



The Road to EIDAS 2.0 Payment Wallets

An example implementation of a European Union Digital Identity Wallet

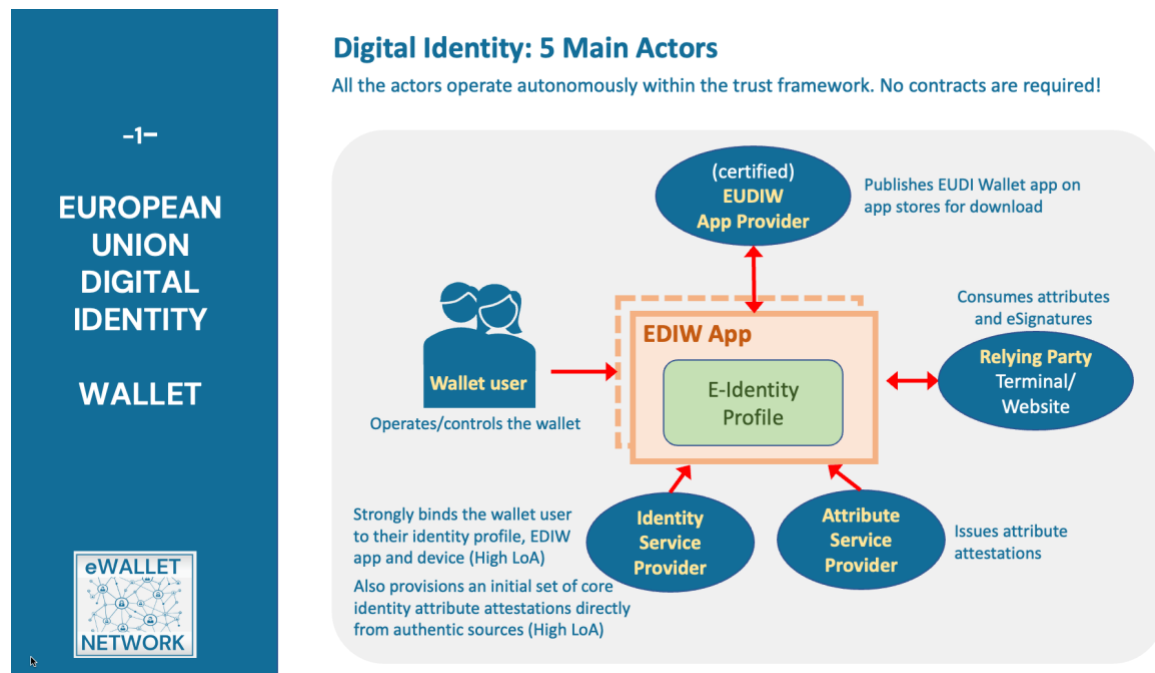
OIX Workshop
29th March 2022

Michael Adams
michael_adams@quali-sign.com
www.quali-sign.com

I am Michael Adams of Quali-Sign, we are a mobile app developer focussing on payments and identity. We have built a prototype Digital Identity Wallet, based on an approach advocated by the e-Wallet Network, which is a group of European identity and payments experts.

The ambition of eIDAS 2.0 is for every European citizen to have access to a (reusable) digital identity wallet which can be used online and offline to authenticate, present attributes, create qualified electronic signatures and authorise payments.

Our proposed approach is closely aligned to the eIDAS expert group's Architecture Reference Framework (ARF) Outline and implements some of the interoperability standards that are being considered by the expert group.



To begin with, let us describe the main actors that will participate in the proposed European Union Digital Identity Wallet (EUDIW), based the eIDAS 2.0 trust framework.

Firstly, we have the person that will install the wallet app on their smartphone. The wallet is certified at country level and is issued by a wallet app provider.

Within the wallet, the person can operate one or more identity profiles. So, for example, they can segregate their personal and business lives as well as potentially managing profiles for a child or elderly relative.

The Identity Service Provider (ISP) is the issuer of identity profiles. They are responsible for binding a real person to their electronic identity, so that we can be sure that the person touching the fingerprint sensor is either the holder of the identity or permitted to operate it.

A wallet identity profile only becomes useful when it holds attributes for the user to present. The ISP is therefore also responsible for provisioning the person's core identity attributes (and chains of trust) to their wallet, ideally from authentic sources, such as government departments.

