Dissemination level: Public

PAYMENT ENABLERS SERVICES
WP 2

Author: Visa Europe

Contributors: Banca Transilvania, BPC, University of the Aegean & Arthur's legal

Day of submission: 24/07/2025

Contents

Co-funded by the European Union

Co-funded by the European Union

Revisions

Version	Date	Author	Changes
V0.1	20/5/2025	Visa Europe	Initial Draft
V1.0	9/7/2025	Visa Europe	Final version reviewed and agreed by contributors. SoA section still to be updated. Under review of Project Coordinators.
v1.1	15/7/2025	Visa Europe	Updated SoA version + format improvements
V1.2	22/7/2025	Visa Europe	Updates following EWC Management board review and legal review

Co-funded by the European Union

Executive Summary

Payment is a key use case as it could help drive the adoption of EUDI Wallets by anchoring EUDI Wallets in European citizen daily lives and bring benefits to the payment industry by helping fight fraud and innovate by combining identity and payment credentials together at merchant's checkout.

The European Wallet Consortium (EWC) Payment Taskforce has made significant achievements in piloting and designing the use of the European Digital Identity Wallet (EUDI Wallet) as a means of Strong Customer Authentication (SCA) for online payments. The work aligns with the evolving regulatory landscape in the EU, notably PSD3, PSR, and eIDAS2, and addresses both technical and user experience (UX) challenges to drive adoption across the payment's ecosystem.

Scope and Focus

- eIDAS2 introduces the requirements for banks to accept EUDI Wallets for **online payment Strong Consumer Authentication (SCA)** by the end of 2027 - although some clarification is still needed, this has been the primary focus of EWC.

- Beyond SCA requirements, EWC's ambition in Payments was very high, with a wide scope that includes **payment initiation**, in store or online, transforming the EUDI Wallets into true payment wallets holding payment credentials.

Organization and Approach

- The Payment Taskforce, consisting of 18 EWC partners, is dedicated to bridging identity and payments, guided by principles of broad inclusion (cards and accounts), minimal disruption to existing infrastructures, and innovation through combining identity with payment credentials.

- Key objectives included developing SCA specifications for both cards and accounts, piloting these in real-world settings, and creating a feedback loop with payment and identity industry stakeholders.

Production Pilots

- We piloted online card payment transactions in a production environment in Q2 2025, by teaming up with a bank (**Banca Transilvania**, and their technology provider **BPC**), a wallet (**iGrant.io**), a merchant (**Cyclades Fast Ferries** and their payment provider **Worldline**) and a card scheme (**Visa**).
    - **First-ever online card payment in production** using an EUDI Wallet as an SCA method: Conducted in March 2025 with real users, real credentials, and real money movement.

Co-funded by the European Union

- Two online payment SCA flows piloted:
  - **Bank-led flow (March)**: Bank authenticates the user via the EUDI Wallet.
  - **Merchant-captured flow (June)**: Merchant captures authentication data and relays it to the bank. Additional services like **combined presentation of payment and studentID** for discount eligibility, **"Fast Checkout", payment receipts**, **boarding passe**s and **trusted list** were also implemented.

Deliverables and Contributions

Despite the absence of payment specifications in the ARF and Implementing Acts, the lack of maturity of standards eg OpenIDC4VCI/VP and the regulatory uncertainty due to the interplay of eIDAS2 and PSD2/PSR, EWC Payment taskforce has **produced actionable deliverables**[1] **that will serve as inputs to the EC for upcoming ARF / Implementing Acts** versions and guide the payment industry:

- developed functional and technical **specifications for online payment SCA** (Strong Customer Authentication) both for card and account (Implementation Guide, RFCs, Integration Guide, Data Schemas) - those served as the foundations for the payment pilot.
- developed functional specifications for **payment initiation for card and account**, and a IBAN Attestation for Individuals Rulebook.
- engaged with **standard organisations**, with concrete results notably with OpenID Foundation which **updated OpenID4VP protocol** to support dynamic transaction data required for payments, and with EMVco, the international card standardisation body, who published an **EMVco White Paper** about the support of additional authentication data in EMV 3DS for the EUDI Wallet.
- evangelized how EUDI wallet can play a role in payments with five quarterly **Payment Interest group webinars**, the development of a **Payment White Paper** and educational deck and videos, participation in tens of industry events or client meetings.
- through a close **collaboration with NOBID**, we have
  - developed a joint **Payment Rulebook** that has been shared with DG CONNECT at the end of March, that will eventually be referenced by the EC[2]
  - brought to the Commission's attention the **regulatory challenges** that need to be clarified and **proposed a solution** that could solve for this.

Key Learnings

1. **EWC specifications have proven to work in production**

EWC's technical specifications for Strong Customer Authentication (SCA) using the EUDI Wallet were successfully implemented in a real-world environment. They are the solid foundations on which the upcoming Payment Rulebook and Use Case Manual will be based.

2. **Scalability requires further standardization**

[1] see Deliverables section
[2] See Rulebook section

Co-funded by the European Union

While existing standards like OpenID4VP and EMV 3DS supported the pilot, enhancements are needed for large-scale deployment.

3. **UX/UI needs refinement**

The wallet's interface, especially around the SCA attestation terminology and the display of PSD2 required payment information should be carefully designed to avoid users' confusion.

Fast Checkout future versions should include standardized UX guidelines and simplified flows to remove unnecessarily friction e.g. using Digital Credential APIs and card tokenization.

4. **User Acceptance: survey early results are positive**

- **59% of users preferred the EUDI Wallet experience** over traditional authentication methods; 53% were very likely to adopt it if offered by their bank.
- **80% found the EUDI Wallet "Fast Checkout" was easier** than standard checkout, with a Net Promoter Score (NPS) of 75.
- Some users **requested clear benefits and more reassurance on data protection and security**.
- Further **improvements to checkout speed** and **mobile flow** were also requested.

(disclaimer: very limited number of participants, results are not necessarily representative but provides an early direction)

5. **Technical implementation learnings**

Bank-Side Learnings:

- Integrating EUDI Wallet registration and lifecycle management into online/mobile banking was not feasible during the pilot due to overloaded development roadmaps.
- Online/mobile platforms are critical for customer engagement, so banks must plan early to prioritize such integration.
- The impact on the bank's authentication system (ACS) was manageable when using third-party identity solutions, making external integration viable.

Merchant-Side Learnings:

- Direct integration of EUDI Wallet at the merchant (rather than PSP) worked but may not scale; PSP-side integration might be better for smaller merchants and broader eIDAS2 service adoption.
- Technical challenges arise with payment pages in iFrames, as they block wallet invocation; hosted payment pages are more compatible.

Co-funded by the European Union

Identity Expertise Gap:

- Payment developers often lack identity expertise, making identity stack integration complex and resource heavy.
- Simplified APIs and abstraction layers are crucial for easier developer adoption and reduced integration friction with digital identity solutions.

6. **Regulatory clarity is urgent**

The pilot assumed PSD2 compliance without requiring outsourcing agreements between banks and wallet providers. However, broader adoption hinges on clear regulatory guidance, especially around PSD3, PSR, and eIDAS2 interplay.

7. **Non-technical domains will be impacted**

Pilot participants needed significant onboarding help, including wallet setup, credential issuance, and troubleshooting. Real-time support (e.g., WhatsApp groups, call centres) was essential, highlighting the need for robust user education and support infrastructure.

- **Marketing and Communication**: Consumer banks, wallets and merchants need to build messaging, value propositions to drive awareness and usage of the EUDI Wallet for SCA and login.
- **Customer Support:** Consumer banks, wallets and merchants need to update their support channels processes and train their CSR.
- **Legal**: Consumer banks, wallet providers and merchants need to update their consumer's T&Cs to include the necessary Payment regulation (eg PSD2/PSR/RTS) and GDPR provisions. In particular, the pilot revealed uncertainty around the data controllership role of wallet providers, necessitating **guidance from the European Data Protection Supervisor**.
- **Dispute management and fraud reporting** processes and tools

  Note: managing end-users' pilot for payment requires significant efforts

Co-funded by the European Union

Key drivers and headwinds[3]

For the EUDI Wallet in the online payment SCA space:

Drivers

- **Unified Authentication Tool**: EUDI Wallet offers a single, trusted method for both login and payment authentication across services.
- **Enhanced Checkout Innovation**: Enables seamless "Fast Checkout" by combining payment and identity credentials and potentially superior experience on mobile devices
- **Security & Fraud Reduction**: Trust marks and verified credentials can reduce fraud, especially APP scams (Authorized Push Payment).
- **Government Adoption Potential**: High-frequency use case (payments) could drive wallet adoption, starting with implementation at online public services before moving to private sector.

Headwinds

- **Consumer Behavior Change**: Shifting payment habits is difficult and requires strong communication and incentives.
- **Merchant Adoption Lag**: the optional Fast Checkout feature requires significant merchant-side changes, risking a chicken-and-egg problem.
- **Bank Readiness by 2027**: Many banks are unaware or unprepared for the required changes. And are unlikely to progress without regulatory clarity.
- **Brand Dilution Risk**: Banks may fear losing visibility if customers stop using their apps for authentication

Next Steps and Recommendations for scaling the EUDI Wallet in online payment SCA

- **Collaboration with the European Commission:** Finalize the Payment Rulebook and Use Case Manual, resolve regulatory issues, develop UX guidelines and define Rulebook governance and certification frameworks.
- **Specification Improvements:** Focus on UX optimization (e.g., card tokenization, DC APIs) and merchant integration
- **Evolving Standards:** Advance alignment with EMV 3DS, Berlin Group, and relevant open banking bodies.
- **Pilot additional features** such as real-time wallet registration, multi-card/account support, and transaction logs. Expand support for account-based payments (Open Banking PIS) alongside card payments
- **Improve technical specifications** by integrating card tokenization, Digital Credential APIs, and better merchant integration (e.g., PSP-side, iframe compatibility).
- **Run large-scale user surveys** to gather representative insights and refine the UX and value proposition.

[3] For more details see: Key drivers and headwinds for the EUDI Wallet in the online payment SCA space

Co-funded by the European Union

- **Prepare non-technical domains: marketing, customer support, and legal frameworks (e.g., T&Cs, GDPR, PSD2 compliance) for 2027 readiness**
- **Evaluate fraud prevention potential of EUDI Wallets (e.g., trust marks, fraud signals, step-up authentication) and impact on dispute management processes and tools.**

In addition, continue to explore the potential of EUDI Wallet for **Payment Initiation, in store and online**.

Conclusion

The EWC Payment Taskforce's work validates the EUDI Wallet's ability to deliver secure, compliant, and user-friendly SCA for online payments. Continued industry cooperation, technical refinement, and regulatory alignment are essential in the next LSPs to achieve commercial-scale deployment and realizing the vision of a pan-European digital payments authentication and initiation solution.

Co-funded by the European Union

List of abbreviations

Acronym	Explanation
(Q)EAA	(Qualified) Electronic Attestation of Attribute
EAA	Non-Qualified Electronic Attestation of Attribute
Pub-EAA	Public Body Electronic Attestation of Attribute
ACM	Access Control Mechanism
ARF	Architecture and Reference Framework
CBOR	Concise Binary Object Representation
CIR	Commission Implementing Regulation
COSE	CBOR Object Signing and Encryption
DTC	Digital Travel Credential
EDIR	European Digital Identity Regulation
eID	electronic Identification
eIDAS	Electronic Identification, Authentication and trust Services
ETIAS	European Travel Information and Authorisation System
EUDI	European Digital Identity
F2F	Face-to-Face
FAQ	Frequently Asked Questions
FAR	False Acceptance Rate
FRR	False Rejection Rate
IBAN	International Bank Account Number
IA	Implementing Acts
ICAO	International Civil Aviation Organization
ISO	International Organization for Standardization
JOSE	JSON Object Signing and Encryption
JSON	JavaScript Object Notation
MRTD	Machine Readable Travel Documents
NFC	Near Field Communication
PAD	Presentation Attack Detection
PAN	Primary Account Number
PID	Person Identification Data
QC	Qualified Certificate
QES	Qualified Electronic Signatures

Co-funded by the European Union

Acronym	Explanation
QSCD	Qualified Signature/Seal Creation Device
QTSP	Qualified Trust Service Provider
SD-JWT	Selective Disclosure for JWTs (JSON Web Tokens)
SOG-IS	Senior Officials Group - Information Systems Security
T&Cs	Terms and Conditions
TSP	Trust Service Provider

Co-funded by
the European Union

1. Introduction

1.1 Reminder of initial scope

The initial scope as agreed in the Grant Agreement was broad:

Deliverable D2.5 – Payment enablers services

Deliverable Number	D2.5	**Lead Beneficiary**	48. Visa Europe
Deliverable Name	Payment enablers services		
Type	R — Document, report	**Dissemination Level**	PU - Public
Due Date (month)	18	**Work Package No**	WP2

Description
Payment capabilities leveraging EU ID Wallet a) eCom card & account trx, EU ID for
SCA b) B2B request to pay validate OID and SCA with EU ID wallet c) Push payment credentials and make payments with existing payment wallet d) Issue and push payment credentials into EU ID wallet, and make payment (eCom, face-to-face best effort)

1.2 Revised deliverable scope

As we were advancing in our thinking and delivering the specifications, we realized that with the resources available, we would be able to deliver a pilot in production for online card payment SCA. This is what has driven our energy and resources as being able to reach that stage with real data and real citizens will bring so much more value than just having theorical specifications.

Updated timeline

D2.5 was expected to deliver a report by M+18 (30 September 2024) about payment enablers. We have asked for a new due date 31st July 2025, in line with the global EWC 4 months extension (31st March + 4) that has allowed us to deliver a payment pilot in production in Q2 2025.

