EPSG European Payments Stakeholders Group

# A Taxonomy of Digital Wallets

INNOET 01-07-2025

# Executive Summary

These slides aim to provide a preliminary taxonomy for digital wallets and include a brief overview on the following topics

| | | | | |
|---|---|---|---|---|
| High Level definitions 1. | Scope of the Taxonomy 2. | Generic Architecture 3. | Classification of wallets 4. | Differences within wallets 5. |
| Typical Payment Flow 6. | Use Cases 7. | Relevant regulations 8. | Conclusions 9. | |

**As stated in the Conclusions section:**

- Functionality of digital wallets is steadily increasing and moving away from being a simple container mimicking a card
- Consequences of opening up digital wallets for cards, open banking, digital euro, stable coins backed and unbacked crypto creates a multi-faceted narrative with greater NFC accessibility
- There are now changing business models, variety of vendors, applications/use cases, merchant types, differing services and the mobile device which now acts as a soft POS itself – what is the risk of interconnection in the next 5-10 years?

# High Level Definitions

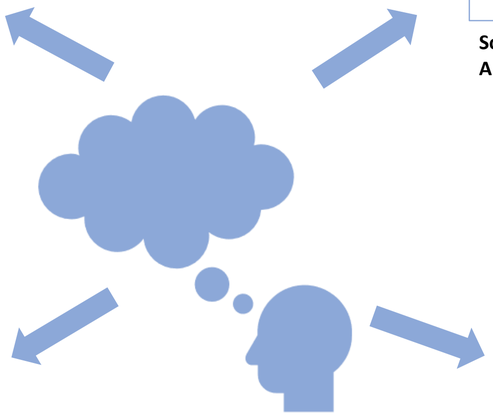
There is a wide variety of definitions for digital wallet, where the primary purpose is payment methods container/facilitator.

"**digital wallet**, also known as an **e-wallet** or **mobile wallet**, is an electronic device, online service, or software program that allows one party to make electronic transactions with another party bartering digital currency units for goods and services. This can include purchasing items either online or at the point of sale in a brick-and-mortar store, using either mobile payment (on a smartphone or other mobile device) or (for online buying only) using a laptop or other personal computer. Money can be deposited in the digital wallet prior to any transactions, or, in other cases, an individual's bank account can be linked to the digital wallet. Users might also have their driver's license, health card, loyalty card(s) and other ID documents stored within the wallet. The credentials can be passed to a merchant's terminal wirelessly via near field communication (NFC)."

**Source: Wikipedia**

***"A digital wallet is an interface to interact with and manage verified data and digitised assets securely".*** This definition reflects the broadened functionality of digital wallets beyond mere financial transactions, encapsulating their role in managing a diverse range of digital assets and personnal data.

**Source : Beyond Payments: Navigating the Next Generation of Digital Wallets A report from Mobey Forum's Digital Wallet Expert Group (2024)**



**A digital wallet is a software-based system** that securely stores **users' payment information and passwords** for numerous payment methods and websites. It enables its users to make transactions electronically, often through a mobile device.
With a digital wallet, users can complete purchases easily and quickly with near-field communications technology. It can also store loyalty cards, identification documents, receipts, and even tickets to events or transportation.
Digital wallets can be linked to the individual's bank account or can be loaded with money to make transactions. They offer convenience and can often be secured with advanced security measures like encryption and two-factor authentication, making them a popular choice for transactions both online and in physical stores.

**Source: ChatGPT**

"Digital wallets **are applications that store digital objects** in way as physical wallets do. Many of us are already using digital wallets on our smartphones to store our boarding passes or to keep our virtual bank cards"

**Source : Q&A Digital Identity | Shaping Europe's digital future (europa.eu)**

## Proposal for a generic EPSG definition:

**A digital wallet is a software-based system that securely interacts and manages verified data and digitised assets such as payment credentials and/or identity credentials. When the digital wallet embeds payment credentials, it can be used for remote and/or in-store purchases. It's designed to offer a convenient and secure method for consumers to make purchases using a digital device, most commonly a smartphone. Some digital wallets allow users to store credit or debit card information securely, while others may include more comprehensive features like online shopping and contactless payments.**

# Scope & key working assumptions

## Digital Wallet

This taxonomy only considers digital wallets that provides at least one payment feature. The payment credential used for this purpose can refer:

- either to a payment instrument (such as a card or a payment account)
- Or to money itself, i.e. Digital Euro

☑ In the scope of this taxonomy

☒ Out of scope of this taxonomy

## Digital Identity Wallet EUDIW

This taxonomy introduces the questions a Digital Identity wallet could reveal aside the digital wallet when they are complementary used.
There is no assumption about the distinction or conjunction between the wallet operator involved.