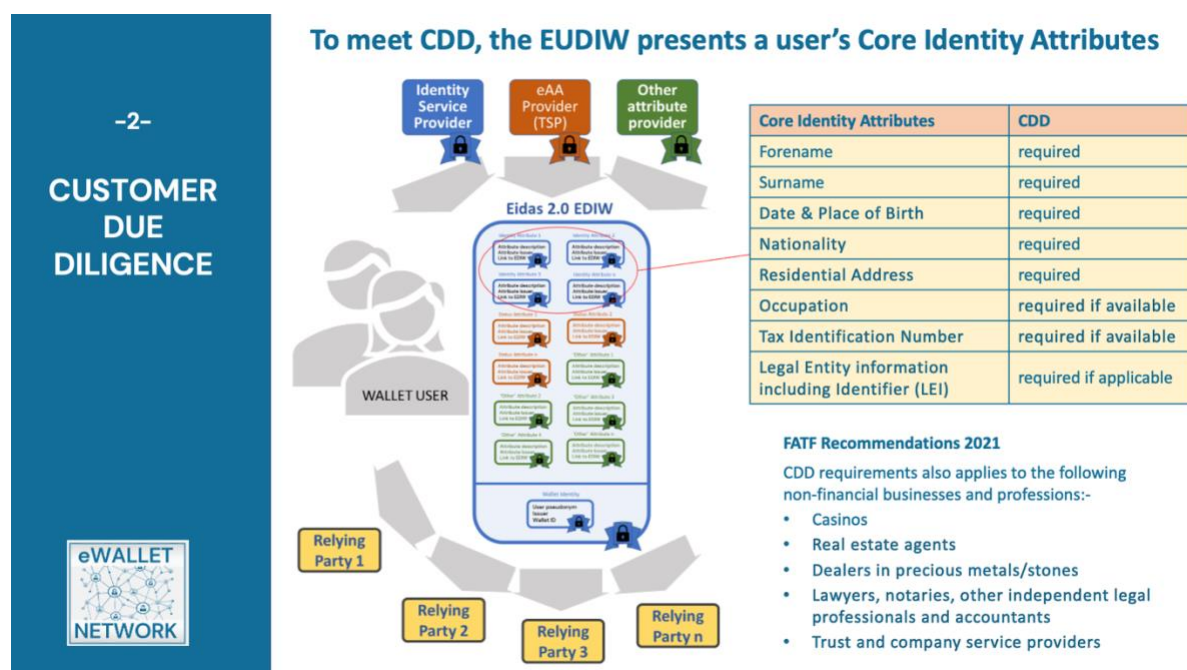
If the person wishes to load additional attributes from other sources into their wallet, they can procure these directly from Attribute Service Providers (ASPs). These could range from electronic car keys, cinema or flight tickets or a hotel room booking that would allow them to bypass reception and open the door to their room. Furthermore, to support the payment use case, banks and card issuers may also issue IBAN & card attribute attestations. More on this later.

Neither the ISP nor other attribute providers have any visibility of the other attributes that the person loads into their wallet. All the attributes are held locally on the device, in the custody of the holder (no need for a GDPR data controller).

Relying Parties are the consumers of the person's attributes and cover a multitude of use cases which can include authenticating with a third-party website, signing a contract, presenting a driving license or covid status, authorising a payment at a Point-Of-Sale (POS) or Point-Of-Interaction (POI) and passing through a turnstile.