Updated scope

As mentioned in the 1-year intermediary report, we had to slightly change the prioritisations of the use cases:

- With the announcement that the NFC interface on iOS will now be available for face-to-face payments, we have decided to prioritise D2.5d as it represents a potential business opportunity for Wallet Providers
- We also focused on payment use cases that drive the EUDI wallet usage and minimize impacts on payment infrastructure (Deliverable 2.5 a. and d.) while ensuring regulatory compliance and a great UX (we designed two authentication flows, one led by the bank, the second led by the merchant that enables more innovations). This is a high priority as the banks would need to accept EUDI wallet to online payment SCA by end 2027.
- We deprioritized the request to pay B2B scenarios (Deliverable 2.5b) and the provisioning of payment credentials into another payment wallet (Deliverable 2.5c) as

Co-funded by the European Union

we did not have partners ready to deliver on those scenarios (B2B partner or payment wallet)

This revised scope (D2.5 a + d) and timeline has enabled the team to focus on what's most urgent for the industry and on delivering a pilot in production, demonstrating that the EWC payment specifications work effectively in real-world scenarios.

1.3 Organisation of work

EWC has setup a Payment Taskforce dedicated to exploring the intersection of identity and payment technologies. With a strong belief that payments are a key use case for driving EUDI-Wallet adoption, the 18 partners have been working on developing open standards to benefit the entire financial ecosystem.

Our Guiding principles:

- Inclusion of card and account payments, covering everyday payments
- Minimization of the impact on existing payment infrastructure
- Innovation by combining identity and payment credentials

The Payment Taskforce has outlined several key objectives to drive the adoption of EUDI-Wallets within the payments space:

- SCA Specifications and Use Cases: Developing SCA specifications for both card and account online payments to ensure compliance with regulatory frameworks and identify real-world barriers to adoption, such as regulatory constraints and user experience challenges.
- Beyond SCA: Exploring opportunities where EUDI-Wallets can be used to initiate payments, being card or account, in person or online.
- Pilot EWC specifications to ensure they are actionable and use lessons learned from pilots to serve as the foundation for future standards across, for example, the ARF (EUDI-Wallet Architecture Reference Framework), OIDF, EMVco for card-based payments, and the Berlin Group for Open Banking/Account-based payments.
- Awareness and Feedback: Raising awareness of the taskforce's developments within payment and identity communities while collecting valuable feedback from stakeholders

Co-funded by the European Union

EWC Payment taskforce members, as of 17th december 2024

Organisation legal names and roles:

Name	Role	Legal name	PIC
Lissi	AP	Lissi GmbH	879889717
iGrant	BEN	LCubed AB	907079593
Digidentity	BEN	DIGIDENTITY BV	911288714
Raiffeisen	ERP	Raiffeisen Informatik GmbH & Co KG	n/a
	ERP	Raiffeisen Bank International AG	n/a
Piraeus Bank	AP	TRAPEZA PEIRAIOS AE EL	905415364
Banca Transilvania	AP	BANCA TRANSILVANIA S.A.	904924350
BankID	BEN	FINANSIELL ID-TEKNIK BID AB	886186472

Co-funded by the European Union

BPC	ERP	BPC AG	n/a
University of the Aegean	BEN	PANEPISTIMIO AIGAIOU (UAEGEAN)	999840693
Fast Ferries	BEN	KYKLADES FAST FERIS NAFTIKIETAIREIA	885474492
Infocert	BEN	INFOCERT SPA	990330037
Outpayce	AE	Amadeus Affilated Entity	n/a
Google	AP	Google Inc.	n/a
Wordline	BEN	WORLDLINE FRANCE	887916273
Netcetera	ERP	Netcetera AG	n/a
Token ID	BEN	BELL IDENTIFICATION BV (BELL ID)	990255929
Tink	BEN	TINK AB	885709232
Visa	AP	VISA EUROPE LIMITED	885401451

Co-funded by the European Union

2. State of the Art

Understanding the range of payment instruments, consumers habits, authentication requirements, and the regulatory approaches shaping the European market helps position the EUDI Wallet in the crowded payment landscape.

Disclaimer: this chapter has been written using GenAI capabilities combined with human experts' knowledge and curation. All sources are public information.

2.1 Defining the Types of Payments

Consumer payments can be categorized as follows:

- Non-recurring / day to day payments. This category includes:
  - REMOTE: Online payments for goods/services ordered and paid remotely (including mobile or desktop e-commerce).
  - PROXIMITY: Physical point-of-sale (POS) payments for goods/services made in person in proximity situation.
  - P2P (Person-to-person) payments / money transfer not tied to specific purchase obligations.
- Recurring payments. These are ongoing payments such as rent, phone bills, utilities, or subscription services.

2.2 Payment authentication versus Payment initiation

PSD2 has defined and requires Strong Customer Authentication (SCA) for several different cases, including online payments being by card or account. This category is particularly relevant when it comes to the EUDIW, as eIDAS2 mandates banks to accept EUDIW for the purposes of SCA.

Banks under PSD2 have implemented SCA methods (SMS OTP, push to mobile banking app, …) to authenticate both card and Open Banking PIS online payments. By 2027 EU banks under eIDAS2 would have to implement a new SCA method: the EUDIW as a working alternative to the existing one.

But beyond SCA regulatory play, EWC has started to explore Payment Initiation where EUDI Wallets can become a true Payment wallet, holding payment credential (card or account) and initiate a payment for both instore and online payments.

Co-funded by the European Union

Payment Authentication

EUDIW as an alternative SCA method for online payments

Satisfying regulatory obligations

- **Linking a user's EUDI wallet with his payment account or card** (registration)
- **SCA for card-based transactions –** EUDI wallet invoked by payer's bank (card issuer) or authentication data captured by the merchant
- **SCA for account-based transactions** – EUDI Wallet invoked by payer's bank (ASPSP) or authentication data captured by the merchant
- **Add identity attributes** to a payment transaction

Payment Initiation

EUDIW as a payment wallet, holding payment credentials

Beyond SCA, opportunities instore or online

- EUDI Wallet to provision **card and account tokens** to initiate online or instore payments
- **Instore NFC card payment** with no impact on merchant acceptance
- Push the **card or account token payload to an online merchant** for payment processing
- **Add identity attributes** to a payment transaction

12

2.3 Payment Landscape in Continental Europe: Overview & Trends

Europe's retail-payment market is in the middle of a once-in-a-generation transition. Although consumers are still fond of cash for everyday purchases, the latest ECB SPACE [11] survey shows the value picture is already digital: the share of online payments in consumers' day-to-day payments has continued to increase in value from 28% to 36% (2022 vs 2024), mobile payment wallets are gaining traction both in store and online.

Two powerful regulatory packages—PSD3/PSR and the 2024 Instant Payments Regulation (IPR)—will accelerate the shift over the next five years, while a third, the new EU AML/CFT package, rewrites compliance obligations from KYC to crypto transfers. On the technology side, strong customer authentication (SCA) has become the backbone of secure commerce, driving card-fraud rates to historic lows and creating the conditions for a soft "sunset" of weak authentication methods such as SMS OTP.

Big-tech wallets keep expanding their reach (and now venture into digital-identity credentials), domestic alias-based A2A wallets flourish, and a pan-European contender—Wero—is due to launch in 2025. Finally, the ECB's preparations for a retail digital Euro could add a new form of public money to this already crowded landscape before the decade is out.

2.3.1 Common Payment Methods in Europe

European consumers use a variety of payment methods, with preferences differing between online (e-commerce and mobile commerce) and in-store (point-of-sale) contexts. **In general, electronic payments are steadily gaining ground across Europe, although cash remains in use, especially for small in-person purchases[1].**

Co-funded by the European Union

Online Payments (E-commerce & Mobile Commerce)

Digital wallets are now the leading online payment method in Europe, accounting for roughly one-third of e-commerce transaction value in 2024[2]. These include services like PayPal and big tech wallets (Apple Pay, Google Pay/Wallet), which allow users to pay conveniently via stored cards or bank details. Cards (especially debit cards) are the second-most popular way to pay online[2].

Mobile commerce – shopping through smartphones or tablets – has grown rapidly, blurring with e-commerce. Many Europeans now shop on mobile devices, leveraging features like one-click payments and in-app wallets. For example, Poland's mobile payment system **BLIK**, integrated into banking apps, has become hugely popular for online purchases[3], making account-to-account bank payments (via BLIK codes) a dominant mode for Poland's e-commerce. Similarly, in Spain, the mobile payment service **Bizum** has over 20 million users and is fueling growth in instant bank transfers for online payments[3].
Other online payment trends include the rise of **Buy Now, Pay Later (BNPL)** solutions (like Klarna or Afterpay), which allow shoppers to split purchases into installments. BNPL still represents a single-digit share of e-commerce value (around **5% of online transaction value globally in 2022, and growing**[4]), but it has established a foothold in European e-commerce checkouts.

Key Takeaways (Online): European online shoppers increasingly prefer **digital wallets** due to their convenience and security. Cards are still widely used, but **alternative methods (wallets, instant bank transfers)** are growing[3]. The trend is toward frictionless, one-touch payments often via mobile devices.

In-Store Payments (Point-of-Sale)

At brick-and-mortar stores, **cards have become the dominant payment method by value, although cash remains the most frequently used by number of transactions in many countries[1].** According to a 2024 European Central Bank survey, cash was used for **52% of point-of-sale transactions** across the euro area (down from 59% two years prior), while cards accounted for most of the rest[1]. In terms of money spent, however, **cards made up 45% of POS transaction value versus 39% for cash[1]**, indicating that people tend to use cards for higher-value purchases and use cash for smaller daily items.
Debit cards (often with contactless tap-and-go capability) are especially popular in retail transactions. For example, in Germany debit and prepaid cards held a 41% share of in-store payments in 2024, followed by cash at 35%[3]. Northern European countries have some of the lowest cash usage – in places like the UK and Scandinavia, card payments (including via mobile phone) have largely overtaken cash for point-of-sale. In the **UK**, for instance, **digital wallets already comprise 18% of in-store payments (2024) and are projected to reach one-third by 2030[3]**.

Mobile in-store payments (using smartphones or smartwatches at the checkout) are rising quickly. Solutions like **Apple Pay** and **Google Wallet** leverage the contactless card infrastructure: a tap of the phone transmits a card token. Though starting from a small base, these mobile wallets have gained foothold: e.g. in **France**, digital wallets have a 13% share at

Co-funded by the European Union

POS in 2024 but are expected to reach ~23% by 2030[3]. **Domestic mobile apps** are also entering stores – Spain's **Bizum** plans a contactless in-store payment feature by 2025[3], and in the Nordic region apps like **Swish, Vipps, and MobilePay** (originally P2P transfer apps) are enabling merchant payments – in particular **Vipps** has been the first launching an alternative to Apple Pay for in-store payments[12].
It's worth noting that **contactless card payments** (be it via plastic card or a phone) surged during the COVID-19 pandemic, as consumers and merchants favored tap payments for hygiene and convenience. This accelerated the adoption of mobile and contactless methods. For example, **in Norway, a sharp increase in mobile payments was observed post-pandemic[5]**, and similar patterns occurred across Europe with contactless card usage limits being raised.

Key Takeaways (In-Store): Cards (especially debit) are the workhorse of in-store payments, having eclipsed cash in value and closing the gap in volume[1][3]. **Cash is still commonly used for small purchases**, but its share is steadily declining each year. Meanwhile, **contactless and mobile wallet payments are the fastest-growing at POS**, expected to capture a much larger share by the end of the decade[3].

2.3.2 Regulatory Landscape: Key EU Payment Regulations

Europe's payment ecosystem is strongly shaped by regulation. The European Union has introduced directives and rules to **make payments safer, more competitive, and more integrated across member states.** Below is a summary of the major regulatory frameworks:

PSD2 – The Second Payment Services Directive (2015/2018)

The **Second Payment Services Directive (PSD2)** is a cornerstone of EU payments law. Adopted in 2015 and in effect since January 2018, PSD2's goal was to **boost competition and innovation in payments while enhancing security**[6]. **Key features of PSD2 include:**

- **Open Banking:** Banks must allow licensed third-party providers access to customer accounts (with consent). This created two new roles:
  - *Account Information Service Providers (AISPs)* – who can retrieve account data (for budgeting apps, etc.).
  - *Payment Initiation Service Providers (PISPs)* – who can initiate payments on behalf of the user, directly from the bank account.
  - This **"open banking" framework opened the door for fintech companies to offer new services** (like apps that aggregate your finances or services that pay merchants from your bank account) and increased competition beyond traditional banks[6].
- **Strong Customer Authentication (SCA):** PSD2 introduced requirements for two-factor authentication for electronic payments (see SCA section for details). This was meant to reduce fraud by ensuring that a user approving a payment is strongly verified[6].
- **Consumer Protection & Transparency:** PSD2 improved refund rights (e.g. in case of unauthorized transactions), mandated clearer information on fees/exchange rates, and set rules for liability and dispute resolution across the EU.

Co-funded by the European Union

Overall, **PSD2 has been a major driver of change**, leading to the development of new services (for example, many European banking apps or e-commerce checkouts now offer a direct bank transfer option powered by PSD2 open banking). It also **raised security standards** through SCA, albeit with some growing pains in implementation. The directive needed to be transposed into each country's law, and by now it is fully operational across Europe.

PSD3 and PSR – The Upcoming Update

Recognizing that payments continue to evolve, the EU is now working on **the next iteration: PSD3 (Third Payment Services Directive) along with a new Payment Services Regulation (PSR). In June 2023, the European Commission released draft proposals for PSD3/PSR as an evolution of PSD2[6].** These are **not yet law** (expected enforcement is **unlikely before 2027** after negotiations and a transition period[6]).