☑ In the scope of this taxonomy

## Custodial Wallet

This terminology refers to the ownership of the private keys of the end user. In a custodial wallet, the storage and the management of the private keys are under the responsibility of third party which is not the end user. In such a case, the ownership of the digital asset is fully dependent on the third party provider. In the payment industry, custodial wallets are nevertheless explored, as a way to allow programmable money or programmable/recurring payments.

☒ Out of scope of this taxonomy

# Generic Architecture (from a Digital Wallet Operator perspective)

Each Digital Wallet Operator (DWO) deals with a general architecture which involves the integration of several different components and services

## Application (Client)

The application component is the set of subcomponents that make up the application that users interact with.
This component includes:

1. **SDKs and software** are internals and core of the application.
2. **User Interface (UI)** is the front-end of the application that users see. It implements the user experience and is designed to be user-friendly and intuitive.
3. **Security features:** local protection against retro-ingineering and dynamic analysis, security of the device, especially in order to enhance the efficiency of the 2 factors authentication mechanism.
4. **APIs** are used between the Application (Client) and the wallet server, in order to ensure the synchronicity of the services and UX/UI with the backend server databases.
5. **Notification Service:** This service sends users important notifications, such as transaction confirmations, balance updates, or fraud alerts.

## Wallet Server

This is the back-end of the application that processes transactions, manages user data, and communicates with other services. The server is responsible for functions such as transaction processing, security checks, user authentication, and data encryption.
This component includes:

1. **Database:** The database stores user account information, transaction history, and other relevant data. It's crucial that this data is stored securely to protect users' sensitive information.
2. **Security module:** This component handles all the security aspects, including data encryption, fraud detection, and user authentication. This module may use technologies like SSL/TLS for secure data transmission, two-factor authentication (2FA) for user verification, and tokenization for secure payments.
3. **APIs** are used to integrate the wallet with external services and allow the wallet to send and receive data from them, back-to-back. In payments, for instance, these include services offered by banks, Card networks and merchants.

**This is a general view, and the specifics can vary depending on the digital wallet operator, the technologies used, and the specific features and services provided by the wallet.**

# Classification of Wallets - Definitions

## Pass-Through Digital Wallet

Transactions initiated using **Pass-Through Digital Wallets transmit the customer's payment credential (usually tokenised) to the merchant**, who then processes the transaction directly with their acquirer like any other card payment transaction.

- Apple Pay, Google Pay, Samsung Pay, Wero, MB Way
- Issuers' Wallets | Blik, Revolut, N26
- Merchants' Card on File/ Credential on File

## Staged Digital Wallet

Unlike Pass Through Wallets, staged digital wallets use multiple stages to complete the transaction between the customer and the merchant and especially make a difference between the funding stage and the payment stage. The **transaction is processed within the Staged Digital Wallet's proprietary network** which implies that the payment credential of the customer is not shared with the merchant.

- PayPal, Klarna, Vipps

## Stored Value Digital Wallet

Stored Value Digital Wallets also use multiple stages to complete the transactions, except that:

- the **prefunding of the wallet account** is a prerequisite for the user before being able to initiate any transaction.

- Burn Digital Loyalty Programs
- PayPal, Paysafe

**Notes: 1.Each Click-to-Pay Solution (per each Scheme Brand) could also be considered as a specific kind of Pass-Through Digital Wallet.**
**2.The brands referenced in these slides are non-exhaustive examples provided solely to support comprehension of the content.**

# Types of Wallets



1. **Device-Based Digital Wallets:** These wallets typically use Near Field Communication (NFC) or Magnetic Secure Transmission (MST) to facilitate contactless payments at physical stores. They may also support online payments. They are generally secured with biometrics or a passcode.

2. **Online Wallets:** These wallets provide a secure and quick way to pay for online purchases without needing to enter card details for every transaction. They may support one-click checkout, recurring payments, and often offer buyer protection features.

3. **Cryptocurrency Wallets:** These wallets provide the ability to send, receive, and manage balances of various cryptocurrencies. Advanced features may include the ability to interact with decentralized apps (dApps), participate in staking, or swap between different cryptocurrencies.

4. **Bank Wallets:** These wallets often allow users to manage their bank accounts, view transaction history, make transfers, and pay for purchases. Additional features may include the ability to deposit checks through the app, set up direct debits, or split bills with contacts.