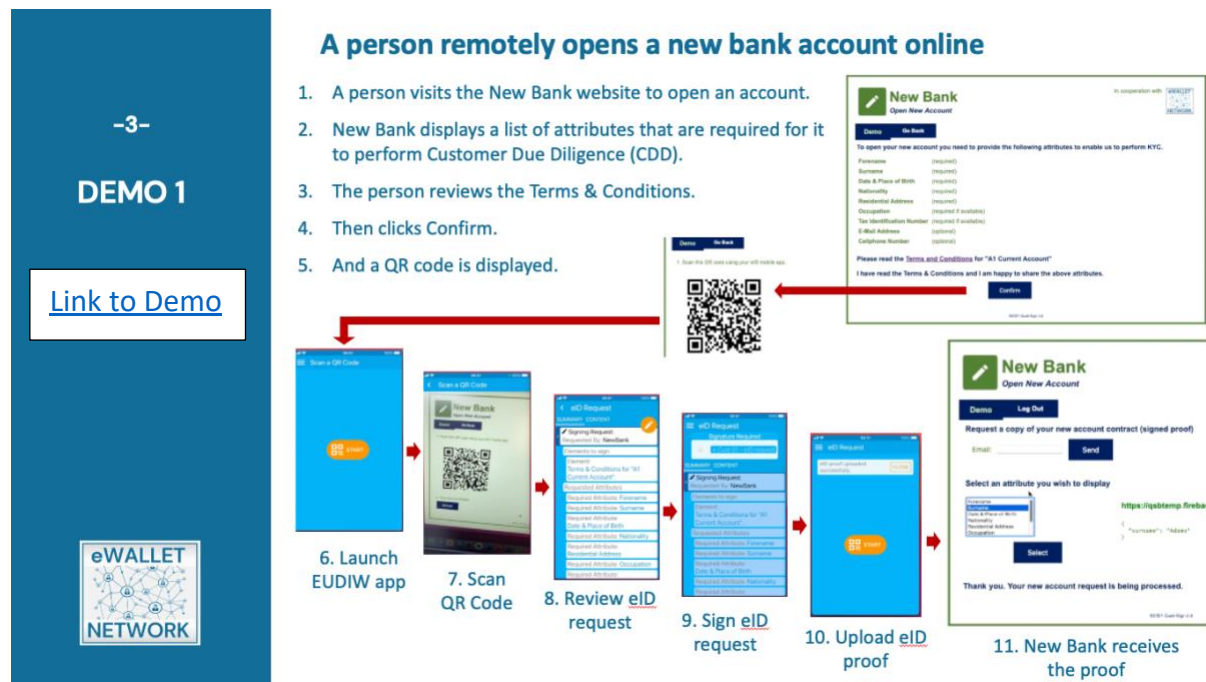
The wallet communicates directly with the Relying Party so that none of the other actors have any visibility of the interaction. Further privacy by design mechanisms ensure that nobody can track the user as they move between websites, or as they travel on public transport or move from shop to shop.

This approach follows Self Sovereign Identity principles.



Customer Due Diligence (CDD) must be performed by Financial Institutions (FIs), and other obliged entities, as per Financial Action Task Force (FATF) Recommendations. These obliged entities must obtain and verify a set of core identity attributes before, for example, when entering into a new business relationship. You can see some of these attributes on the slide.

CDD can be seen as one of the main drivers behind the need for an EUDIW.



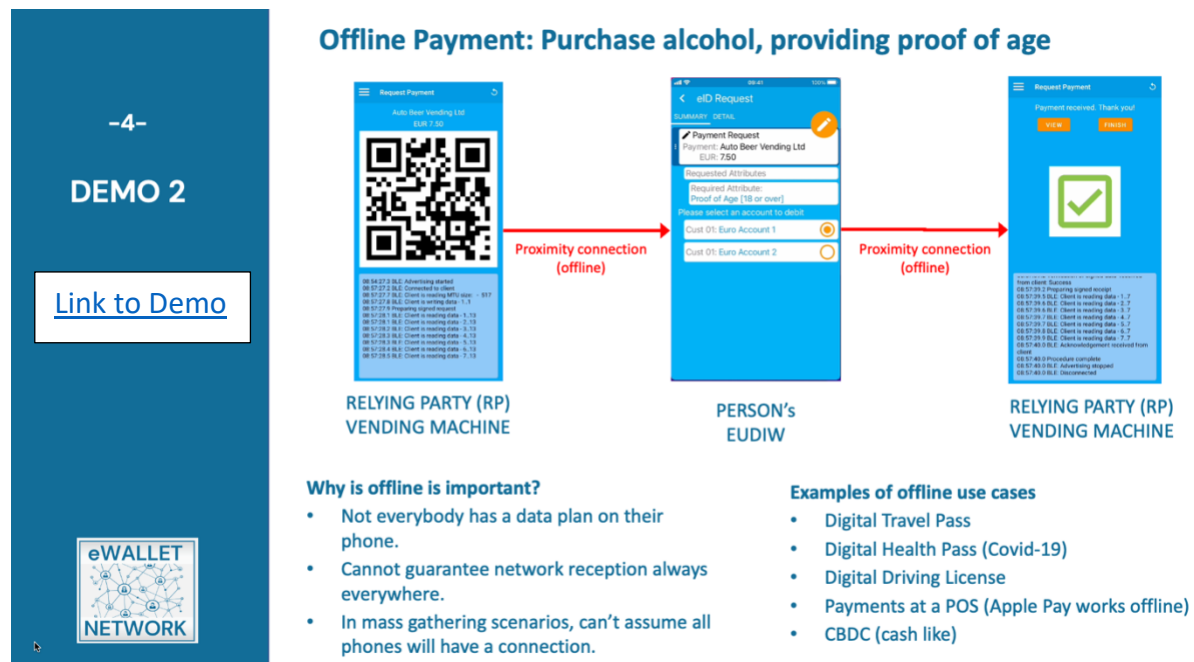
In 2021 we produced this CDD demo for the EU funded eIDAS iBanking Project. It shows a person opening a bank account remotely, potentially with an FI in different member state.