What's new in PSD3/PSR? While still being finalized, the broad aims are:

- **Modernize and fix gaps:** Payments technology and fraud patterns changed quickly since PSD2. PSD3 seeks to address inconsistencies and new issues – *it will enhance consumer protection, improve open banking uptake, and further harmonize rules across Europe*[6].
- **Structure:** The regulation is split into two parts. **PSD3 (directive)** will focus on licensing and supervision of payment providers (this means it deals with requirements to be authorized as a payment institution, etc.). **The PSR (regulation)** will contain operational rules applied directly across all member states – covering things like security requirements, SCA, rights and obligations of providers[6]. By using a Regulation, the European Commission ensures uniform application through all Member States, as there is no need for local transposition.
- **Improved Open Banking:** PSD3 is expected to make **open banking easier and more secure**, possibly mandating more standardized data access and eliminating remaining barriers, and improving requirements for APIs. It's essentially "building on PSD2's foundation" to encourage broader adoption of open banking services[6].
- **More flexible approach to SCA elements**: It is expected that the new text will allow the use of two factors from the same category when performing SCA if the independence is preserved.
- **Fraud Reduction Measures:** *Increased consumer protection* is a major theme. For example, proposals include **mandatory verification of payee name against IBAN for bank transfers (to avoid misdirected payments)** and clearer refund rules for fraud cases[6]. Provisions to address new types of frauds are also included, like bank employee impersonation. Other likely changes are updated rules for new types of payments (like crypto-assets or fintech innovations) and closing regulatory loopholes to ensure **both banks and fintechs play by the same rules (level playing field)[6]**.
- **Sunset of "screen scraping":** Under PSD2, some third-parties accessed bank accounts by simulating user logins ("screen scraping"). PSD3/PSR is expected to fully remove this in favour of **secure APIs only**, improving security and privacy.

In essence, **PSD3/PSR aims to refine and strengthen the framework established by PSD2**. Banks and payment firms are preparing for changes, but since the rules are still in draft,

Co-funded by the European Union

details could evolve. The timeline is to have the framework in place around 2025, with enforcement a couple years later[6].

AML/CFT Frameworks

In parallel with payment-specific rules, Europe has robust **Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT)** regulations that all payment service providers must follow. These ensure that the financial system isn't used for illicit purposes. **Key elements include:**

- **Customer Due Diligence:** Banks and payment companies must verify customers' identity (Know Your Customer, KYC) and monitor transactions. For example, when you open a bank account or a payments account, you usually must show ID documents – that's AML rules at work.
- **Transaction Monitoring and Reporting:** Unusual transactions or patterns must be analyzed and, if suspect, reported to authorities (Suspicious Activity Reports). There are also strict **sanctions screening** requirements (to prevent payments to/from prohibited parties).
- **EU AML Directives:** The EU has updated its AML laws multiple times (the 4th AML Directive in 2015, 5th in 2018, and 6th in 2021) to strengthen defenses. The **latest reform, adopted in June 2024, is a comprehensive overhaul**[7]:
    - It creates a new centralized regulator, **the EU Anti-Money Laundering Authority (AMLA)**, to coordinate supervision across member states[7].
    - It introduces a **single EU rulebook** (likely an AML Regulation) replacing many nation-by-nation rules[7]. This will unify standards on things like customer verification, reporting, and internal controls, reducing fragmentation.

EU Instant Payments Regulation (IPR)

This regulation[4] adopted on 13 March 2024, is a major legislative step to make instant credit transfers in euro the norm across the European Union. Here's a concise summary of its key elements:

Objectives

- Accelerate adoption of instant payments across the EU.
- Ensure equal access and affordability for consumers and businesses.
- Enhance security and fraud prevention in payment systems.

Key Provisions

1. Mandatory Instant Payments: All payment service providers (PSPs) that offer standard credit transfers must also offer instant credit transfers in euro.
2. Fee Equality: Charges for instant payments must not exceed those for standard credit transfers.
3. Verification of Payee (VoP): PSPs must provide a free service to verify the name of the payee before a payment is made, helping to prevent fraud.

[4] ECB https://www.ecb.europa.eu/paym/integration/retail/instant_payments/html/instant_payments_regulation.en.html

Co-funded by the European Union

4. Sanctions Screening: PSPs must screen daily whether any users are subject to EU financial sanctions.

Implementation timelines depend on requirement but in general spread between now and end 2027.

In summary, European regulations (PSD2/PSD3, AML, IPR, etc.) create a framework that prioritizes security, competition, and integration. They encourage **innovation (like open banking)** but also demand **responsibility (like strong authentication and AML duties)** from payment service providers, all of which ultimately benefits consumers through safer and more varied payment options.

2.3.3 Payment Instrument Mix: Usage & Trends

European consumers can choose from a wide **mix of payment instruments**, and the popularity of each is shifting with technology and preferences. This section examines the main categories of instruments and their usage trends **both online and in-store**.

Card Payments (Debit and Credit Cards)

Cards remain the most ubiquitous non-cash payment instrument in Europe. Virtually every adult has a debit card (linked to their bank account) and many have credit cards or prepaid cards. In stores, debit cards are often the primary cash alternative, used for everything from groceries to transit. As noted earlier, cards comprise a large share of payment volume and an even larger share of value at POS[1]

Contactless card usage is very high – most European cards now have an embedded NFC chip allowing tap-and-pay. This has made card usage even more convenient for small purchases, directly challenging cash. As a result, cash usage is dropping even in historically cash-friendly countries. For example, Italy's cash share at POS fell from ~30% to 25%, and is projected to dip to 20% by 2030 as card and wallet use grow[3]

Online, cards are commonly used often via entering card details or saving cards in wallets but are **trending toward greater convenience and security**. Innovations include:

- **Tokenization & Mobile:** Linking cards to mobile wallets (Apple Pay, Google Pay) effectively turns them into a token on a phone, blending card infrastructure with mobile tech.
- **Stronger Security:** Under PSD2's SCA rules, online card payments now often require a two-factor auth (like 3-D Secure code or app confirmation), reducing fraud at the expense of a bit more friction.
- **Click to Pay (CtP)**: **Click to Pay** is a secure, streamlined online checkout solution designed to make paying with a credit or debit card faster and easier. It's backed by major card networks like **Visa, Mastercard, American Express, and Discover**, and works across participating merchants. Once you've enrolled your card, you can check out with a single click—no need to enter your card number, billing address, or other details every time. Card details are not shared with the merchant. Instead, a token is used to process the payment, enhancing security.

Co-funded by the European Union

- **Payment Passkeys:** Payment Passkeys are a modern, passwordless authentication method designed to streamline and secure online payments. Built on **FIDO** (Fast Identity Online) standards, they replace traditional passwords with biometric authentication (e.g. fingerprint or facial recognition) or device-based credentials. This approach enhances both security and user experience by eliminating the need for passwords or one-time passcodes

Account-to-Account Payments (Open Banking & Instant Transfers)

A major shift underway is the rise of **account-to-account (A2A) payments** – where money moves directly from the payer's bank account to the merchant's (or receiver's) account. This can happen via traditional bank transfers, **open banking payment initiation** services or specific domestic A2A solutions.

Open Banking PIS: Thanks to PSD2, fintech providers can initiate a payment from your bank on your behalf. This means at an online checkout, you might see an option like *"Pay by bank"* or a specific service (e.g., Trustly) which, if selected, lets you securely log in to your bank and approve a transfer on the spot. It's a direct bank transfer using SEPA Credit Transfer (**SCT**) and where available SEPA Instant Credit Transfer (**SCTInst**), the later being close to real-time. **Adoption is still emerging** but growing:

- **Overall Share of Digital Payments**: PIS accounts for approximately **5–10%** of online payments in Europe, depending on the country[13]
- **United Kingdom**: Leading adoption with **10–15%** of online payments initiated via PIS, driven by strong API infrastructure and fintech innovation.
- **Nordics (e.g., Sweden, Finland)**: High digital maturity has pushed PIS usage to **8–12%** in some sectors.
- **Germany, France, Netherlands**: Moderate adoption, with **5–8%** of online payments using PIS.
- **Southern and Eastern Europe**: Lower adoption, typically **below 5%**, due to slower API rollout and consumer trust issues.

Other A2A solutions

- In the **Netherlands**, a form of A2A payment called **iDEAL** has been popular for years (even pre-PSD2). **iDEAL accounts for the majority of Dutch e-commerce transactions**, showing what A2A can achieve.
- **Wallet based** A2A solutions – see next section on Digital Wallets

Another form of account-based payment is **SWIFT or SEPA credit transfers** for larger purchases, but those are more common in B2B or invoice payments, not day-to-day consumer retail.

In summary, **account-to-account payments are not a niche anymore in Europe's payment mix, particularly online.** Open Banking has unlocked innovative services and **by 2030, account-based payments could comprise a sizable chunk of retail payments** in many countries[3]. Consumers might not always realize it (as they might experience it via a branded wallet or app), but behind the scenes it's their bank sending money directly to the seller.

Co-funded by the European Union

Digital Wallets – Global, Domestic, and Emerging

Digital wallets refer to electronic solutions (often apps) that store payment credentials and enable quick payments. They come in a few flavours:

- **Global wallets by tech giants:** The likes of **Apple Pay**, **Google Wallet/Pay**, and **Samsung Pay** allow a user to digitize their credit/debit cards into their phone (based on EMVco card tokenization standard). At the store, these act like a contactless card (NFC tap); online, they often enable one-click payment or within-app purchase. Apple Pay, for example, is now accepted by many European merchants in-app and on websites (especially via Safari browser on Apple devices) as a streamlined way to use a saved card with biometric confirmation. While hard numbers of users in Europe aren't always published, adoption is strong among smartphone users – millions use these wallets daily to commute, shop, and dine. **By 2024, mobile wallets (including these global ones) represent a growing share of both e-commerce (one-third+) and in-store payments (around 10% or more in many markets, and rising)[3].**
- **Global online wallets: PayPal** is a major example – it's an online wallet (with an account and stored balance/cards) rather than a device-bound one. PayPal is extremely popular in European e-commerce; for instance, it commands a large share of online checkouts in Germany, Italy, and elsewhere. Other similar services include Amazon Pay or Visa's Click-to-Pay, but none have the widespread consumer mindshare of PayPal in Europe. **PayPal and similar online wallets make up roughly 10% of e-commerce payments in some markets like France[5]**, and even more in others (Germany's online wallet usage is higher).
- **Domestic/regional wallets:** Several European countries have homegrown mobile payment apps, often born out of a collaboration of local banks or as an evolution of bank transfer systems:
    - **Swish** in Sweden, **MobilePay** in Denmark/Finland, **Vipps** in Norway – these Nordic wallets started as person-to-person payment apps linked to bank accounts and phone numbers. They enjoy huge user bases (over 80% of adults have Swish in Sweden) and are now expanding to retail payments (e.g., you can Swish to pay merchants or invoices online, or use Vipps for mobile payments in-store as an alternative to Apple Pay[12]
    - **Bizum** in Spain with 20+ million users (about half of Spanish adults)[3], initially used for splitting bills and now moving into merchant payments both online and expected in stores.
    - **Blik** in Poland which is used for everything from online shopping to ATM withdrawals (via code) and in-store QR payments. It's become the most-used payment method for Polish e-commerce.
    - **Payconiq by Bancontact** in Belgium and **Paylib** in France, now merged into **Wero**
    - **Bancomat Pay** in Italy or **MB WAY** in Portugal have also strong position in their home country
- **Emerging pan-European initiatives**
    - **Wero by EPI** (**European Payments Initiative** is a consortium of major European banks developing a unified payment solution for the EU. Wero aims to allow **instant payments between individuals and merchants across Europe**.

Co-funded by the European Union

- The **EuroPA (European Payments Alliance)** is a strategic initiative launched by **Bizum (Spain), Bancomat Pay (Italy), and MB WAY (Portugal)** to create a **pan-European, interoperable A2A mobile payment network**.

In summary, digital wallets (of all types) are transforming payments in Europe. They offer speed and convenience – no need to carry cash or even cards, and for online they avoid repeatedly typing card details. The data shows **wallets already lead online payments in aggregate and are set to grow further**[2][3]. At the point-of-sale, they currently piggyback on card infrastructure, but could also leverage bank account rails (as Wero aspires to do). Consumers benefit from a smoother payment experience, while merchants often see faster checkouts and potentially lower fraud (wallets can be more secure). We can expect **wallets – both global and local – to continue rising, potentially accounting for nearly half of all online payments in Europe by 2030**[2] **and a substantial portion of in-person payments as well**[3]**.** In that context, the EU DI Wallets could represent a viable alternative to existing payment wallets for initiating payments both online and in-person (see chapter **Payment Initiation: potential role for the EUDI Wallet**)

2.3.4 Strong Customer Authentication (SCA) in Europe

One of the most impactful recent changes in European payments is the rollout of **Strong Customer Authentication (SCA)** under PSD2. SCA is a requirement according to which certain payment related actions performed by the payer must be authenticated by the payment services provider using at least **two independent factors**, out of:

- **Something you know** (e.g. a password or PIN),
- **Something you have** (e.g. a phone or hardware token),
- **Something you are** (e.g. a fingerprint or face ID).

These elements must be independent, meaning the breach of one does not compromise the reliability of the others, and the authentication process is designed to protect the confidentiality of the authentication data.

Implementation Status: As of 2021-2022, **SCA has been fully implemented across Europe's card payment ecosystem**. Although the official SCA mandate date was September 2019, many countries gave extensions for e-commerce to avoid disrupting transactions. By late 2020 and into 2021, one by one, EU countries enforced SCA for online card payments, and the UK followed by March 2022. Now, virtually **all online card transactions in Europe require an SCA check (with some exemptions for e.g. low-risk or small amounts)**. Additionally, banks have applied SCA to online banking logins and certain sensitive actions. In-store chip-and-PIN was already a form of two-factor (card + PIN) and contactless taps are limited by amount and sporadically require PINs, complying with SCA rules via the "contactless exemption" logic.

For the average consumer, this meant that since SCA took effect, they encounter a **verification step for online payments** far more often than before. For example, when buying something online with a card, instead of just entering card details and hitting submit, one might be redirected to their bank's 3-D Secure page to approve the purchase. **The "approval" can take many forms** depending on one's bank:

Co-funded by the European Union

- **Mobile App Confirmation:** Many banks now prefer their smartphone banking app for SCA. The user gets a push notification and can confirm the transaction in-app (often by entering a PIN or biometrics like fingerprint/FaceID – fulfilling multi-factor via phone possession + PIN/biometric). This method is considered more secure than SMS and is the most widely adopted method.
- **SMS One-Time Passwords (OTPs):** A common method has been the bank sending a text message code to the cardholder's phone, which the user must enter on the verification screen (this uses possession of the phone + knowledge by typing an additional password). Still common, though usage is *declining* due to security concerns (SIM swap, phishing) and poor UX.
- **Physical Token or Card Reader:** Some banks issue a token device or use card readers that generate codes. These are less common now for consumers, but some people (especially in certain countries or with older setups) might use them.