5. **Merchant Wallets:** These wallets are typically tied to a loyalty program, allowing users to earn points or rewards for purchases. They may feature order-ahead functionality, personalized offers, and the ability to manage gift cards.

6. **P2P Wallets:** These wallets allow users to send and receive money from contacts, often without any fees. They may also support group payments, request money feature, or the ability to split bills.

7. **Cross-Border Wallets:** These wallets allow users to send money to different countries, often supporting multiple currencies. They may offer competitive exchange rates, low transfer fees, and the ability to track transfers.

**Many digital wallets contain a combination of these features and are not limited to a single category.**

**For instance, PayPal is an online wallet, but it also supports P2P transfers and can be used for in-store payments in certain locations.**

# Different features within digital wallets

## Ownership types

- Bank lead wallet e.g. ViPPS, Wero
- European association: Cross-wallet interoperability e.g. EMPSA
- Merchant led e.g Amazon or consortium
- Fintech / independent e.g. Satispay, Lydia

## Types of payment enabled

- P2P
- In store
- Online using mobile web
- Online App (potential white label) or no app
- Cross-border

## Initiation technology use

- NFC
- QR Codes
- one-time use code (e.g. Blik code)

## Acceptance Scope

- Retail Specific
- Multiple retailers

## Payments instrumented supported

- Account to account
- Card
- Multiple networks or specific ones
- Crypto
- Digital Euro

## Holding of funds

- Pass-through digital wallets
- Staged digital wallet
- Stored Value digital wallets

## Holder other nonpayment related

- Identity/drivers license
- Loyalty
- Transit tickets
- Hotel reservations
- Messaging apps

## Form Factor

- Mobile
- Watch
- Browser-based

# Classification of wallets – Main characteristics (1/2)



| | Pass-Through Digital Wallet | Staged Digital Wallet | Stored Value Digital Wallet |
|---|---|---|---|
| **Functionalities** | • Acceptance Network: DW can be used widely<br>• Channel : NFC, Ecomm, In app<br>• Cross-border | • Acceptance Network: DW can be used widely<br>• Channel : NFC, Ecomm, QR<br>• Can be crossborder | • Acceptance Network: DW can be used at one or more Merchant<br>• Channel : NFC, Ecomm, QR<br>• Can be crossborder |
| **Use cases** | • Payment<br>• Travel<br>• Loyalty<br>• Entertainment<br>• Access (digital key for cars) | • Payment (e.g may be chosen when consumer doesn't want to share card details with merchant. ) | In most cases, the funds used are earned through a closed loop:<br>• Payment<br>• Loyalty program<br>• Cashback reward<br>• Discount on purchase made through the wallet |
| **Governance drivers** *(from a Scheme perspective)* | **Depends on each Payment Scheme policy and can be different from one Scheme to another:**<br>• Digital Payment Credentials Policy (e.g. Tokenisation Program)<br>• Specific AML/LCLF risks on the Merchant<br>• Ability to intermediate a Third Party such as a Payment Facilitator | | • Shall the DWO have an EMI License? |
| **Contractual aspects** *(from a DWO perspective)* | • Contract DWO/ Acceptor**: No**<br>• Contract DWO/ Acquirer: No<br>(**there is a direct contract through the Acquirer with the Acceptor**)<br>• Contract DWO / Funding Issuer: Yes<br>• DWO Statement to the DW User : Merchant label as known by the Payment Scheme<br>• DWO Statement to the Merchant : Banks Customer as known by the Payment Scheme | • Contract DWO / Acceptor: **Yes**<br>• Contract DWO / Acquirer: **Yes** (DWO is seen as an Acceptor)<br>• Contract DWO / Funding Issuer: No<br>• DWO Statement to the DW User : Merchant Label as known by the DWO<br>• DWO Statement to the DW Merchant : User account as known by the DWO | • Contract DWO / Acceptor**: Yes * (White Label Options)**<br>• Contract DWO / Acquirer: Yes (DWO is seen as an Acceptor)<br>• Contract DWO / Funding Issuer: No<br>• DWO Statement to the DW User: Merchant label as known by the DWO<br>• DWO Statement to the Merchant : User account as known by the DWO |
| **Payment Credentials Management** | • **The DWO manages a User account**. There are underlying payment credentials linked to this user account under DWO responsibility. **These underlying payment credentials are securely shared with the Merchant** (usually tokenized as required by the Payment Scheme rules/Payment Network processing).<br>• Bank Statement to Banks Customer: Acceptor of a payment is the merchant<br>• Bank Statement to the Acceptor : End User of a payment is the Banks customer | • **The DWO manages a User account** which can share user data with the merchant. There are underlying payment credentials linked to this user account under DWO responsibility. **These underlying payment credentials are never t shared with the merchant**. .<br>• Bank Statement to Banks Customer : Acceptor of a payment is DWO (plus sometimes an addition of the merchant label known by the Payment Scheme)<br>• Bank Statement to the Acceptor : End User of a payment is DWO | • **The DWO manages a User account** which can share user data with the merchant. There are underlying payment credentials linked to this user account under DWO responsibility. **The sharing of underlying payment credentials with the Merchant depends on Payment Scheme rules.**<br>• Bank Statement to Banks Customer : Acceptor of a payment is DWO<br>• Bank Statement to the Acceptor : End User or the DWO or Payment Credential |