On its website, NewBank lists the CDD attributes that it requires and asks the person to review and accept the account terms and conditions.

It then displays a QR code which it asks the person to scan with their EUDIW. The wallet establishes a secure connection to NewBank and downloads an eID request, signed by NewBank.

The EUDIW verifies the signature to authenticate NewBank, before presenting the request to the user. The user agrees to supply the requested attributes and signs the T's & C's with a single touch of the fingerprint sensor.

NewBank then receives and verifies the user's countersignature, which includes the requested attributes, and proceeds to open the customer account.



An important eIDAS 2.0 requirement is that the eID procedure must be capable of operating offline. This includes situations where either the wallet or the terminal or both are offline (i.e., without an internet connection). In these situations, the devices will communicate via proximity technologies such as BLE or NFC. To achieve this, both devices (EUDIW and Terminal/POS/Vending Machine) must be capable of verifying the signature of the other party offline.

As mentioned in the ARF, The EUDIW must authenticate the Relying Party before sharing potentially sensitive personal data. And the terminal needs to verify the user signature including the supplied attributes before allowing them to pass through a turnstile or releasing the goods at a point of sale. It is important to note that Apple Pay does not require the smartphone to have an internet connection.

I'll now show you a combined eID/payment procedure being performed between two devices, both of which are offline. Each device fully verifies the signature and certificate chains of the other. This is made possible because the chains of trust for both parties are stored locally on each device. Only by doing this allows both parties to fully verify the transaction offline.


Offline verification is identical to that performed online with one exception. When online, the real time certificate revocation status of each certificate can be checked. This is the only compromise.

The demo simulates the purchase of alcohol at a vending machine. The procedure starts with the vending machine preparing a Request-To-Pay which includes attribute attestations representing the payee and their account. A proof of age attribute attestation is also requested. The signed request is transmitted to the EUDIW and verified before being displayed to the user. The user reviews the request including the amount and the payee. They proceed to select an IBAN or card attribute and then authorise the payment. The

user's proof of age attribute is automatically included in the approval signature. The procedure is completed with a signed receipt being returned to the wallet.

-5-

AML REGULATION



AML Funds & Crypto Transfer Requirements are challenging for PSPs

The EUDI Wallet provides the solution

Consider the following two scenarios:

- A person visits a Bureau de Change kiosk to exchange cash (any amount) e.g., from \$ to €.
- Or a person visits a money transfer website (amount > €1,000).

Before the Payment Service Provider can initiate the transaction, they must obtain and verify the attributes listed below.

| | Attributes required [For transfer of funds & crypto assets] | Payer PSP must verify | Must be supplied [Within EU] | Must be supplied [Outside of EU] |
|-------|--|--------------------------|---------------------------------|-------------------------------------|
| Payer | Payment Account Number or Unique Transaction Identifier | > €1,000 or Cash | With transfer | With transfer |
| Payer | Name | > €1,000 or Cash | On request | With transfer |
| Payer | Legal Entity Identifier (if applicable) | > €1,000 or Cash | On request | With transfer |
| Payer | Address | > €1,000 or Cash | > €1,000 On request | > €1,000 |
| Payer | Official Person Document Number | > €1,000 or Cash | > €1,000 On request | > €1,000 |
| Payer | Customer Identification Number or Date and Place of Birth | > €1,000 or Cash | > €1,000 On request | > €1,000 |
| Payee | Payment Account Number or Unique Transaction Identifier | | With transfer | With transfer |
| Payee | Name | | On request | With transfer |
| Payee | Legal Entity Identifier (if applicable) | | On request | With transfer |