Mix of methods across Europe: It varies by country and bank:

- Southern European banks initially relied heavily on SMS OTPs for SCA, but are shifting to app-based methods.
- Nordic countries, which had long used **BankID** systems, often integrated those for PSD2 SCA (e.g. Swedish BankID app to verify payments).

Impact of SCA: So far, **SCA has significantly reduced fraud in card-not-present (online) payments in Europe**. Early data from the European Banking Authority indicated that **the fraud rate on transactions authenticated with SCA is about five times lower than on those without SCA[8].**

However, SCA hasn't been without friction:

- **Checkout friction:** Some consumers abandon purchases if the verification is too cumbersome or if it fails. Banks and merchants have worked to optimize this – for example, by using "frictionless flow" (invisible checks) when risk is low, or making the challenge screens more user-friendly.
- **Customer learning curve:** Initially, many customers were confused by the new prompts (*"Why is my bank asking me to do this?"*). Over time it's becoming the new normal, and public education plus experience have smoothed the process.

Beyond cards: SCA also applies to accessing payment accounts, so whenever you log in to online banking or a payment app, you likely perform SCA (e.g., password + an SMS code, or fingerprint on your phone app). Additionally, direct debit electronic mandates and certain high-risk transfers may trigger SCA.

To sum up, **Strong Customer Authentication is now a fixture of European payments.** It adds an extra step for users but dramatically improves security. Europe's approach is being watched by other regions as a model for combatting fraud. The focus now is on refining SCA implementation to reduce any unnecessary friction – for instance, improving mobile authentication flows and ensuring merchants can take advantage of exemptions and analytics to make payment experiences both **secure and smooth**. As we discuss next based on the learnings of EWC pilot, the upcoming **EU Digital Identity Wallet might further streamline authentication in the future**.

Co-funded by the European Union

Sources: The information in this report is derived from publicly available sources, including European Central Bank reports, European Commission regulations, industry analyses, and press releases. Each number within the brackets corresponds to a source as listed bellow.

References

[1] Study on the payment attitudes of consumers in the euro area 2024
[2] E-commerce payment methods in Europe 2024| Statista
[3] The Most Popular Payment Methods in Europe 2025
[4] Account-to-Account Payments Set to Revolutionize Shopping, with E ... - FIS
[5] EUROPEAN E-COMMERCE REPORT
[6] PSD3: The EU's Third Payment Services Directive | J.P. Morgan
[7] The new EU AML framework: Guide to key changes for financial ...
[8] PSD2 and SCA: Where are we now - what will follow?
[9] EU digital identity wallets: steps for successful implementation
[10] EU Digital Identity Wallet: Transformational leap for payments
[11] ECB SPACE
[12] Vipps MobilePay launches the world's first alternative to Apple Pay on iPhone
[13] Open banking in Europe: A 2025 market overview

Co-funded by the European Union

3. Deliverables

Through EWC's Payment taskforce, an extensive number of deliverables has been produced. All deliverables have been included in a Zip Archive file provided to the European Commission jointly with this document. Most deliverables are public and can also be accessed via a web link.

3.1 Implementation Guides

Implementation Guides are functional specifications describing flows and UX/UI between all actors involved

- SCA for online payment using EUDIW - IG 1.2

This document describes the functional specifications of the EUDI Wallet for registration (section 2) and implementation of SCA (Strong Customer Authentication) using the EUDI Wallet in both card (section 3) and account (section 4) online payment use cases

- Payment Initiation with EUDIW - IG 1.1

This Implementation document describes the provisioning of payment credentials to the EUDI Wallet. It also covers paying with these payment credentials stored in the EUDI Wallet. Payment credentials can represent both cards and accounts.

3.2 Data schemas

Describes the data schema and structure of the attestations required for payment. The credential/data format used is SD-JWT

- ds007 Payment Wallet Attestation
- ds008 Payment Data Confirmation
- ds015 IBAN Attestation for Individuals

3.3 RFCs

RFCs are EWC's technical specifications. Two main RFCs have been built specifically for payments, and are valid for both card and account online payments SCA.

- RFC007 "Payment Wallet Attestation" : this specification implements payment wallet attestation and is based on "SCA for online payments using the EUDI Wallet" Implementation Guide. The PWA (also called "SCA Attestation" in this document) is issued by the bank when registering the wallet for SCA.
- RFC008 "Payment Data Confirmation" : This specification defines how a Relying Party (RP) can interact with an EUDI wallet to receive verifiable confirmation that a user has agreed to specific details of an (intended) payment transaction

Both RFCs have been used for the production pilot.

Co-funded by the European Union

3.4 Rulebooks

- **Payment Rulebook**

EWC & NOBID came separately on very similar conclusions on the best way to implement SCA with EUDIW and very similar specifications (SCA attestation, registration, bank or merchant initiated flow).

We decided in January 2025 to create a joint task force, which has built a single specification called “Payment Rulebook” that has been shared with DG CONNECT on the 27th of March. This document is not public and subject to change, but is included in the Archive package jointly with this report document.

At the time of writing this report, DG CONNECT is in the process of reviewing the Payment Rulebook with the goal to include it amongst the existing PID and mDL Rulebooks in a new Rulebooks repository, and to develop a Use Case Manual for Payments.

(the draft Payment Rulebook is not public yet, but included in the Archive pack joint to that report)

- **IBAN Attestation for Individuals Rulebook**

The rulebook rb007 is for IBAN attestation for individuals (Natural Persons). A version of the IBAN Attestation Rulebook for businesses (Legal Persons) rb003 has also been developed in WP3. Both rulebooks could potentially be consolidated into a single document at a later stage.

3.5 Integration guide

Based on the learnings from the pilot, this document provides technical guidance to the bank teams that needs to integrate EUDI Wallets in their authentication platform (ACS) for online card payments

3.6 Regulatory analysis

EWC has brought to DG CONNECT’s attention the challenges due to the interplay between eIDAS2, PSD2 and upcoming PSR/RTS. Multiple meetings between initially EWC and DG CONNECT, then jointly with EWC and NOBID, have been held in Q2 2025. At the time of writing this report, DG CONNECT is in the process of engaging with DG FISMA based on the regulatory analysis that has been jointly developed and shared by both consortia.

(see chapter Regulatory considerations)

3.7 Standardisation activities

Standardisation is key to ensure adoption and scale. The challenge is that ARF references standards that may need to evolve to support payment use cases, and does not yet reference payment standards that need to evolve to support EUDI Wallets in the field of payments. EWC has defined as a priority the engagement with standardisation bodies to help tackling the challenge above:

- **OpenID Foundation**

A key requirement for compliance with PSD2 is for the EUDI Wallet to be able to display the merchant name, amount and currency before the payer can approve the payment (so called “dynamic linking” requirement). This information is by nature dynamic and changes per

Co-funded by the European Union

transaction, but in OpenID4VP, the presentation capability was only supporting static attestation exchange.

EWC (represented by Visa) has engaged with OIDF to develop a new presentation feature called “transaction_data”, that is now **included in OpenID4VP draft 23**.

- **EMVco**

EMVCo is a global organisation that manages and evolves EMV Specifications and supporting programmes that enable card-based payment products to work together seamlessly and securely worldwide.

EWC (represented by Visa) has engaged with EMVco to develop a White Paper that addresses the requirements of the EMV 3DS protocol when integrating with an authentication method such as the European Digital Identity (EUDI) Wallet. It was published in June 2025 and can be downloaded here.

- **Berlin Group**

The 'Berlin Group' is a pan-European payments interoperability standards and harmonisation body in charge of definition of Open Banking specifications, and in particular the so called Payment Initiation Services for account to account payments (SCT or SCTInst) as defined by PSD2, and that would also be impacted by eIDAS2 SCA obligations. Note that not all EU banks are following BG technical specifications, there are other Pan-EU standardisation bodies in that field (eg STET, Polish APIs, …) but BG is the largest one in terms of participants. That is why EWC decided to start from there, not to exclude the others but due to limited resources.

EWC (represented by Tink) has developed a draft White Paper that has been shared with BG in March 2025 for review by the openFinance Expert Group. At the time of writing that report, BG openFinance Taskforce is in the process of reviewing the proposal.

(the draft white paper is not public yet, but included in the Archive pack joint to that report)

3.8 Contribution to other EWC deliverables

EWC’s payment taskforce has also been involved in cross-consortium activities:

1) the design of WP3’s IBAN for business rulebook and data schema, providing expertise in the field of IBAN and account payments,
2) analysing and defining the business model for payments for input to the WP2 D4.5 Economic Model and provided
3) actively contribute to dissemination of our activities and developed communication materials in collaboration with WP5:

a) EWC Payment Interest group

We have setup in October 2024 the Payment Interest group to increase awareness and understanding of the EWC payment taskforce developments within payment and identity broader communities (outside EWC), collect feedbacks and continue the exchanges in bilateral if needed

We ran 5 quarterly webinars where EWC’s payment task force shared the high level flows & UX, strategic roadmap, overall project progress, key learnings and identified blockers (not exhaustive).

Co-funded by the European Union

Any private company, government/public organization, industry body, even if they are not an EWC member (AP, BEN, ERP) could join.

As of July 2025, here is the list of participants

Merchants	Amazon, Expedia, ByteDance, Etsy, Free Now, Netflix, Sony, TicketMaster, Tier-Dott, La Poste	**Standardisation bodies**	EMVco, Berlin Group, EPC (European Payment Council), EPSG (European Payment Stakeholder Group)
Financial organisations	Banca Sella, BNP Paribas, Checkout, DSGV, Intesa San Paolo, EPI company, JP Morgan Chase, Nordea, Raiffeisen Digital, SEB, Stripe, ING Poland	**Professional associations**	DPA (Dutch Payment Association), PSA (Payment Services Austria), ABIlab (Italian Banking Association), Finanssiala (Finnish Banking Association), IATA (International Air Transport Association), EPIF (European Payment Institution Federation)
Wallet providers	Docaposte, Evrotrust, Gataca, Walt.id, Samsung	**Government / Public organisation**	Bank of Finland, European Commission, Traficom (Finnish Transport and Communications Agency), Keva
Technology and service providers	Accenture, Cryptomatic, Endaevour 3D Secure, Finegan, Infocert, Nord Security, ReceiptHero, Microsoft, Oliver Wyman, OnePoint, T-system	**+ EWC members**	70 public/private companies accross 27+ Member States (*);
Card schemes	American Express, JCB, Mastercard		

b) White Paper "what does it take to use the EUDI Wallet for payments?"

Published in October 2024 (before the pilots), this White Paper has been developed to start educating the payment and identity industries about the challenges and opportunities for the EUDI Wallet in payments

c) Public Conferences & presentations to industry bodies and key stakeholders

Communication materials have been produced, in particular EWC Payment Educational deck and pilot videos, that can be found in EWC4s GitHub here, and EWC Lunch Webinar recording and materials about Payments on EWC website.

Co-funded by the European Union

4. Payment Authentication (SCA) production pilot

EWC ran a pilot in production in two phases in March and June 2025. By 'production' we mean:

- production infrastructure for all participants (bank, merchant, PSP, wallet, scheme)
- real citizens using real credentials (passport, card)
- real money movement: card payment transactions fully authenticated, authorized, cleared and settled (visible on the pilot user bank statement)

4.1 Objectives

EWC has defined[5] the following flows for online payments SCA either for card or account:

- *the "bank-led" authentication flow, where the payer's bank does interact with the EUDI Wallet to authenticate the payer*
- *the "merchant-captured" authentication flow, where the merchant (or the merchant's PSP) interacts with the EUDI Wallet to capture the authentication data before providing it back to the payer's bank for approval*
- *a prerequisite to the above flows is that the payer has registered his EUDI Wallet with his bank, which consist of the bank issuing an "SCA attestation" (or "PWA Payment Wallet Attestation") in the payer's EUDI Wallet*

The primary objective of the pilot was therefore to implement in a "real world" environment the above flows and evaluate if they work technically and how to improve where needed. In addition, collect real end-users feedback to evaluate how citizens perceive those new capabilities.

The secondary objective was to implement payment checkout related features that could improve further EUDI Wallet value

- "Fast Checkout" where the payer can choose to share attestations with the merchant to avoid filling online forms (eg name, address, loyalty card) and prove attributes about himself (eg age verification, student status) whilst authenticating the payment in a single tap
- automate the issuance of Payment Receipt issuance and Boarding Pass after payment has been confirmed without requiring a second interaction between the EUDI Wallet and the merchant
- EWC Trusted list implementation, that provides reassurance to wallet users that the merchant or bank is a certified, trusted and valid relying-party.

Pilot KPIs (Key Performance Indicator)

- both bank-led and merchant-captured flows live in production
- 50+ transactions in production in Q2 2025 across both flows

Note that we decided to set the target to this relatively small but controlled number of transactions so that the pilot partners and in particular the bank were comfortable from a risk and compliance perspective.

[5] see EWC "online SCA with EUDIW" Implementation Guide on EWC's Github

Co-funded by the European Union

4.2 Partners and related roles

- Banca Transilvania: A leading Romanian bank, Banca Transilvania is actively involved in digital innovation and is a Visa card issuer.
- BPC: BPC is globally known for its digital banking and payment solutions, often partnering with banks and fintechs to modernize financial services.
- Cyclades Fast Ferries (CFF): A Greek ferry operator, enabling passengers to purchase securely ferry tickets online.
- iGrant.io iGrant.io is a Stockholm-based provider of digital identity wallet infrastructure, specializing in consent-driven data exchange and verification services using verifiable credentials.
- University of the Aegean: An academic partner in the EUDI Wallet pilot, the university provides expertise and technical development capabilities
- Worldline: A global leader in payment and transactional services, Worldline is the existing provider of CFF payment gateway
- Visa: a global payments technology company operating in over 200 countries, enabling digital transactions for consumers, businesses, banks, and government

In addition, WP2 partners have also been involved: Arthur's legal for pilot GDPR and pilot participation T&CS, Gen and Yonder for the landing pages and online surveys.