# Classification of wallets – Main characteristics (2/2)



| | Pass Through Digital Wallet | Staged Digital Wallet | Stored Value Digital Wallet |
|---|---|---|---|
| **Transaction Processing** *(from a Scheme perspective)* | Uses the Payment Scheme Network only | Uses both the Payment Scheme Network and the proprietary network of the DWO | Is often a closed loop wallet : uses the proprietary network of the DWO |
| | • The credentials (cards, account) underlying the payment are directly used (pass through). | • 2 successive transaction types :<br>○ Purchase: DWO uses the user account to pay the merchant. (Merchant label, wallet balances are under the responsibility on the DWO). No sharing of the underlying payment credentials with the Merchant.<br>○ Funding: Back-to-Back Funding transaction (or Purchase driven load or real time load) :**Merchant name as known by the Payment Scheme** | • 2 successive transaction types :<br>○ Funding: (ad hoc funding, not linked with a simultaneous purchase). Under its policy, a card scheme may forbid the back-to-back funding option for this category of Digital Wallet. (From a scheme perspective, the Merchant Name is the DWO name)<br>○ Purchase: DWO uses the user account to pay the merchant. (**Merchant name, wallet balances are under the responsibility on the DWO**). No sharing of the underlying payment credentials with the Merchant. |
| **Acceptance Mark** | • Dispute resolution is provided by the Payment Scheme<br>• Payment Scheme Brand and, for ecommerce only, the DWO brand | • Dispute resolution is provided by the DWO<br>• DWO Brand | • Dispute resolution is provided by the DWO<br>• DWO Brand |
| **User Identity** | | Verified at the account sign up | Verified at the account sign up |

- Best in class UX/UI are prioritised (through biometrics (FaceID/TouchID) or device pass code (e.g. Android devices).
- Wallet user Identity is managed as the customer of the DWO. It is out of scope of PSD/RTS. What are the AML requirements for a DWO ?
- The Organization who hosts the DWO may also handle other businesses (eg device manufacturer, proprietary OS platform and/or proprietary browser) which provide the ability to check the user identity, per or cross devices. How is the Data Act involved ?
- **EUDIW Regulation to be seen as an alternative/mandatory option for DWO ? Also true for PSP and/or Payment Schemes involved in Digital Wallet processing ?**

| | | | |
|---|---|---|---|
| **Payment SCA** | For each payment transaction – Performed by the Issuer | For each transaction – Either performed by the Issuer (Back to back Funding) or by the DWO (Purchase) | For each transaction – Performed by the DWO or by the Issuer (ad hoc Funding) |

- PSD and RTS are the relevant regulations with specific requirements on Issuer side
- The authentication of a payment mean is also governed by each Payment Instrument Scheme rules

# Typical Digital Wallet payment flow

1. **Wallet Initialisation/Enrolment:**
   - The user installs and opens a digital wallet app on their smartphone or digital device.
   - For the first time, they need to add their credit/debit card or bank account details into the wallet. Some wallets allow adding multiple payment methods.
   - Verification / authentication steps to ensure the security of the user's information including identification of the payer, authentication of the payer.

2. **Transaction Initiation:**
   - When a user wants to make a payment, they open their digital wallet and choose the payment method they want to use (if multiple methods are added).
     - For online transactions, the user selects the digital wallet as the payment option at the checkout page, then authenticates the payment.
     - For in-store transactions, when the initiation technology is NFC, the user typically brings their device near the Point-of-Sale system, then authenticates the transaction using a passcode, fingerprint, or face ID.
     - When the initiation technology is QR-code/one-time code, the UX/UI is different but also consistent in both contexts (online and instore transactions).