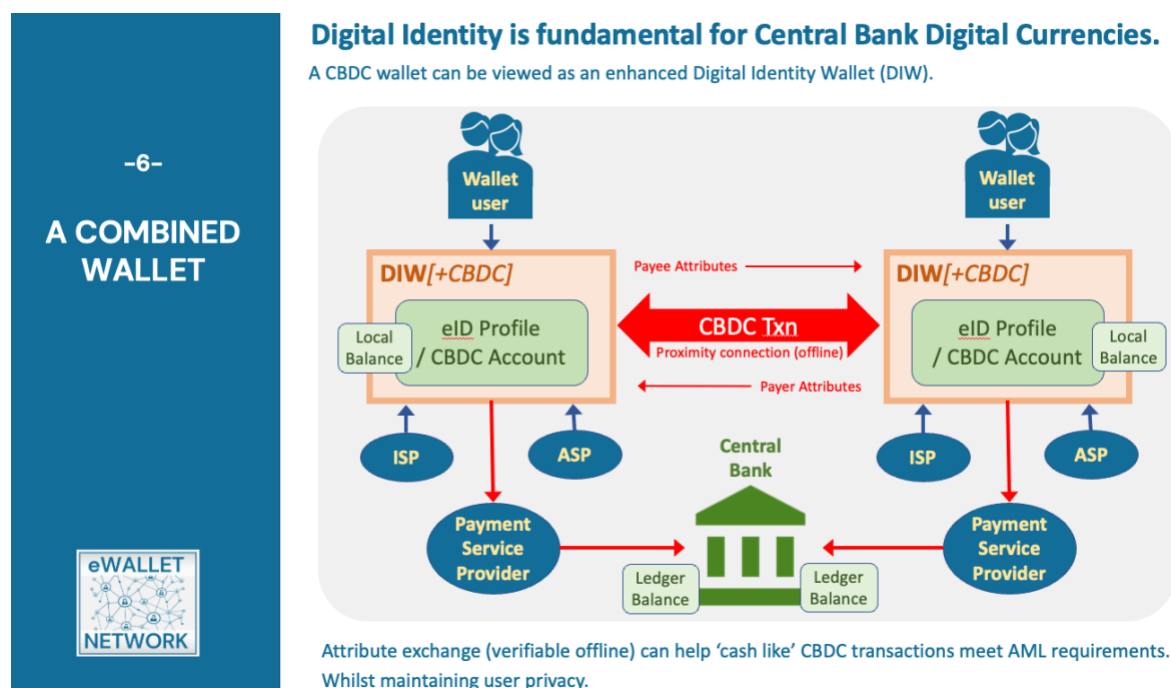
Especially beneficial for customers who visits a kiosk or website once, never to return!

The EUDIW is also highly relevant to the Anti-Money Laundering (AML) and Countering Financing of Terrorism (CFT) requirements with respect to the transfer of funds and crypto assets.

The requirement to capture and verify attributes is particularly challenging for Payment Service Providers (PSPs) whose customers may only transact with them once.

However, using an EUDIW, the procedure becomes simple and highly efficient.

I list on the slide the attributes required by the EU's new AML regulations. Also of note is that transfers in and out of the EU require these attributes to be included with the payment instruction.



Finally, we are seeing the worlds of Identity and Payments come together, not least with the forthcoming introduction of Central Bank Digital Currencies (CBDC).

A CBDC wallet can be viewed as an enhanced Digital Identity Wallet, based upon Self Sovereign Identity principles. The balance is held against the public/private key representing the holder's identity profile. CBDC transactions will also require the exchange of identity and attribute attestations, in order to meet AML requirements.

With CBDC, one of the most ambitious objectives is to mimic physical cash (i.e., the notes and coins in your pocket). This involves digital cash being transferred between two wallets offline with finality. Any funds received can immediately be re-spent, even before the wallet goes back online.

As you have just seen from the previous demo, there really are no technological impediments to providing an offline capable identity wallet. Extending this to include the transfer of digital cash is only a small additional step.

Thank you!

END.