During the project, we onboarded BPC to EWC as Relying Party and Worldline has applied to become a Beneficiary which has required an amendment to the Grant Agreement.

Co-funded by the European Union

4.3 Scope

During an initial scoping phase, the partners came along with the following key choices, assumptions and limitations for the pilot

- Card payments: we implemented card payments only as the partners volunteering for production did not have the possibility nor capacity to implement account payments (Open Banking PIS) in the available time frame.
- Visa cards only as this is the only scheme supported by the bank partner (note that our specifications are card scheme agnostic)
- Only one card per end-user was allowed
- Registration portal: ideally the citizen would register from his bank online / mobile banking app environment after he securely logged in. For the pilot, due to the sensitivity and roadmap unavailability of the bank app, the registration / SCA attestation issuance was done through the bank Call Center: after a bank representative authenticated the pilot user, he/she then sent an email with a QR code for the citizen to register his wallet. The SCA attestation issuance was not in real-time ("deferred" issuance) so that the bank can proceed with the required checks manually.
- Absence of PID: no member state was available with a valid EUDI Wallet and a PID, we therefore used Passport, leveraging iGrant.io NFC reader capability, and derive a PhotoID
- Lifecycle management of the SCA attestation (eg suppress, disable, …) has not been implemented by the bank. End-users will need to proceed manually.
- PSD2 compliance: assumption that the EUDI Wallet is compliant by design with PSD2 regulation, the absence of outsourcing / bilateral agreement with the wallet and the liability with the bank is acceptable by the bank in this controlled pilot context with limited number of end-users
- User Acceptance Testing (UAT) done in production with cardholders from the project team to avoid building UAT environment across the full value chain (merchant-wallet-bank) to save resources and time

4.4 Implementation & project settings

The partners decided to run the pilot in two phases, starting with the bank-led flow, and then expand the scope to merchant-captured flow plus innovative features (eReceipt, fast checkout, …)

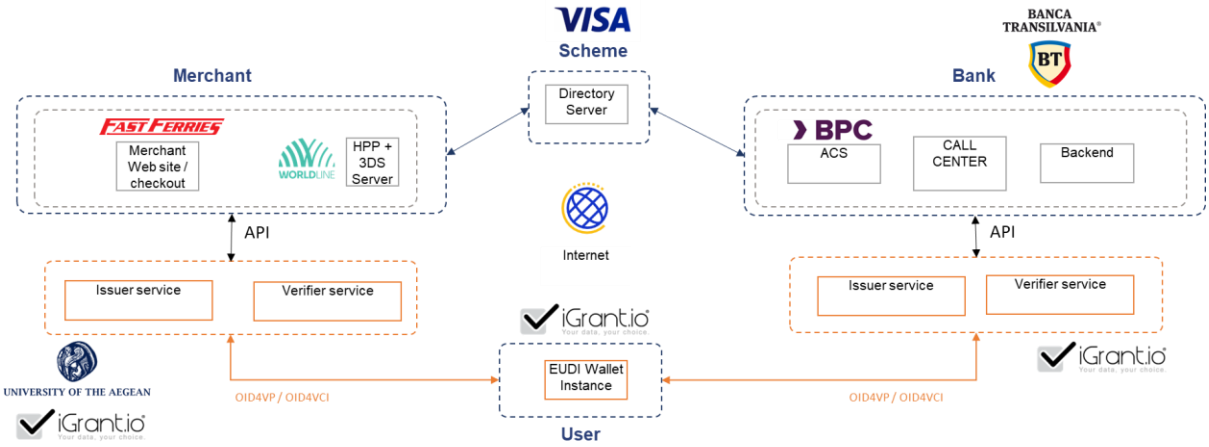
The pilot scoping and planning did start in the summer 2024, and once the partners were committed, the project kicked off in November 2024, during which the partners delivered the following activities:

- Banca Transilvania: Banca Transilvania has implemented registration process for the EUDI Wallet, provided end-users recruitment for the bank-led flow pilot, invested in their authentication production platform (ACS see bellow), provided Call Center support service for the pilot, and testing capabilities (with real cards)
- BPC: BPC provides the card authentication platform (ACS = Authentication Control Server) to Banca Transilvania and has configured the ACS for the pilot and implemented issuing and verification capabilities from iGrant
- Cyclades Fast Ferries (CFF): CFF has developed a new front-end web site to support the EUDI Wallet and payment checkout flow, including "Fast Checkout" button,

Co-funded by the European Union

verification capability for authentication data, PhotoID, loyalty card and student attestation, issuing capability for payment receipt and boarding pass, and changes to payment APIs.

- iGrant.io : iGrant provides the pilot with an EUDI Wallet, and verifying / issuing capabilities to both Banca Transilvania and Cyclades Fast Ferries. iGrant has implemented EWC specifications in wallet and verification/issuance platforms.
- University of the Aegean: designing of the Fast Checkout flow for CFF, and providing the necessary wallet connectors to seamlessly integrate the merchant with an organisational EUDI Wallet
- Worldline: has enhanced their existing APIs to support merchant-captured flow.
- Visa: Visa leads EWC payment taskforce, providing expertise and acting as pilot project lead (including finding committed partners, defining objectives, scope and plan, ensuring pilot is delivered against agreed plan, reporting). Visa also provided the Directory Server that carries the authentication messages between Merchant's PSP and the bank.



4.5 End-users pilot

This truly pan European cross border use case involved real Romanian citizens.

4.5.1 User story

A Romanian Citizen client of Banca Transilvania studying in a Greek or Romanian University wants to take a break and enjoy the Cyclades Islands. He therefore goes to CFF web site to buy a ferry ticket, using his EUDIW for authenticating the card payment and sharing his student attestation to benefit from a student discount and identity credentials (PhotoID, derived from the passport) to avoid manual key entry. After payment is confirmed, the student receives the receipt and boarding pass in his wallet.

Pre-requisites:

- provisioning of the student Romanian Passport in iGrant Data Wallet and registering his wallet with Banca Transilvania to enable the wallet for online SCA

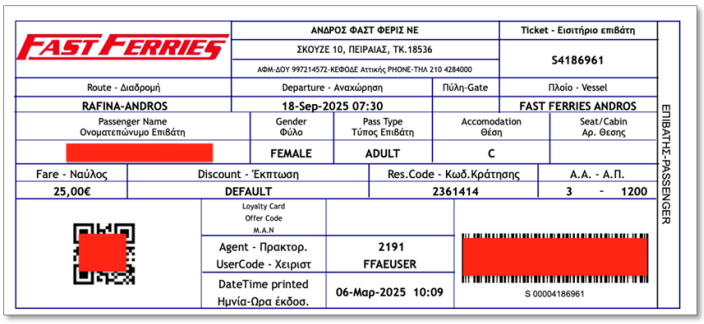
Co-funded by the European Union

- provisioning of the student attestation so as to benefit from reduced ticket price by simply presenting his digital student credential at checkout

4.5.2 Bank-led flow in March

In March the “bank-led” authentication flow, where the payer’s bank interacts with the EUDI Wallet to authenticate the payer, went live in production - including the registration of the EUDI Wallet with the bank, which consists of the bank issuing an “SCA attestation” (or “PWA Payment Wallet Attestation”) in the payer’s EUDI Wallet

The first ever payment in production enabled by an EUDI Wallet has been completed on the 6th of March 2025: a 25 euros ferry ticket purchase.



FAST FERRIES

ΑΝΔΡΟΣ ΦΑΣΤ ΦΕΡΙΣ ΝΕ
ΣΚΟΥΖΕ 10, ΠΕΙΡΑΙΑΣ, ΤΚ.18536
ΑΦΜ-ΔΟΥ 997214572-ΚΕΦΟΔΕ Αττικής PHONE-ΤΗΛ 210 4284000

Ticket - Εισιτήριο επιβάτη: S4186961

Route - Διαδρομή	Departure - Αναχώρηση	Πύλη-Gate	Πλοίο - Vessel
RAFINA-ANDROS	18-Sep-2025 07:30		FAST FERRIES ANDROS

Passenger Name Ονοματεπώνυμο Επιβάτη	Gender Φύλο	Pass Type Τύπος Επιβάτη	Accomodation Θέση	Seat/Cabin Αρ. Θεσης
[redacted]	FEMALE	ADULT	C	

Fare - Ναύλος	Discount - Έκπτωση	Res.Code - Κωδ.Κράτησης	Α.Α. - Α.Π.
25,00€	DEFAULT	2361414	3 - 1200

Loyalty Card Offer Code Μ.Α.Ν		
Agent - Πρακτορ. UserCode - Χειριστ	2191 FFAEUSER	
DateTime printed Ημνία-Ωρα έκδοσ.	06-Μαρ-2025 10:09	S 00004186961

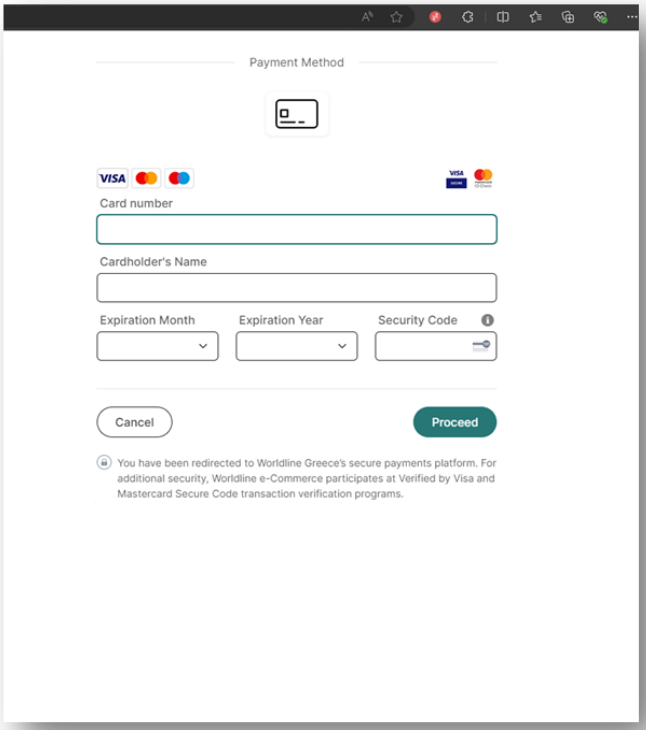
ΕΠΙΒΑΤΗΣ-PASSENGER

This transaction was completed by a Banca Transilvania employee from the Cyclades Fast Ferries website https://fastferries.com.gr/ .

As we were struggling to get students to register for the pilot, we decided to pivot to transactions from a Romanian charity website https://www.viatransilvanica.com/ro/doneaza/ with the recruitment of the pilot users led by Banca Transilvania. Post transaction, the pilot users could provide feedback using an online survey form.

Co-funded by the European Union

UX/UI implementation[6]



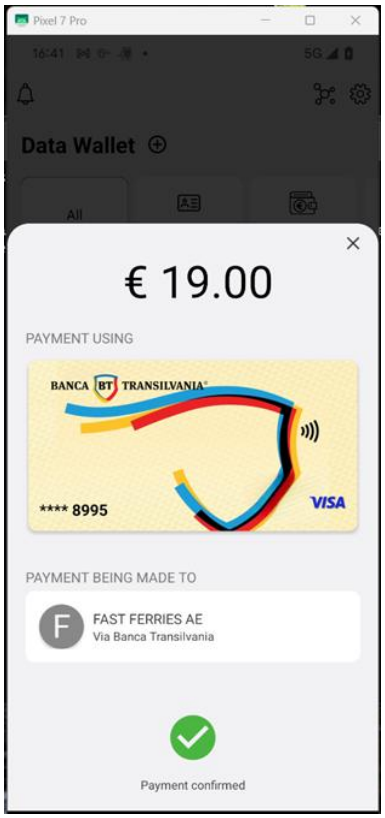
1 - users choose to pay by card as they are used to - they are then asked to type in their card details

Note: works with any merchant, no changes are needed on the merchant side to support that flow.

2 - after they have typed in their card details, the bank displays a QR code (cross device flow) or provides a link / button (same device flows)

[6] Video of the bank-led flow and recording of an actual payment made in production can be found in EWC's Github https://github.com/EWC-consortium/eudi-wallet-papers-and-discussions

Co-funded by the European Union

3 - 

the user scans the QR code, reviews the amount and merchant names in wallet, and confirms the payment in one tap.

4.5.3 Merchant-captured in June

The March pilot was followed by the implementation in June in production of the "merchant-captured" authentication flow, where the merchant (or the merchant's PSP) interacts with the EUDI Wallet to capture the authentication data before providing it back to the payer's bank for approval. No changes were needed for the registration with the bank.

