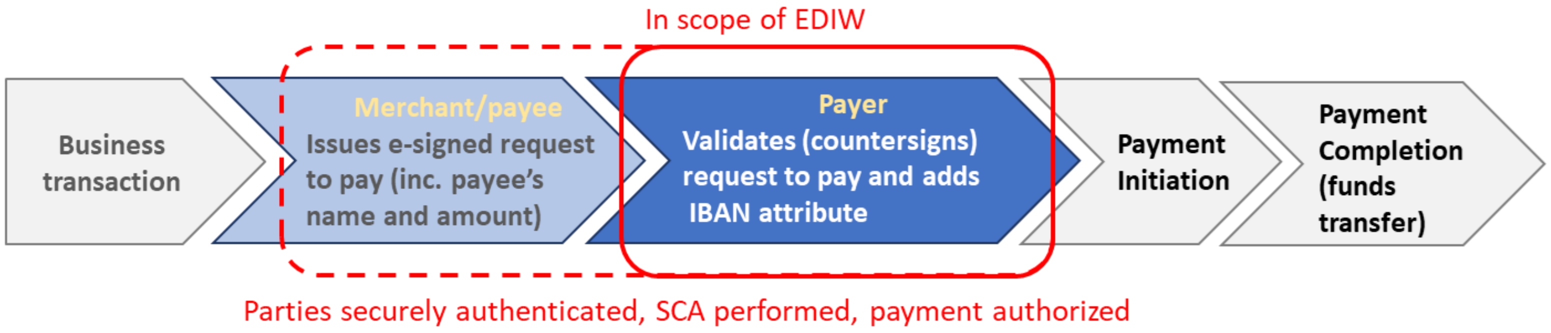
- (Q)SCD to store the private key of a (Q)cert – "identity certificate"
- Storage of additional attribute certificates - "attribute certificates"



The overall wallet architecture is also consistent with the forthcoming ISO Standard 23220-1 (Architecture of mobile eID systems)

Payment-enabling EUDIW – Payment functionalities

The EUDIW operates *before* a payment service provider (or payment initiation service provider) is involved. It securely captures the payer and payee's consents to the payment transaction and once all details have been provided (including IBAN *or* card details), issues a payment instruction that can then be processes by payment service providers in the usual course of business.


In scope of EDIW
Business transaction
Merchant/payee
Issues e-signed request to pay (inc. payee's name and amount)
Payer
Validates (countersigns) request to pay and adds IBAN attribute
Payment Initiation
Payment Completion (funds transfer)
Parties securely authenticated, SCA performed, payment authorized

This is achieved by the EUDI wallet performing 3 key actions

- Connecting the wallet with relying parties both online offline for proximity connections, as is currently the case for card payments and the Apple Pay service;
- Securely authenticating the relying party – and reciprocally having the relying party securely authenticate the wallet user, always in compliance with PSD2 strong customer authentication requirements;
- Securely approving the payment by having the relying party (merchant) issue a request to pay message reflecting its key terms (amount, payee and account details) that is reviewed and approved by the wallet user, and to which the wallet user (the payer or a representative) adds payment details (IBAN or card details) needed to process the payment.

The eWallet Network has worked on a EUDIW design with payment authorisation functionality – and PSD2–compliant strong customer authentication

Stéphane Mouy
SGM Consulting

Payment-enabling EUDIW – Technical overview

- **The EUDIW is in essence a SDO (signed data object) tool allowing**:
  - ➢ Secure online and **offline** interactions between EDIWs and relying parties - with full signature verification
  - ➢ **Countersigning** of payments for legal certainty (full audit trail)
- **All data exchanges with relying parties – irrespective of whether payment related - are treated in the same way**
  - ➢ used for communication of ID attributes and other attributes

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 EUIDW 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

Thank you for your attention

Stéphane Mouy
sgmouy@sgmconsultingservices.com
https://www.linkedin.com/in/stephanemouy/

SGM CONSULTING
Digital transition
expertise for
financial services