

PAYMENTS WITH HIGH PRIVACY, SECURITY AND VERSALITILY

THE [Q]eAA POTENTIAL FOR EUDI WALLETS

6 June 2024

The European Digital Identity (EUDI) Wallet – a digital Swiss army knife

The payment use case is not yet fully specified

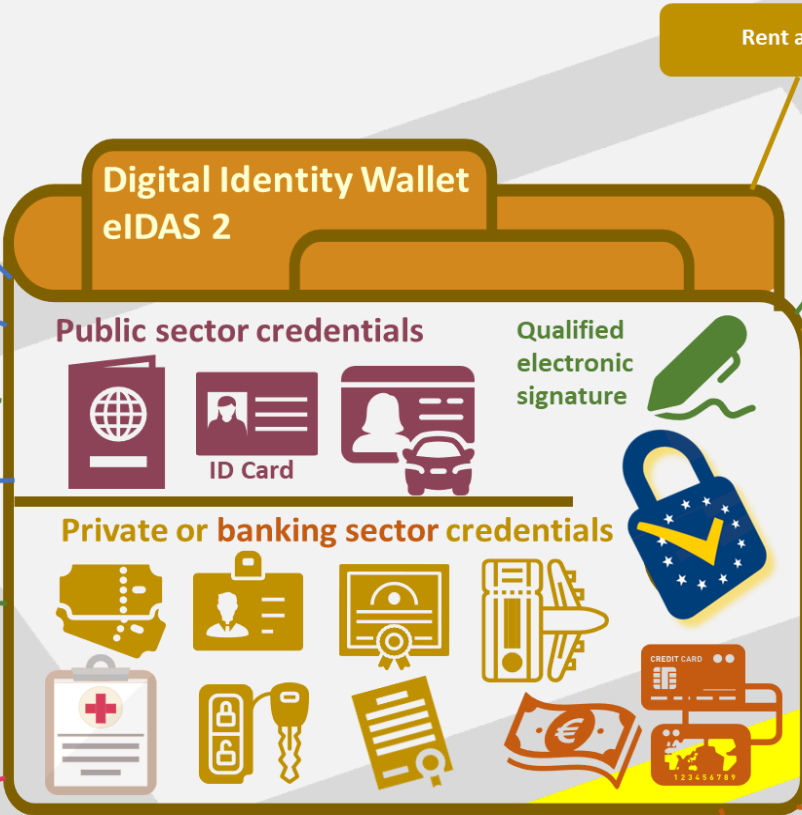
...But may well be the killer use case of EUDI Wallets

Public sector use cases

- Show passport/ID card
- Show driving licence
- Sign tax form
- Implement admin process
- Sign a public contract
- Access health file or medical records

Private or banking sector use cases

- Rent a car
- Sign a contract
- Book a flight
- Apply for school or university course
- Make online purchases
- Communicate in a secure way
- Rent a house/hotel room
- Open a bank account
- Authorise an online or offline payment
- Tomorrow, hold and manage CBDCs?



CAUTION CAUTION CAUTION CAUTION

When digital identity meets payments...

...eIDAS meets PSD2/PSR (Payment Services Regulation)

And it can get *really* complicated



The eIDAS2 regulation is enacted, yes..

But many implementing acts are still to be released

And the future Payment Services Regulation is not finalised

UNDER CONSTRUCTION UNDER CONSTRUCTION UNDER CONSTRUCTION

EUDI Wallets and Payments

A critical but
challenging
use case

- eIDAS2 regulation now enacted, but much uncertainty remains regarding the technical implementation of EUDIWs
- **Private-sector interactions are key** for EUDI Wallets acceptance and deployment
 - key service providers 'required to accept' EUDI Wallets
- **Payment use case – by far the largest (huge ecosystem)**
 - Critical for EU citizens and huge impact but very specific
- **Payment interactions are:**
 - **Very diverse** (A2A, Cards, Direct Debits, P2P, PoS, etc.)
 - **Technically challenging** and subject to very specific processes (card or SEPA schemes – e.g. instant payments)
 - **Highly regulated** – PSD2 and future PSR
- For payments, **security and fraud prevention are very important but user convenience is absolutely essential**
- The **NOBID and EWC Large-Scale Pilots** work on the payment use case but not much has emerged yet...