The value-added services were also implemented:

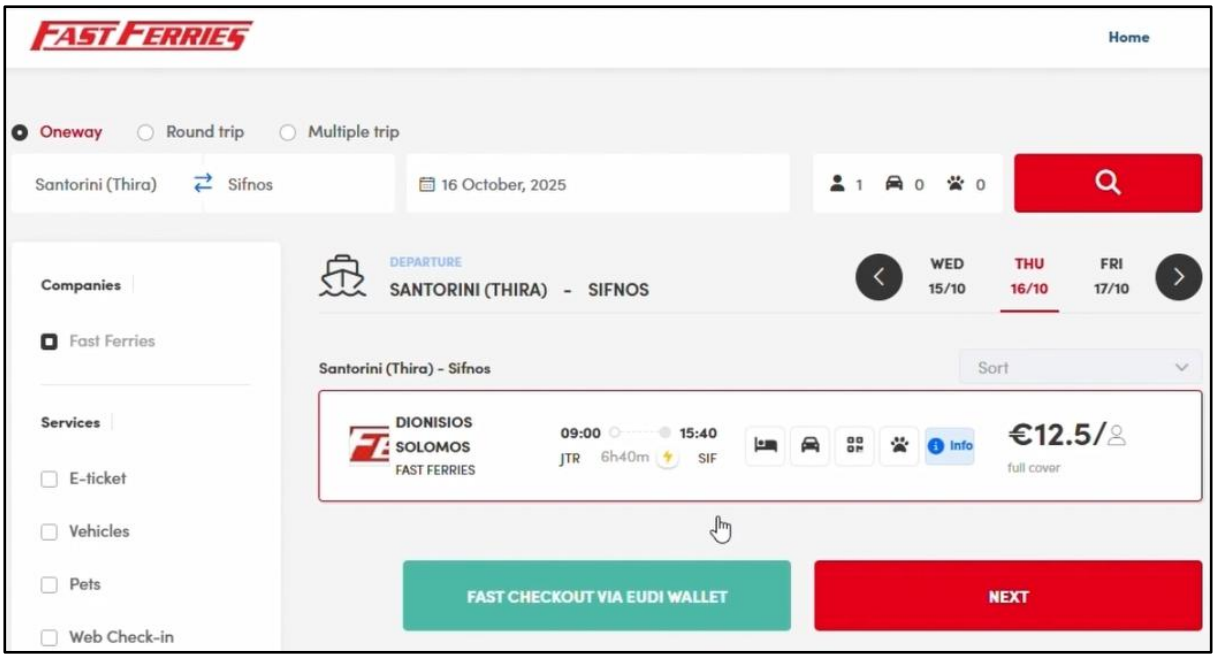
- "Fast Checkout" button
- Payment Receipt and Boarding Pass issuance
- EWC Trusted list

Pilot users have been recruited by the University of the Aegean, and post transaction they were asked to respond to an online survey.

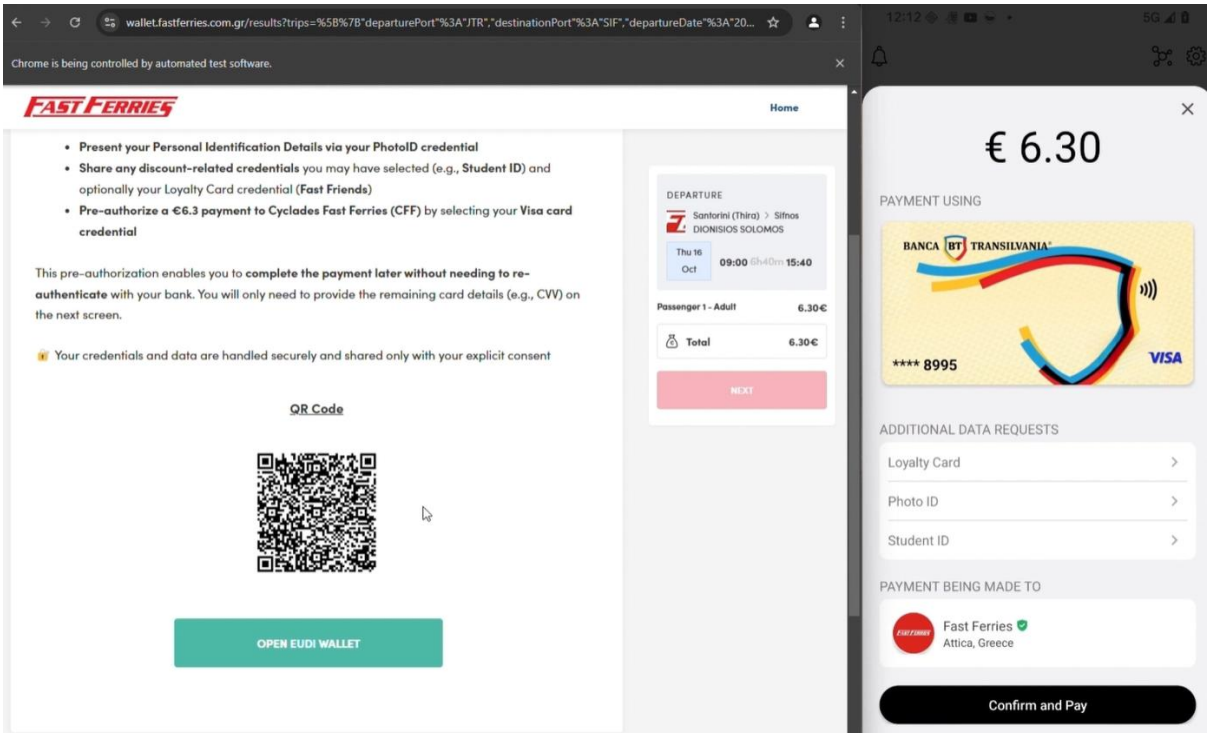
Co-funded by the European Union

UX/UI implementation

(video of a merchant-captured payment made in production can be found in EWC's Github fttps://github.com/EWC-consortium/eudi-wallet-papers-and-discussions)



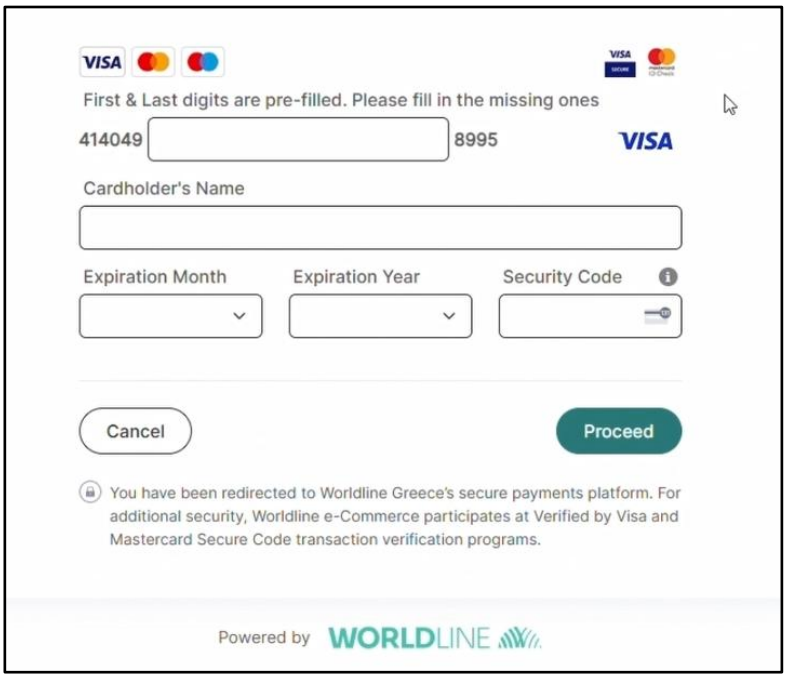
1 - Fast Checkout option enables to skip manual key entry by sharing Passport/Photo ID details from the EUDI Wallet



Co-funded by the European Union

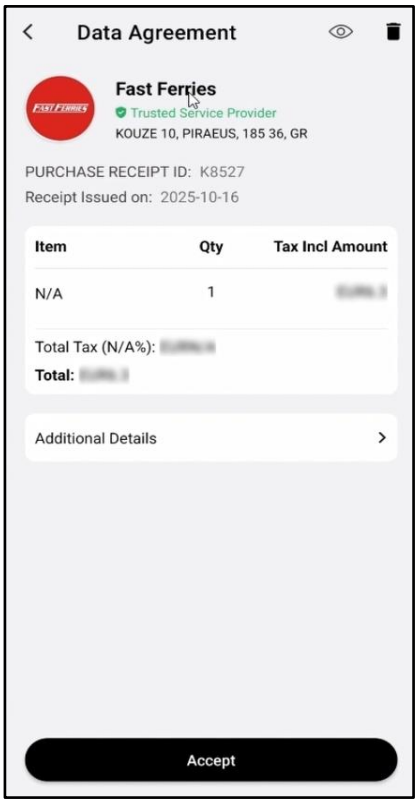
2 - User can review the amount and merchant name before confirming the payment.

User can consent to share additional data (Photo ID, Student ID, Loyalty card details) to avoid filling online forms (name, address, loyalty card) and prove attributes about himself (student status) whilst authenticating the payment in a single tap. *The Trusted mark (green check) provides reassurance to wallet users that the merchant is a certified, trusted and valid relying-party.*



3 - User just need to type in partial card details (first 6 digits and last 4 digits of the card are prefilled from the SCA Attestation)

Note: due to compliance with card industry standard PCI DSS, the full card details cannot be stored in the wallet. In future versions we expect to remove the need to type in any card details using card tokenization capabilities.



4 - the payment receipt and boarding pass are automatically issued after payment has been confirmed without requiring a second interaction between the EUDI Wallet and the merchant

Co-funded by the European Union

4.6 Key Results

1) A successful technical implementation in production

"EWC has delivered in March 2025 the first payment ever made in production with an EUDI Wallet"

Going live in production with real citizens was an ambitious goal set by the pilot partners. However, this approach provided far more valuable insights than a purely technical proof of concept. Beyond ensuring technical functionality, the service had to be truly usable by real citizens—addressing user experience, terms and conditions, technical support, refund capability, and more.

2) KPIs targets completed

With 61 **transactions in production** (49 in phase 1 bank-led, 12 for phase 2 merchant-captured), we have exceeded our target of 50.

Note that we decided to set the target to this relatively small but controlled number of transactions so that the participants and in particular the bank was comfortable from a risk and compliance perspective, and the merchant who will need to manually handle the refunds.

3) End-users feedback collected

We have collected **feedback from 22 end-users** (bank-led flow 17 users; merchant-captured 5 users).

Unfortunately the merchant-captured June pilot survey was open for only 2 days, which has limited the number of feedback received.

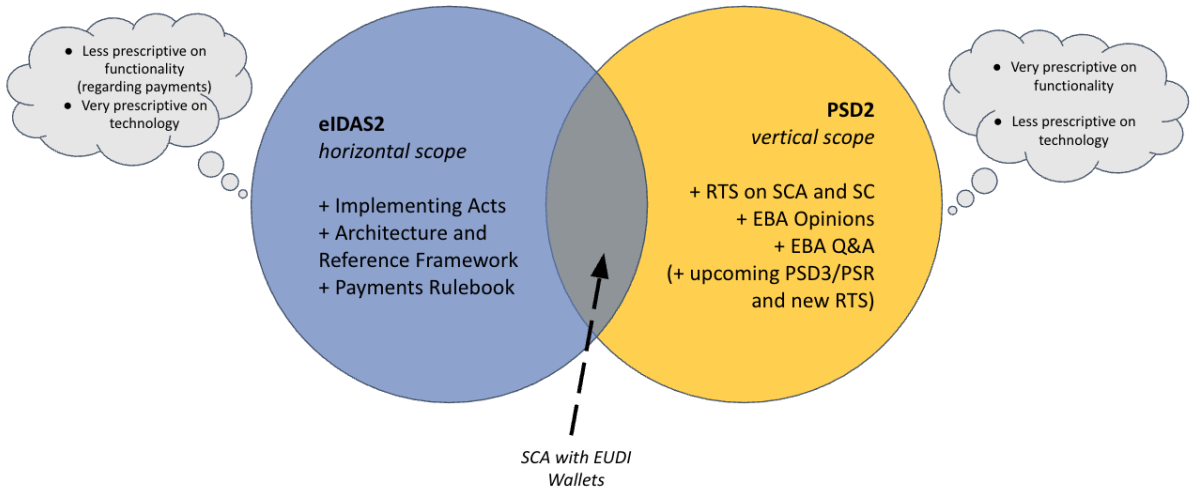
4.7 Regulatory considerations

Utilising the EUDI Wallet to perform SCA is a novel approach which faces unique challenges. While all wallets use cases will need to cater for standard requirements such as GDPR, the payments solution needs to specifically satisfy requirements at the intersection of two major regulatory frameworks, the (revised) eIDAS regulation as well as the PSD2 directive.

While PSD2 is well established and has been refined over the years by introducing EBA's Regulatory Technical Standards, EBA Opinions and the Single Q&A, it predates the very concept of an European identity wallet, sometimes making it difficult to apply its rules to this new setup. eIDAS2, on the other hand, is still very much evolving with Implementing Acts and the ARF being updated as this report is being written. Furthermore, the two frameworks take different approaches when looking at the degree of prescriptiveness regarding functionality and technology.

Co-funded by the European Union

A characterisation of the regulatory landscape around SCA with EUDI Wallets can be visualised as follows:



EWC has therefore developed its solution specifically with the target to meet applicable requirements from PSD2 with the (anticipated) technology available under eIDAS2.

4.7.1 Strong Customer Authentication (SCA)

PSD2 requires SCA for a number of use cases, including making payments online. The main elements of SCA are two-factor authentication and dynamic linking.

Two-factor authentication

The EWC solution approaches this requirement by leveraging core capabilities of EUDI Wallets, which will need to be certified at LoA High.

Before being able to confirm a payment at the point of transaction, the user needs to complete a “Registration” process with his/her bank, which results in a dedicated, functional credential (which we call the “SCA Attestation”) being issued into the user’s wallet. The SCA Attestation is cryptographically bound to the user’s wallet’s private key, which in turn is bound to the wallet instance (i.e. the device).

When confirming a payment, to present this SCA Attestation, the user needs to successfully provide a knowledge (e.g. password/PIN) or inherence factor (e.g. device biometrics) to the wallet. This will unlock the device-bound private key (possession factor), which is used to sign the verifiable presentation. The bank can validate this signed message as it knows the corresponding public key from the Registration process.

Dynamic linking

The EWC solution approaches this requirement by leveraging the newly introduced “transaction data” feature of the *OpenID for Verifiable Presentations* protocol. As part of this, when requesting the wallet to present the SCA Attestation, the requestor can transmit dynamic linking information specific to the transaction (typically the amount and payee as a minimum) alongside. The wallet will display this data to the user when asking to confirm the payment and include it in the signed response. The wallet also generates and includes a unique, verifiable code which can serve as authentication code as per PSD2 RTS requirements. This

Co-funded by the European Union

way, the bank can validate that the user has seen and confirmed the transaction details and that the transaction was not sent multiple times (known as replay attack).

