SGM CONSULTING

Digital transition expertise for financial services

iproov

NEW EU DIGITAL ID WALLET BRIEFING

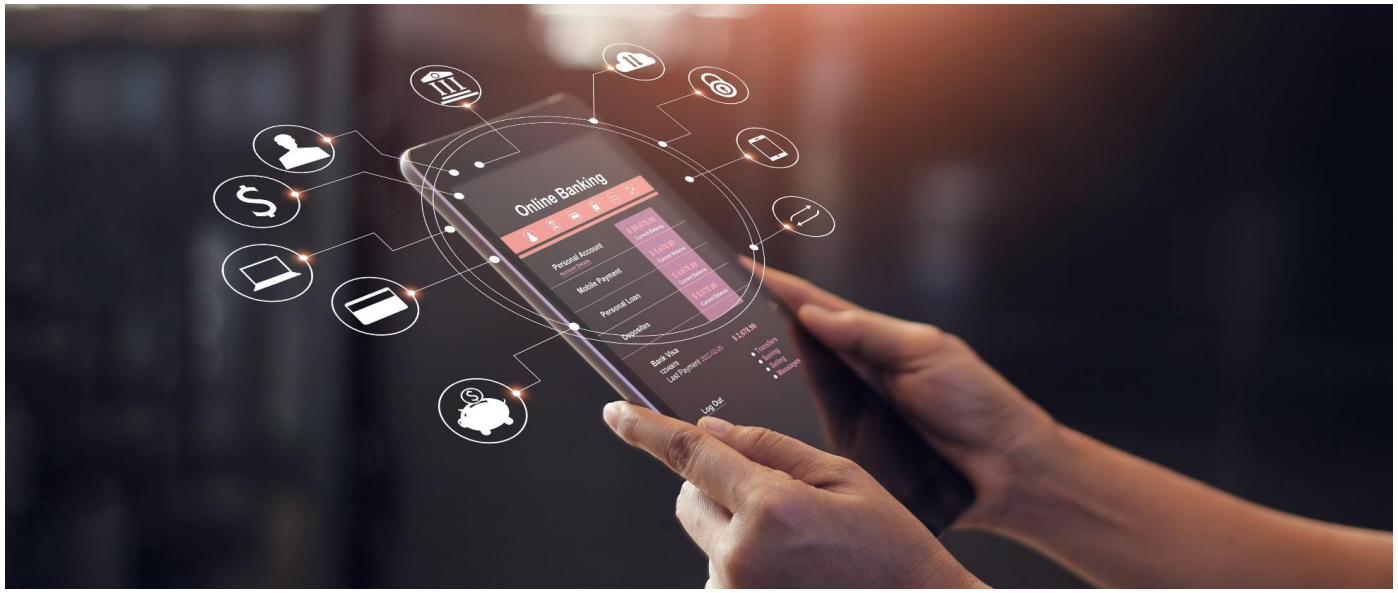
26 April 2022 – iProov

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)

But many banking services imply offline (proximity) connections, especially for POS interactions

Stéphane Mouy
SGM Consulting

EUDIW key specs.

Toolbox approach

MUST-HAVES	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	**WITH STRUCTURAL IMPLICATIONS**
	Must support Strong Customer Authentication requirements (inc. for payment authorisation)	
NICE (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	

First draft of the **European Digital Identity Architecture and Reference Framework document** released in February 2022 – more versions to follow

A major impact on the financial sector

- **(Very) ambitious proposal + tight implementation timeframe**
  - Call for proposals – to be presented in May 2022
  - Multi-stakeholders consortia focusing on pre-production implementation

- **The EDIW – a near universal digital credential**

All key service providers *MUST* accept EDIWs – including AML/CFT *'Obliged entities'* (banks)
  - Core EDIW identity attributes available for CDD purposes (EU AML draft regulation)
  - No need for Obliged entities to reverify identity when receiving EDIW attributes (High LoA)

- **A structural impact on the financial sector**

1. Data providing side : Financial institutions can provide electronically attested attributes on EDIWs (IBAN, account information, etc)
   - Unlikely to imply TSP status – EAAs rather than QEAAs