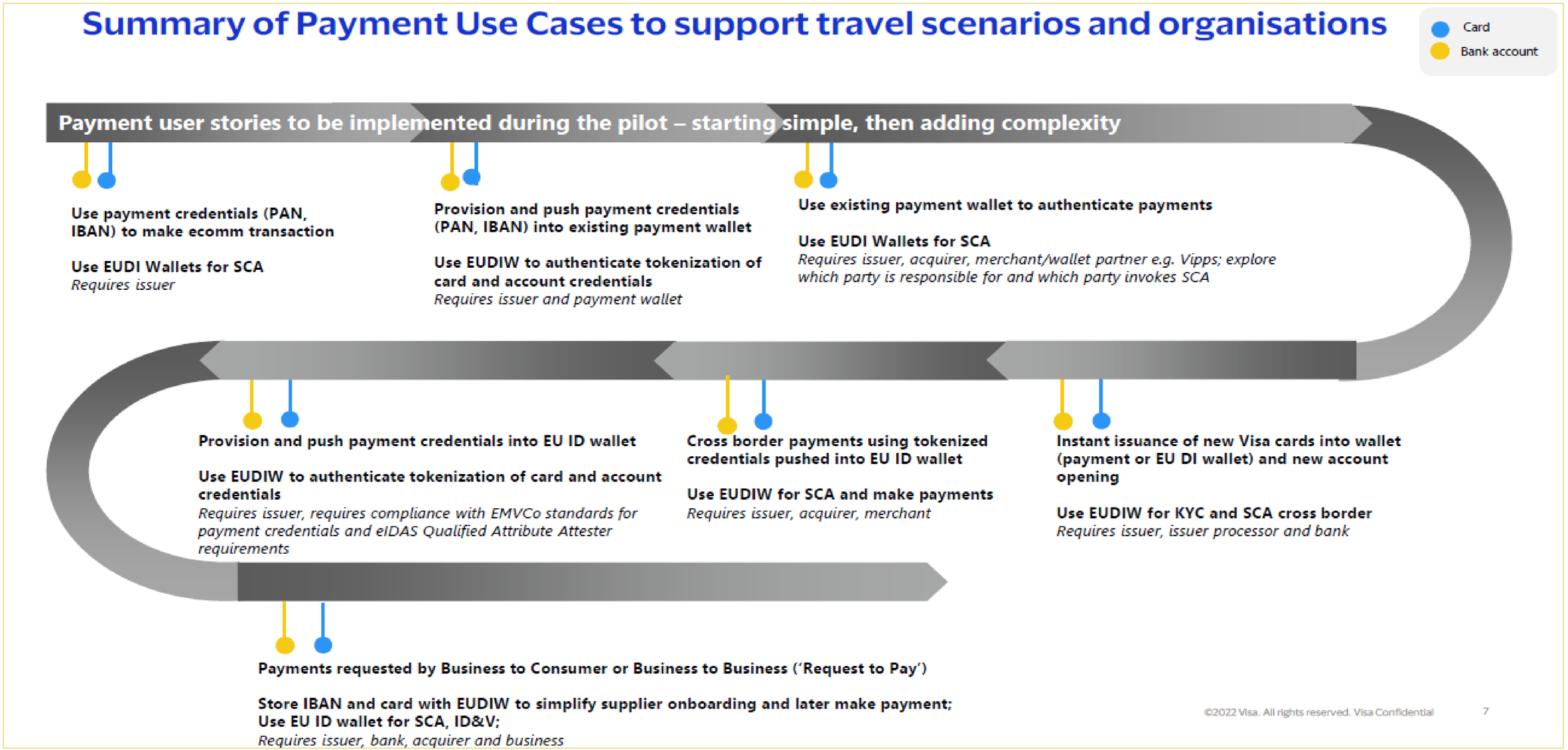
3. **Transaction Processing:**
   - Once the user has authenticated the transaction, the digital wallet sends a token to the merchant that represents the user's credit/debit card or bank account. This token is a random string of characters that does not contain the actual card or account details, which keeps the user's information secure.

4. **Payment Authorisation:**
   - The merchant submits the token to the payment processor, which then contacts the user's bank or card issuer.
   - The bank or card issuer verifies the transaction, then sends back an approval or denial.

5. **Transaction Completion:**
   - If the transaction is approved, the payment processor sends the approval back to the merchant, who completes the sale.
   - The user's account is then debited for the amount of the sale.
   - The user receives a notification or a receipt in their digital wallet app confirming the transaction.