*Union citizens and residents in the Union should have the right to a digital identity that is under their sole control [...]. To achieve that aim, a European digital identity framework should be established allowing Union citizens and residents in the Union to **access public and private online and offline services throughout the Union** (eIDAS2 - Whereas 5)*

*Payments make use of the **Risk-Based Approach** principle*

- *Identify and assess the risks associated with products, services, customers and geographic areas of operation.*
- *Implement risk mitigation measures proportionate to the identified risks,*

Illustration : low risk exemption for Strong Customer Authentication under PSD2

This is different from the High LoA approach of EUDI Wallets

- PID and eAAs are **electronic attestations stored and managed by EUDI Wallets**
- **PID** – identity attributes issued by PID issuers in compliance with High Level of Assurance
- **eAAs** – attributes issued by any third party. Can be identity attributes, status attributes or other attributes – no inherent limitation
- Whilst eAAs are not specified and therefore not necessarily trustworthy, **Qualified eAAs (QeAAs) are ‘guaranteed attestations’ legally equivalent to paper-based attestations**
- **QeAAs are eAAs issued by Qualified Trust Service Providers (QTSPs)** with access to authentic sources and subject to stringent identity-proofing requirements

European Digital Identity Wallet means an electronic identification means which allows the user to securely store, manage and validate person identification data (PID) and electronic attestations of attributes (eAAs) for the purpose of providing them to relying parties and other users of European Digital Identity Wallets; (eIDAS2 - article 3.42)

Differences between QeAAs and PID

- PID have narrower purpose : ‘establish the identity of a natural or legal person’
- Issuers of PID designated by member States
- Communication of PID subject to LoA High requirements
- Public sector relying parties may require PID only

Member States shall ensure that measures are taken to allow QTSPs to verify by electronic means at the request of the user, the authenticity of the following attributes against the relevant authentic source [...]

- Address; Age; Gender; Civil status; Family composition;
 - Nationality or citizenship;
 - Educational or professional qualifications, titles and licences;
 - Powers and mandates to represent natural or legal persons;
 - Public permits and licences;
 - For legal persons, **financial and company data.**
- (eIDAS2 – Annex VI)*

EUDIW in payment interactions

SUA/SCA role for payments

- Reference to payments in eIDAS2 is through **Strong User Authentication (SUA)**
 - the term is meant to imply Strong Customer authentication (**SCA**) for payments
- **SUA/SCA for payments (PSD2 & future PSR)**
 - Required for most payments above 50€
 - Implies ‘dynamic-linking’, an extra secure cryptographic SCA for internet payments
 - **Huge legal impact – with SCA payment is ‘deemed authorized’ and liability shifts from Payment Service Provider to payer**
- **Banks are legally responsible for SCA**
 - will that change when SCA is implemented by the EUDI Wallet?
 - **Draft Payment Services Regulation (PSR)** to be adopted in 2025 hints that PSR technical rules will have to be adjusted to reflect role of EUDI Wallets

*Where private relying parties that provide services [...] are required by Union or national law to use strong user authentication for online identification [...] including in the areas of banking, financial services, those private relying parties shall [...] and only upon the voluntary request of the user, also accept **European Digital Identity Wallets** [...]. (eIDAS2 - article 5f2)*

*The European Banking Authority shall review and, if appropriate, update the regulatory technical standards on a regular basis in order, inter alia, to take account of innovation and technological developments [...] and the **EUDI Wallets** (Draft PSR - article 89)*

Addressing SCA and offline interactions viewed as critical for EUDI Wallets

May 2024 2nd eIDAS Call for Proposals

Wallets for Payments and Banking

The wallet addresses payment and banking relevant functionalities [...] providing a standardised process for using the wallet to complete Know-Your-Customer, **Strong Customer Authentication, and offline transactions and processes** across the EU;

EUDIW in payment interactions

The challenge remains considerable

- **An EUDI Wallet payment use case. Key must-haves**
 - **Integrity** of payment messages + **legal irrevocability** of payment authorizations > e-signature is a solution
 - ***Who did what when?*** - Robust audit trail needed
 - **Offline connectivity** for PoS and P2P interactions
- **Identity plays an increasing role in payments**
 - Digital interactions combine identity and payment attributes
 - AML/CFT requirements for payments converge on LoA 'Substantial' (AML Regulation)
 - And 'verification of payee' requirements impose an identity verification (IBAN name check)
- **Identity versus anonymity : framing the debate**
 - Payment interactions are no longer fully anonymous. Real identities must be 'disclosable'.
 - But payment interactions should protect privacy and prevent usage tracking
 - Ongoing debate for CBDC. How can digital euro payments be partially anonymous?
 - No obvious answers today...

Where is this leaving us? 3 Preliminary conclusions

The Strong User Authentication of EUDI Wallets is a critical functionality for payments

- **But not yet fully specified by the ARF and not reflected in the PSR**
- **Format mDoc, W3C VCs, X509s?**
- **Will it work offline?**

Banks are obvious candidates for QEAs as they are the 'authentic source' of the attested information

- **IBANs and other payment credentials**
- **Good financial standing attestations**

Will they seize the opportunity?