2. For CDD processes : EDIWs will facilitate KYC/CDD data portability
   - EDIWs are digital alternatives to official ID documents – facilitate customer onboarding
   - EDIWs avoid *Third party reliance* constraints (FATF recommendation 17)
   - Key tool for KYC/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)

4. EDIWs will also help with future retail CBDC deployments
   - CBDCs will need wallets – and robust ID credentials for AML/CFT purposes

EUDIWs

Architecture And Reference Framework Document

(February 2022)

- **Presentation of the eIDAS Expert Group's understanding of EUDIWs**
- **A first draft – not a final version**
- **Main use cases defined**
  - Secure and trusted identification to access online services
  - Mobility and digital driving licence
  - Health
  - Education/diploma
  - Digital finance (customer onboarding & payment authorisation)
  - No need for Obliged entities to reverify identity when receiving EDIW attributes (High LoA)

Not clear how this will relate to ISO standards
- ISO 18013-5 Mobile driving licence
- ISO 23220-1 Architecture of mobile eID systems (draft)

- **Defines key roles in the ecosystem (14 identified)**
- **Defines EDIW functional requirements**
  - Perform electronic identification, store and manage QEAAs and EAAs **locally or remote**;
  - Request and obtain from attestations from providers QEAAs and EAAs ;
  - Provide or access cryptographic functions;
  - **Mutual authentication between the EUDI Wallet and external entities**;
  - Selecting, combining and sharing with relying parties PID, QEAA and EAA;
  - User interface supporting user awareness and explicit authorization mechanism;
  - Signing data by means of qualified electronic signature/seal;
  - Provisioning of interfaces to external parties.

custodial wallet versus non custodial wallet is a critical point to be analysed

*The **mutual identification and authentication** capability shall cover both the EUDI Wallet end and the third party end as, depending on the use case, **the EUDI Wallet may identify and authenticate itself or the user, however it shall be able to identify and authenticate the third party it is interacting with.** Additionally, this mutual identification and authentication shall be **possible both online (over the Internet) and offline.***
(ARF Document – Section 4.4)

- **Outlines other non-functional requirements**
  - eIDAS Article 8 – High LoA
  - Privacy by design, data minimisation, no usage tracking, etc.
- **Outlines potential building blocks for EUDIWs**

EUDIWs

Architecture And Reference Framework Document

(February 2022)

- Presentation of the eIDAS Expert Group's understanding of EUDIWs
- A first draft – not a final version
- Main use cases defined
  - Secure and trusted identification to access online services
  - Mobility and digital driving licence
  - Health
  - Education/diploma
  - Digital finance (customer onboarding & payment authorisation)
  - No need for Obliged entities to reverify identity when receiving EDIW attributes (High LoA)

Not clear how this will relate to ISO standards
- ISO 18013-5 Mobile driving licence
- ISO 23220-1 Architecture of mobile eID systems (draft)

- Defines key roles in the ecosystem (14 identified)
- Defines EDIW functional requirements
  - Perform electronic identification, store and manage QEAAs and EAAs **locally or remote**;
  - Request and obtain from attestations from providers QEAAs and EAAs ;
  - Provide or access cryptographic functions;
  - **Mutual authentication between the EUDI Wallet and external entities**;
  - Selecting, combining and sharing with relying parties PID, QEAA and EAA;
  - User interface supporting user awareness and explicit authorization mechanism;
  - Signing data by means of qualified electronic signature/seal;
  - Provisioning of interfaces to external parties.

custodial wallet versus non custodial wallet is a critical point to be analysed

*The **mutual identification and authentication** capability shall cover both the EUDI Wallet end and the third party end as, depending on the use case, **the EUDI Wallet may identify and authenticate itself or the user, however it shall be able to identify and authenticate the third party it is interacting with.** Additionally, this mutual identification and authentication shall be **possible both online (over the Internet) and offline.***
(ARF Document – Section 4.4)

- Outlines other non-functional requirements
  - eIDAS Article 8 – High LoA
  - Privacy by design, data minimisation, no usage tracking, etc.
- Outlines potential building blocks for EUDIWs

Thank you for your attention

Stéphane Mouy
sgmouy@sgmconsultingservices.com

SGM CONSULTING
Digital transition expertise for financial services