**Specifics of this process can vary depending on the digital wallet being used, the payment method, and the merchant's payment processor.**

# Example of payment flow for Digital ID wallet



# Payment Use Cases

Digital wallets have multiple use cases that have transformed traditional methods of payment. Here are some common use cases:

1. **Online Shopping:** e.g. PayPal, Google Wallet, and Amazon Pay
   - secure online purchases without entering card details for every transaction.

2. **In-Store Payments:** e.g. Apple Pay, Google Pay, and Samsung Pay
   - contactless payments in physical stores using NFC technology.

   e.g., Blik
   - One-time code technology

   e.g., Wero
   - QR-code technology

3. **Peer-to-Peer Payments:** e.g., Venmo and Cash App
   - send and receive money from friends and family, often without any additional fees.

4. **Bill Payments:**
   - payment of utility bills directly from the app. Eliminating the need to write checks or visit multiple websites to pay various bills.

5. **Subscriptions and Recurring Payments:**
   - manage subscriptions and recurring payments, such as gym memberships or streaming services.

6. **Travel and Transportation:**
   - book flights, trains, or buses, and even to pay for ride-hailing services like Uber, car/bike sharing services, electric vehicle charging.

7. **Charity Donations:**
   - donate to charities and non-profit organizations.

# Non-payment Use Cases

Digital wallets have multiple other use cases that do not cover types of payment. Here are some common use cases:

1. **Rewards and Loyalty Programs**:
   - integrated rewards programs. Users can earn points or cash back for purchases, which can then be redeemed for goods or services.

2. **Identity Verification**:
   - incorporating ID storage, allowing users to securely store and present identification documents.

3. **Cryptocurrency Transactions**: e.g. Coinbase Wallet and Metamask
   - store, buy, and sell cryptocurrencies.

# Digital Wallets are popular and big tech wallets are under scrutiny



- MEPs back plans for an EU-wide digital wallet (February 2024)

- In UK, a competition investigation is on his way :
  - **2018:** PSR launched investigations in order to understand what Contactless Mobile Payments are
  - **November 2023** : FCA launched a call for input Potential competition impacts from the data asymmetry between Big Tech firms and firms in financial services
  - **July 2024** : PSR and FCA launch joint call for information on big tech and digital wallets.

    > **Target** : collect evidences on :
    - Ranges of benefits that digital wallets bring for service users
    - Whether there are any features that payment means don't work as well as they could for consumers and/or businesses
    - Their role in unlocking the potential of A2A payments and how they could impact competition between payment systems
    - Whether digital wallets could raise any significant competition, consumer protection or market integrity issues either now or in the future.

# Relevant European Regulation: PSD3 general classifications

What can be a digital wallet operator and which payment services does the digital service handle?

## PSPs types

**PSD3 intends to merge payment rules applicable to any PSPs especially considering**

- The Payment Services Directive 2 (PSD2) which contains rules on authorisation and supervision of payment institutions (PIs) and establishes conditions for the relationship between all payment service providers (including EMIs) and payment service users
- The E-Money Directive (EMD) which contains rules on authorisation and supervision of e-money institutions (EMIs).

## PSD3 Definitions

PSD 3 will define “funds”, “payment account” and “payment instrument” and detailed rules on how competent authorities must enforce the rules, including a list of breaches for which specific sanctions must be in place

| | |
|---|---|
| Funds | ‘Funds’ means central bank money issued for retail use, scriptural money and electronic money; |
| Payment account | An account held by a payment service provider in the name of one or more payment service users which is used for the execution of one or more payment transactions and allows for sending and receiving funds to and from third parties; |
| Payment instrument | An individualised device or devices and/or set of procedures agreed between the payment service user and the payment service provider which enables the initiation of a payment transaction; |
| Payment Services | Annex I which provides the list of business activity referred as ‘payment service’ will have to evolve. BNPL services are in principle to be regarded as loans (Credit Directive), but they are in PSD3 scope if BNPL is provided in conjunction with payment services (Recital 35). |

## Fee Regulation

Regulation on interchange fees for card-based payment transactions also caps interchange fees charged between banks for card-based transactions, which indirectly affects digital wallets that facilitate such transactions.

# Relevant European Regulation: Anti Fraud measures



EU PSR also introduces a raft of new measures designed to prevent or reduce payments fraud.