Smoothly integrating the SUA/SCA ceremony into scheme processes and open banking APIs is a challenge but will prove key to adoption

**After a short introduction leaving more
open questions than definitive answers...**


**Here comes a more practical illustration of what
can be done with QEAs for payments**

EUDIW in payment interactions

Using eAAs and QeAAs to meet the payment challenge

QEAA can be included within a payment instruction representing both debtor and creditor

- Removes the need for the actual IBAN or card number to be included (which are trackable)
- Binds the name to the account to provide an offline verifiable 'Verification of Payee' (Confirmation of Payee)


Identity of Debtor/Payer

```
<CustomerCreditTransferInitiation>
...
<PaymentInformation>
...
<Debtor>
  QEAA
</Debtor>
<DebtorAccount>
  QEAA
</DebtorAccount>
...
<CreditTransferTransactionInformation>
...
<Amount>
  <InstructedAmount Ccy="EUR">20.00</InstructedAmount>
</Amount>
...
<Creditor>
  QEAA
</Creditor>
<CreditorAccount>
  QEAA
</CreditorAccount>
</CreditTransferTransactionInformation>
</PaymentInformation>
</CustomerCreditTransferInitiation>
```


Identity of Creditor/Payee

DEMONSTRATION: Merging payments and identity within the same procedure

EUDIW in
payment
interactions

Using eAAs and
QeAAs to meet
the payment
challenge

Quali-Sign Demo

https://qsl-demo.appspot.com/DemoMerchant

DemoMerchant
Checkout

In cooperation with **eWALLET NETWORK**

Demo **Go Back**

Merchant: Prepare the payment (+identity) request

Amount: 0.00 Currency: EUR Payment Method: A2A (instant) **Next**

Request additional attributes [optional]

Proof of Age [18 or over]: Not required

Loyalty Programme Membership: Not required

Forename: Not required

Surname: Not required

Residential Address: Not required

E-Mail Address: Not required

Cellphone Number: Not required

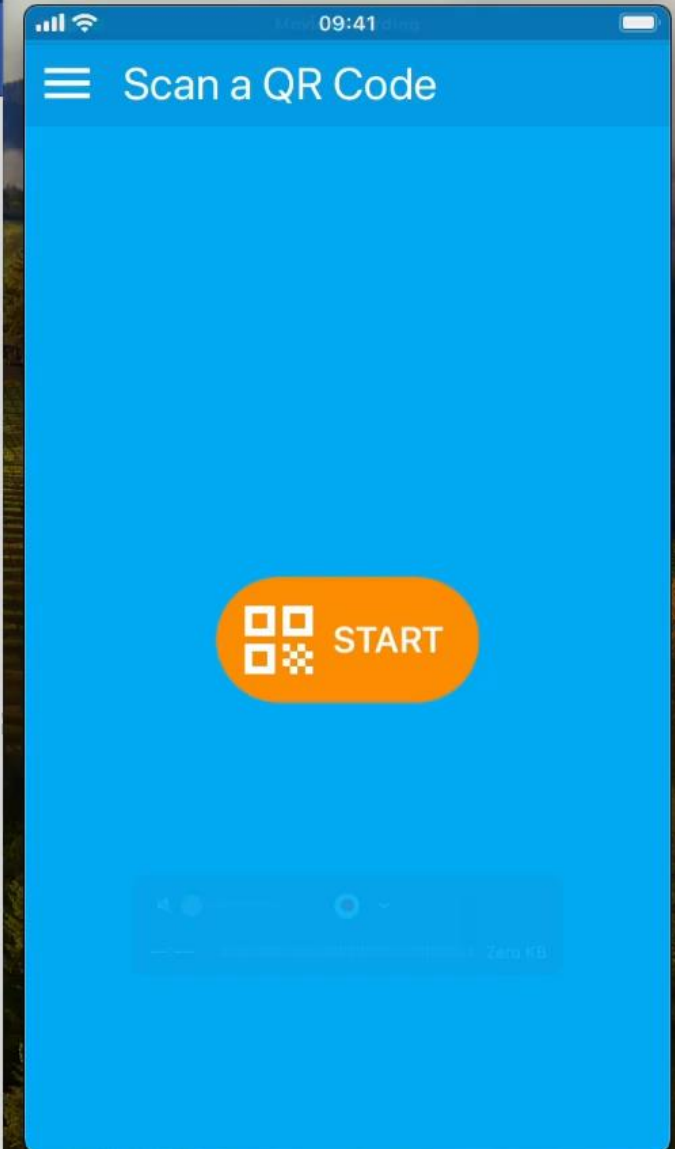
Request Countersignature Mode

Detached Countersignature

Enveloped Countersignature

Enveloped countersignatures are not supported if attributes are requested. They are also not supported in the case of CBDC payments.

©2024 Quali-Sign Ltd



Any questions?

Thank you for your attention

Stéphane Mouy

sgmouy@sgmconsultingservices.com



Michael Adams

Michael_adams@quali-sign.com