4.7.2 Delegation and outsourcing

Under PSD2, banks can delegate SCA to another party. Assessing whether this is the case in a given situation is often not a black-or-white exercise. In general, it can be said that delegation happens when a payment services provider relies on a third party to decide whether the SCA requirements are fulfilled, and therefore, if the authentication was successful..

SCA delegation requires an outsourcing agreement between the bank and the party which authentication has been delegated to, which is subject to compliance of outsourcing regulatory requirements. Considering that in the case of EUDI Wallets the picture consists of several thousand banks across Europe and at least 27 wallet providers, EWC has come to the conclusion that a need for point-to-point outsourcing agreements between all these actors is not desirable.

The EWC solution has hence been designed to avoid delegating authentication, and hence outsourcing agreements would not be necessary, for the following reasons:

- To issue the SCA Attestation as part of the Registration process, the bank first authenticates the account holder using an existing SCA-compliant mechanism under the control of the bank and securely associates him/her with his/her wallet.
- The bank (or an intermediary on behalf of the bank) issues an SCA Attestation into the EU DI wallet of the account or card holder, which means that the bank relies on the wallet as “third party technology” only – similar to how banks today are utilising a phone’s fingerprint reader or Face ID capability for their SCA solutions.
- The decision on whether the SCA requirements have been met always stays with the bank – in the case where the payee/PISP captures the authentication output, it is passed on to the payer’s bank. In either case the bank remains in control and can decide whether to accept, step-up with additional measures, or to decline.

As this report is being written, EWC (together with NOBID) are actively engaging with the Commission to validate the concept being described above and its legitimacy under the PSD2 and upcoming PSD3/PSR regulatory regimes.

Co-funded by the European Union

4.8 Learnings

1) EWC specifications have proven to work in production

The payment industry now has a technical solution to support the EUDI Wallet as an online payment strong customer authentication method. They are the solid foundations on which the upcoming Payment Rulebook and Use Case Manual will be based.

2) Existing standards can support the online payment SCA use case in a pilot, but more work is needed for scalability

a) **OpenID4VP** draft 23 can transport the necessary dynamic data for PSD2 compliance (merchant name and amount) using the new transaction_data feature.

⇒ It now needs to be released as v1.0 to be referenced in the Implementing Acts.

b) **EMV 3DS** can support merchant-captured flows in its current version 2.2.0 (using a generic existing field to pass the authentication data back to the bank).

⇒ Further standardisation is needed to ensure scalability (see EMVco White Paper)

- Details of the data provided by an EUDI Wallet authentication in a merchant-captured transaction
- Clarification for invoking an EUDI Wallet Instance from an iFrame using a Universal App Link on the same mobile device (in the pilot, the payment page was invoked by a redirect, not from an iFrame)

3) Data privacy / GDPR: data controller / processor roles need to be clarified

Within the framework of piloting activities at EWC, the EUDI Wallet has been tested in a payment production environment that includes processing real personal data. When preparing the required legal documents, especially consent forms and information sheets for processing personal data, it has been difficult to define roles, particularly related to data processing activities occurring within the wallet.

Based on existing studies, such as "Allocating Controllership in the European Digital Identity Wallet" (Timón López, 2021) and Annex B of the thesis “The eIDAS2 Regulation : the European Union’s Strategic Vision to Regulate a Digital Identity Metasystem under Citizens’ Control as a Public Service” (Timón López,2024),explaining the applicability of current criteria and guidelines for the determination of the purposes and the means in data processing activities, and therefore, the qualification as data controller, it seems probable that the wallet provider will be regarded as a data controller for the data processing activities that occur within the wallet. More specifically, this policy recommendation explains that, based on existing

Co-funded by the European Union

research, the developers of an application, or in this case, a digital wallet, have the primary control over how data are processed. They determine the purposes of data processing by transforming the data into tangible actions or outcomes. This raises a pertinent question: how can an entity assume the role of data controller without actual access to the data? However, European case law has from the European Court of Justice (ECJ) already supported this concept. For instance, in paragraphs 69 and 82 of the Fashion ID case (Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV, 2019) and paragraph 69 of the Jehovan Todistajat case (Tietosuojavaltuutettu v Jehovan Todistajat, 2018), it was established that a party's actual access to the data is irrelevant when determining its role as a data controller.

However, during the development of this pilot, it was observed that iGrant, the wallet provider, argues that it plays the role of data controller for data processing activities occurring within the wallet. They notably highlight their inability to “effectively control” or even access the data. This is reasonable given the burden this would impose on them, especially since several aspects remain unclear regarding the exercise of traditional GDPR rights, such as the right of access to personal data, which may not make sense in this context, or the extent of the wallet provider's responsibility. For example, the wallet provider should not be held responsible for all decisions made by the user regarding their personal data. Given the necessity to give this pilot a “temporary solution”, iGrant included a provision in their privacy policy to address this, while also contextualising the specific circumstances surrounding this data processing:

The iGrant.io digital identity wallet is a secure software solution specifically designed for individuals to safely store their digital identity credentials. Although iGrant.io implements strong security and privacy measures to protect your personal data, we do not have access to any credentials or data stored within your wallet. This ensures that you retain full control over your information, empowering you to securely share your data with third parties, strictly according to your preferences and their respective policies.

Nevertheless, this solution is only temporary and requires further elaboration, considering the different modalities for the provision of the European Digital Identity Wallet (i.e., directly by a Member State, under its mandate, or independently, but recognised by it), which could lead to different data controllership implications. For instance, if provided directly by a Member State, the public agency or body offering the wallet would likely be considered the data controller. In cases of indirect provision, a data controller-processor relationship might exist. Finally, the scenario where digital identity wallets are recognised but provided independently may be the most complex from a data protection perspective, potentially imposing an excessive burden on the wallet provider.

Consequently, due to the challenges faced during this pilot, it is advisable for the European Data Protection Supervisor to issue guidance clarifying the role of the data controller in the various scenarios for issuing the European Digital Identity Wallet, as specified in Article 5a, paragraph 2 of the eIDAS 2 Regulation. Such guidance should consider the different stakes involved, especially by clearly defining the responsibilities of the wallet provider within the context of empowering users to make decisions regarding their personal data.

Co-funded by the European Union

4) **Legal: bank clients have to agree with new T&Cs**

Participants in the pilot program were required to be informed and provide consent that, by adding the card to the EUDI Wallet, it would be used exclusively to confirm (approve or reject) online payments made with the pilot card—only for transactions with merchants participating in the pilot—via the iGrant Data Wallet.

All other financial operations performed by the client using this card, including online payments to merchants outside the pilot, remained unaffected.

Since the registration and SCA attestation were completed through the bank's Call Center, client consent for this specific amendment to the bank's Terms and Conditions—applicable solely for the pilot—was obtained during the enrollment process via the Call Center. This consent effectively replaced a dedicated set of Terms and Conditions for EUDI Wallet usage, which would otherwise outline all permitted financial operations and aspects related to managing the SCA Attestation. *

5) **User Acceptance: survey early results are very positive**

- Bank-led flow

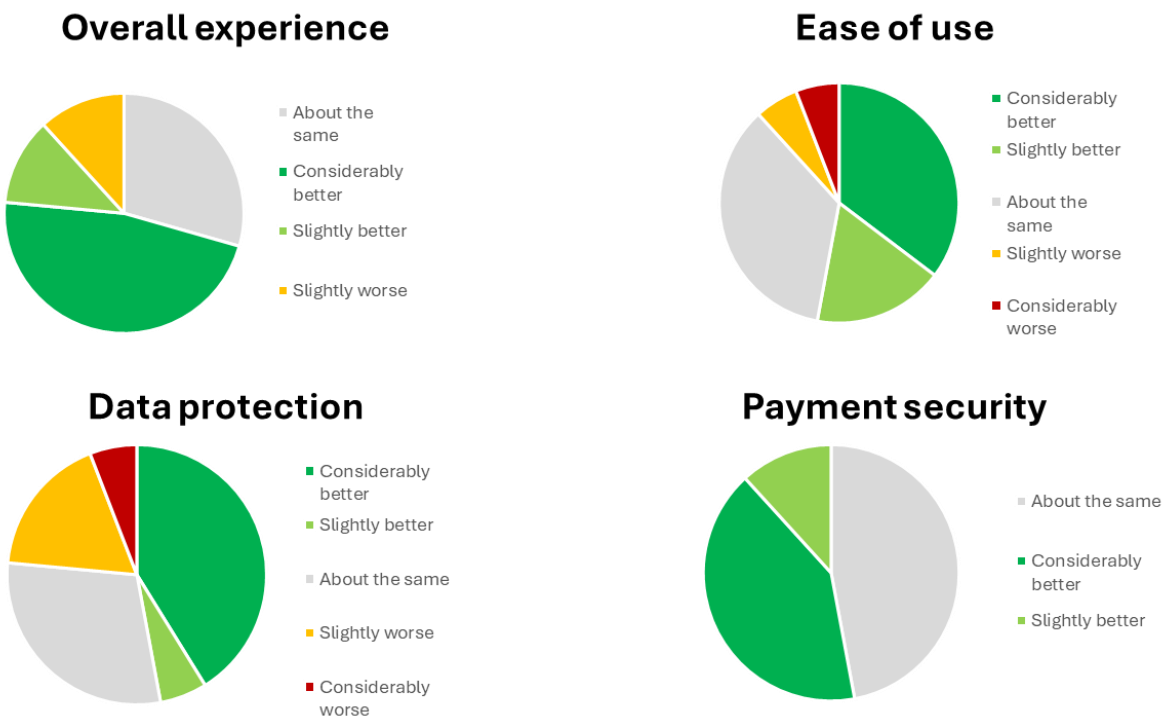
Early results show a **positive acceptance with 59% having a better overall experience** compared to the existing authentication flow. Interestingly, the **perceived security of the EUDI Wallet for payment was equal or higher (53%)** than with the existing authentication app.

Consequently, **more than half of the users (53%) were 'very likely' to switch to EUDI Wallet** if this option was proposed by their bank in the future.

Disclaimer: we could only survey a very small number of participants with specific profiles (employees from Banca Transilvania and their technical partners) so the results may not be representative of the real situation.

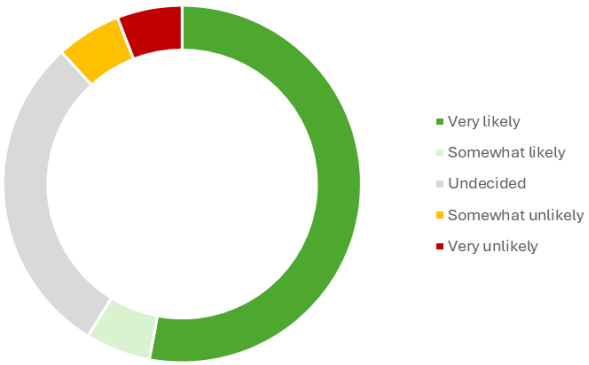
Co-funded by the European Union

"How would you rank the EU digital wallet experience versus the way you currently authenticate online payments with the Banca Transilvania app today? (Please only take into consideration the payment phase, not the registration with the bank phase)"



Results from using the EUDIW to authenticate payment donations at a romanian charity merchant in production / bank-led flow – DISCLAIMER: results are based on only 17 digital payment savvy respondants, briefed individually on EUDIW and are therefore not necessarily representative of the actual market situation

"Would you switch to an EUDI Wallet for authenticating your online payments if your bank proposes you this option in the future ?"



Users with negative views have expressed the following concerns in verbatims:

Co-funded by the European Union

"This feels like everything a scammer would want in one place."

"Considering that the app stores very sensitive personal data, I would like to know how its storage is handled and by which organisation specifically before I trust the wallet"

"I'm using BTPay for all my banking needs, so it would be difficult to switch to another app just for the online payments authorization."

"Nobody want to install a new app for a functionality that already exists"

This should be taken into consideration when building the communication / educational package as this relates to reassurance (security, data protection) and benefits of using EUDI Wallet for SCA.

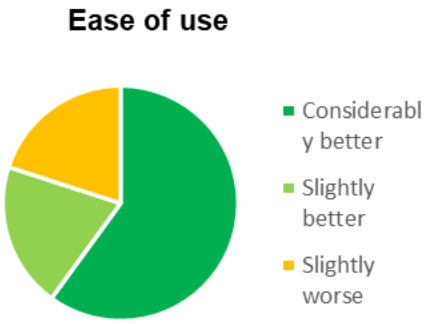
- Merchant-captured flow

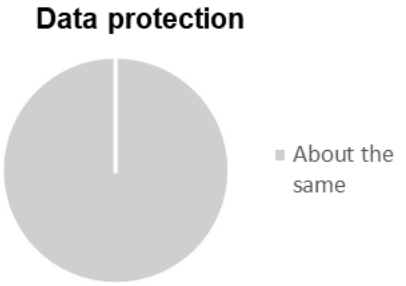
Early results show a **very positive acceptance with 80% having a better overall experience** and finding it **easier to use** compared to a standard online checkout flow, without impacting the perception of **data protection and payment security that stays neutral**.

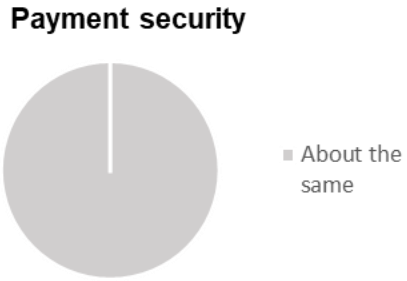
Disclaimer: we could only survey a very small number of participants with specific profiles (students) so the results may not be representative of the real situation.

Co-funded by the European Union

"Compared to your usual card or bank app checkout, how would you rate the EUDI Wallet on each aspect below?