**Verification of payee**

- PSR requires a payee's PSP to verify, on the request of the payer's PSP, whether the unique identifier (e.g., an IBAN) and the name of the payee matches with those details supplied by the payer, and to communicate the outcome of such verification to the payer's PSP. Where the relevant details do not match, the payer's PSP is required to notify the payer of any such discrepancy prior to the payer finalising the payment order and the execution of the credit transfer. However, the payer can decide whether to proceed with the credit transfer despite any discrepancies identified.
- These requirements are broadly like the UK's confirmation of payee requirements and will require PSPs that execute or receive credit transfers for payers or payees to put in place additional procedures.

# Relevant European Regulation: Strong Customer Authentication

**EUDI Wallet intends to manage the authentication/identification for all sectors at the horizontal level but does not aim to regulate the liability for specific sectors**

## EU Digital Identity Framework

**Art 5f2**

- When private relying parties that provide services are required by law to use strong user authentication for online identification or where strong user authentication for online identification is required by contractual obligation (eg : transport, energy, banking financial services), **those private relying parties shall, no later than 36 months from the date of entry into force of the implementing acts referred to in Article 5a(23) and Article 5c(6) and only upon the voluntary request of the user, also accept European Digital Identity Wallets that are provided in accordance with this Regulation**
- **For the payment sector, the PSD/PSR would be applicable including for fraudulent payment transactions**

## Technical Service Provider

**PSD 3 Art 58**

**Technical service providers (PSP) either provide services to the payee, or to the payment service provider of the payee or of the payer**

- Liability of technical service providers for failure to support the application of strong customer authentication
- Outsourcing arrangements

## EBA Requirements

**EBA clarifies the application of strong customer authentication requirements to digital wallets | European Banking Authority**

**Q&A 2020_5622**

- The enrolment of a payment card to a digital wallet, leading to the creation of a token/digitised version of the payment card and requires the application of strong customer authentication (SCA)
- The initiation of transactions with the digitised version of the payment card also requires the application of SCA under Article 97(1)(b) of PSD2, unless specific exemptions apply.

**Q&A 2021_6141**

- The issuer is required to apply SCA when adding a payment card to a digital wallet
- The Issuer is responsible for providing the respective SCA elements to the PSU.
- The issuer has to provide relevant security measures to protect the confidentiality and integrity of PSU's personalised security credentials.

**Guidelines on outsourcing arrangements**

- Issuers may outsource the provision and verification of the elements of SCA to a third party

**Q&A 2021_6145**

- The unlocking of a mobile phone with biometrics (e.g. a fingerprint) or with a PIN/password cannot be considered a valid SCA element for the purpose of adding a payment card to a digital wallet, if the screen locking mechanism of the mobile device is not a process under the control of the issuer

**Q&A 2022_6464**

- The issuance of a new token, replacing a previously existing one, and binding it to a device/user also requires the application of SCA

# Relevant European Regulation: Data Processing



## GDPR

- **Any involved entity (including a digital wallet provider) has to manage policies and procedures accordingly to GDPR regulation**
- This regulation is about data protection and privacy in the EU and the European Economic Area (EEA).
- It also addresses the transfer of personal data outside the EU and EEA areas, and applies to digital wallets since they involve processing personal data

## EU Digital Identity Framework

**key principle for EUIDW : "Your data; your control"**

Regulation - EU - 2024/1183 - EN - EUR-Lex (europa.eu) enter into force in 2024

**Data Minimisation**

- It means that any digital service should collect only the absolute minimum of data required to provide the service.

**Selective disclosure of attributes**

- This feature will allow the user to only share the specific information requested by a service provider, without revealing extra information.
- Digital document issuers will be legally forbidden to combine personal data with third-party data

**Zero-knowledge proofs**

- A feature that allow the verification that an attribute is true without disclosing any further details.

**Unobservability**

- Actions stay entirely private and invisible online. This is opposed to anonymity, where the user is not personally identifiable, but his actions are visible.

**Privacy Dashboard**

- Tracking service for the end user : traceability of the kind of data the user chooses to share, provide the end user with a view of any actor he shared his data with.

## Data Act

A **Framework for Financial Data Access is foreseen in order to regulate customer data access, customer's control on data, the way data should be shared.**

The Data Act will be applicant from September 2025 with the general intention to grant users of connected devices, ranging from smart household appliances to intelligent industrial machines, access to data generated by their usage and use them to select alternative providers (e.g. technical service of car repairing). Previously, this data (and metadata) was exclusively in the hands of manufacturers and service providers.

- Conclusions from Innoet to Volume SubGroup 10 04 2024 : Data Act focuses solely on data generated by devices and its implications for manufacturers.
- NB : A wallet provider can also be a device manufacturer (eg : ApplePay/Apple).

# Relevant European Regulation: Anti Money Laundering (AML)

- Anti-Money Laundering Directive (AMLD): The AMLD, and its various iterations (recently the 5th AML Directive), aim to make financial systems and digital wallets safer and more transparent, but they also impose additional administrative burdens on digital wallet providers. Non-compliance can result in severe penalties. Anti-Money Laundering Directive (AMLD).

  - The regulation states certain obligations to digital wallet providers to prevent illicit activities like money laundering and terrorist financing. Here's how it impacts digital wallets:
    1. Enhanced Due Diligence: Digital wallet providers have to carry out enhanced due diligence on their customers. This includes verifying identities, understanding their source of funds, and monitoring their transactions.
    2. Risk Assessment: Providers are required to conduct a risk assessment to identify, assess, understand, and mitigate money laundering risks associated with their services.
    3. Record Keeping: The directive mandates keeping customer and transaction records for a certain period, often up to five years after the end of a business relationship or completion of a transaction.
    4. Reporting Suspicious Activities: Digital wallets providers have to report any suspicion of money laundering activities to the relevant authorities.
    5. Training: The directive requires digital wallets providers to train their staff to recognize signs of money laundering and to know the procedures for reporting suspicious activity.

# Relevant European Regulation: Other relevant aspects



**Limited Network exclusion**

If a digital wallet is designed to be used only within a limited network of service providers or for a limited range of goods or services, it may qualify for the LNE. For example, a digital wallet issued by a specific retailer for use only within their own stores might fall under this exclusion.
However, if the digital wallet can be used for a broad range of transactions, such as making payments to a wide variety of merchants or transferring funds to other users, it would likely not qualify for the LNE and would thus be subject to the full scope of PSD2 regulation.
This means that digital wallet providers must assess their own services to determine whether they qualify for the LNE or not. If they do not qualify, they must comply with the regulatory requirements of PSD2, which includes obtaining a payment institution license, performing customer due diligence, and following data security standards.

**More Transparency for Payment Statements**

**PSD3 intends to regulate how the legal name or commercial name of the Payee should be used on payment account statements.**

• The current proposal stipulates that PSPs must include in payment account statements the information needed to unambiguously identify the payee, such as a reference to the payee's commercial trade name.

**Geo-blocking Regulation EU Regulation 2018/302**

**The Geo-blocking Regulation (EU Regulation 2018/302)** prohibits unjustified geo-blocking and other forms of discrimination based on customers' nationality, place of residence, or place of establishment within the internal market of the EU. This regulation came into effect on December 3, 2018.
Geo-blocking refers to practices used by online sellers that result in the denial of access to websites based in other member states, or situations where access to goods or services is granted, but under different conditions.
**The impact on digital wallets is significant**. This regulation ensures that digital wallets, like other payment methods, cannot be restricted, denied, or otherwise discriminated against based on the user's nationality or location within the EU.
For instance, a French user should be able to use their digital wallet to make a purchase from a German website without any additional fees or conditions that a German user wouldn't face. Similarly, a digital wallet provider cannot refuse service to customers because they are located in a different EU member state.
This increases the scope of potential customers for digital wallet providers, but it also means they need to ensure their services are fully compatible and compliant with the regulation across the entire EU market. Non-compliance can result in penalties.

# Conclusions



- Functionality of digital wallets is steadily increasing and **moving away from being a simple container mimicking a card**.
- The opening up of digital wallets to cards, open banking, the digital euro, stablecoins (both backed and unbacked crypto) creates a **multi-faceted narrative**, with broader NFC accessibility.
- Changing business models, a variety of vendors, applications/use cases, merchant types, differing services, and the mobile device now acting as a soft POS raise the question: **what is the risk of interconnection over the next 5–10 years?**
- Digital wallets are not intended to be included in Volume v11. The purpose of this taxonomy is to provide a comprehensive understanding of digital wallets in order to support their potential inclusion in future versions — following the usual EPSG assessment procedures and in parallel with related topics such as EUDIW and the Digital Euro.
- The Innovation Expert Team will continue its work to:
  - *Assess the eIDAS Implementing Acts to understand their impact on digital wallet frameworks.*
  - *Follow up on EUDIW pilots by ensuring continuity and engagement with experts involved in the new pilot phases.*
  - *Address any remaining issues based on evolving market and legislative developments.*

# Thank You

EPSG
European Payments Stakeholders Group