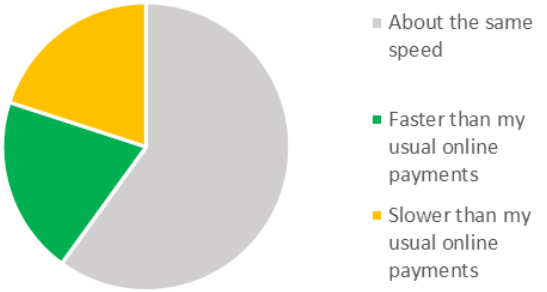






Perceived **checkout speed is good**, but could be **improved by introducing UX improvements** including removing manual card details entry and avoiding app swaping:

"Overall, the wallet checkout felt:"



"I had to swap between apps a lot"

"I liked the fact that my data were already entered in the application, and when I needed them for payment, they were already selected (student card, bank card, passport data)."

"It was fast and worked good."

"I guess it's nice that it's everything in the same place, but I can't remember a time where I needed to introduce more than just my banking information […] And the information that is requested to complete a transaction like name address etc is automatically completed because it's saved in my browser."

"For each payment you have to introduce bank card numbers"

"It took a lot to introduce your bank card informations every time."

Co-funded by the European Union

Overall, users do see the value and are **very likely to use it and promote it in the future**, with a net promoter score **NPS of 75** which is very good in a pilot (bugs, UX limitations, …)

"Would you use this wallet method again? Why / why not?"

"Yes, because I have all documents in one app"

"Yes, I would because all the documents are in the same place."

"Yes, I would use it again but after the developers fix all the bugs. It's a very cool concept, I love the idea"

"Yes, I would. It's easy to use because you introduce your data once, and then use it when you need it. For example, when you need the student discount, you don't have to enter all the data again. "

"How likely are you to recommend paying with the EUDI Wallet to friends or colleagues?:"

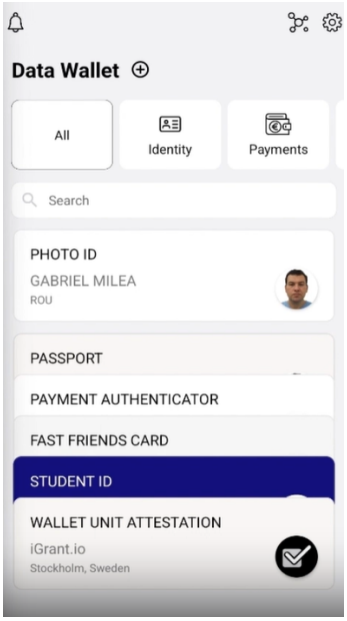
•Promoters (Score 9-10): 75%
•Passives (Score 7-8): 25%
•Detractors (Score 0-6): 0%

Net Promoter Score (NPS): 75

6) UX/UI considerations

- EUDI Wallet UI
  - PSD2 compliance

EUDI Wallets need to display the merchant name, the amount and currency of the transaction to ensure compliance with dynamic linking PSD2 requirements.



We have implemented a double strong authentication (when opening the wallet to comply with eIDAS2, then when confirming the payment to comply with PSD2 and (optionally) sharing additional attributes with user consent).

  - UI display and naming of the SCA attestation

The SCA attestation is a rather technical attestation and a concept not easy to understand by citizens.

Although it can contain some payment credential details (eg last 4 digits of the card, IBAN digits, card art visual) that can be used for display convenience, the SCA attestation is not designed initially for holding full payment credentials that can be used for initiating an online payment.

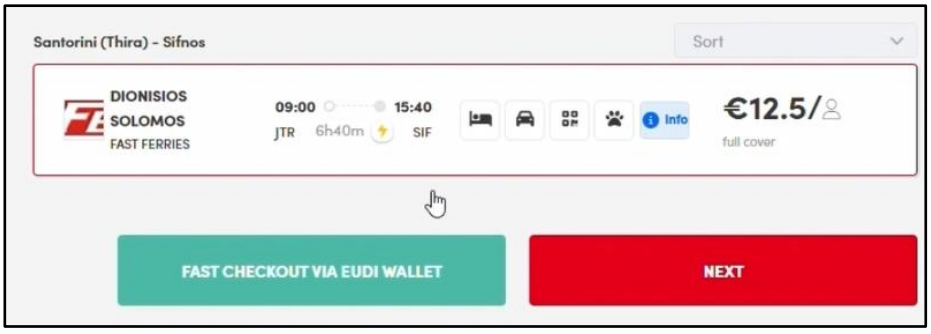
Co-funded by the European Union

To avoid confusion, we have chosen to implement it in the wallet as a "Banca Transilvania payment authenticator", listed amongst the other attestations e.g. PID etc … and not as a payment card (for example like it is today listed in Apple or Google wallets)

When selecting this "payment authenticator" from the main menu, the user can see the payment instruments (cards, accounts - there was only one card in the pilot) linked to that credential.

In addition to the technical specifications, the industry would benefit from having UX/UI guidelines for the EUDI wallet to support payment.

- "Fast Checkout with EUDI Wallet" feature



We have introduced the concept of fast checkout - but going forward, standardisation is required to ensure that this feature can be easily recognized by end users (button, naming, messaging, …)

- App to app switch for same-device flows

For the same-device flow, after confirming the payment in the EUDI Wallet, the user needs to manually switch back to the merchant website to complete the payment. Although not specific to EUDI Wallet (same issue with the bank app), we should be looking at solutions in the future and W3C's Digital Credential APIs may be one of them.

- Manual key entry for the merchant-captured flow

Due to compliance with card industry standard PCI DSS, the full card details (PAN/card number, expiry date, cryptogram) cannot be stored in the wallet, thus the need for the users to type in manually. Although we did simplify the checkout by prefilling the first 6 and last 4 digits of the card, this has created unnecessary friction.

In future versions, we expect to remove the need to type in any card details introducing card tokenization capabilities.

- Future outlook

It is critical for the EUDI Wallet to be accepted by online merchants to deliver seamless and secure checkout UX to the end users.

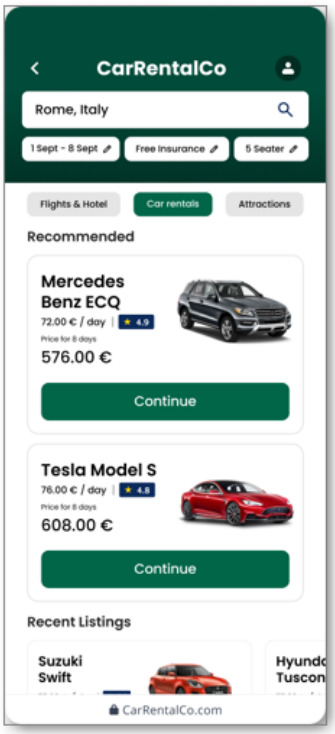
Co-funded by the European Union

This can be achieved by EMVco card tokenization standard, which is already live with the major payment wallets for inApp/eCommerce, and removes the need for the user to type in any card details, in addition to reducing fraud and improving authorization rates.

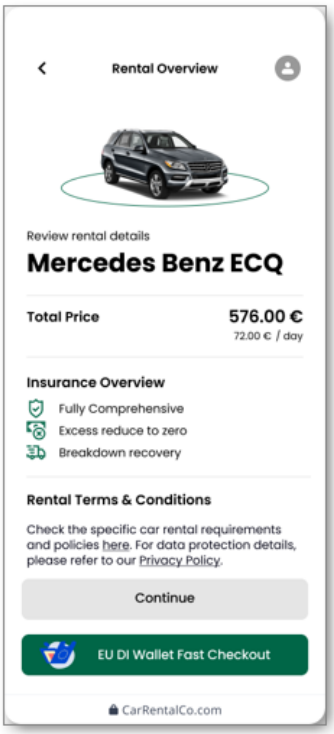
In addition, W3C Digital Credentials has the potential to further improve the UX by removing the need to switch between the Relying party and EUDI Wallet apps, providing to the EUDI Wallet a superior mobile experience compared to the legacy bank-app based authentication.

In the illustration below, we outline how a possible user journey could look like that incorporates both a tokenised card being placed into the wallet as credential as well as usage of the DC API. While still conceptual at this point, it points to promising results with no manual user input and a very small number of steps to complete.

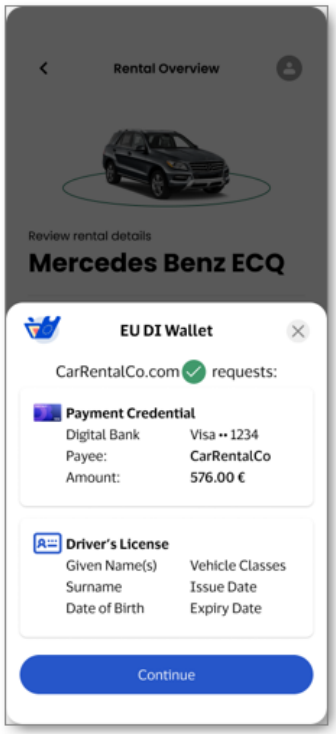
1) User selects good or service at merchant.



2) User chooses fast checkout with EU DI Wallet.

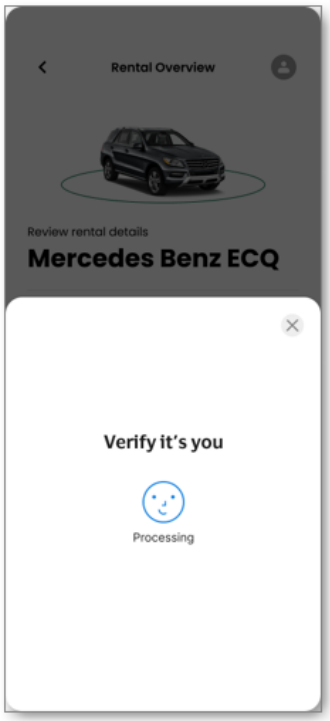


3) Wallet UI comes up. User confirms to release payment and driver's license credentials.

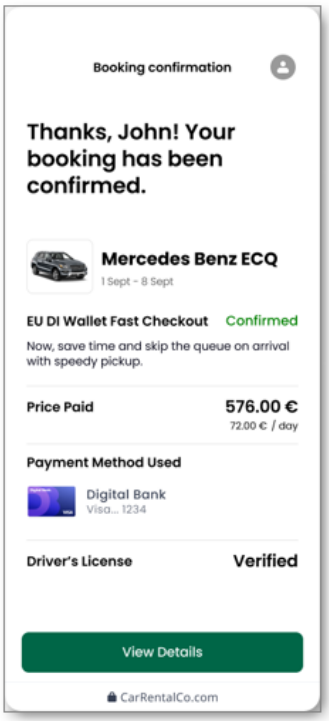


Co-funded by the European Union

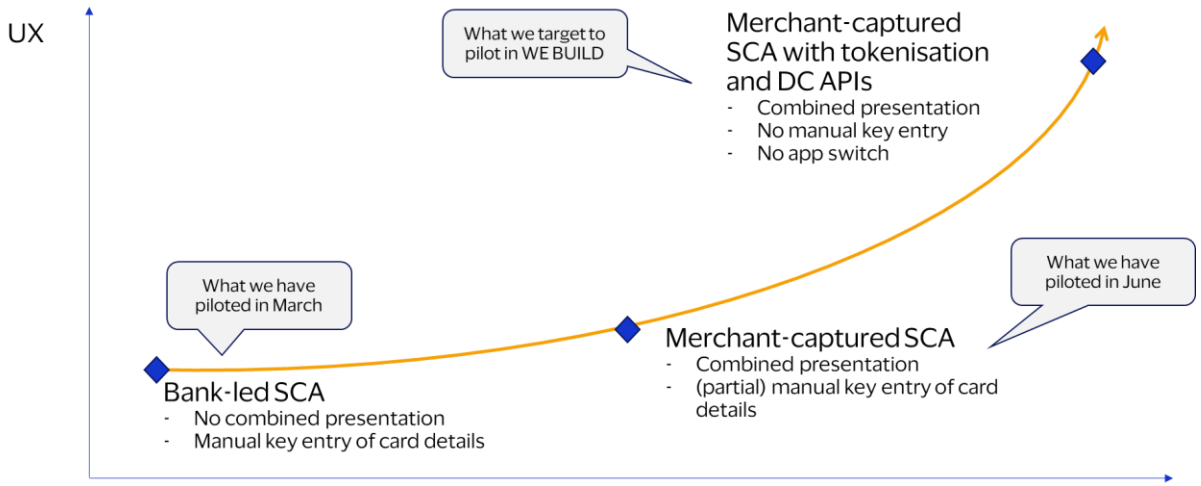
4) User authenticates.



5) Merchant confirms successful wallet data retrieval and validation.



We aim to pilot those two features in the next LSPs, on our journey towards seamless and secure online checkout.



Co-funded by the European Union

7) Technical architecture and implementation learnings

Bank-Side Learnings

a) Overloaded Roadmaps

Bank was unable to integrate EUDI Wallet registration or lifecycle management into their online/mobile platforms during the pilot. These channels are central to customer engagement, and securing development time within them is a major challenge that must be anticipated early.

b) Authentication Platform Impact is Manageable

The impact on the bank's authentication infrastructure (specifically the ACS – Access Control Server) was considered reasonable when using a third-party digital identity stack. This suggests that external integration is a viable path for banks with limited internal capacity.

Merchant-Side Learnings

a) Integration Strategy Matters

In the pilot, EUDI Wallet integration was done directly on the merchant side (Cyclades Fast Ferries), not via the PSP (Worldline). While this worked, PSP-side integration may be more scalable, especially for smaller merchants lacking technical resources. It also opens opportunities for PSPs to offer eIDAS2-compliant services.

b) Technical Limitations

Merchants using iFrames for payment pages face technical constraints. Specifically, sandboxing prevents Universal App Links (used to invoke the wallet) from functioning properly. Hosted payment pages (redirects) are currently more compatible with EUDI Wallet flows

Identity Expertise Gap

Most bank and merchant developers are payment experts—not identity specialists. Building and maintaining identity stacks that support credential issuance, verification, and pan-European wallet compatibility is complex and resource-intensive.

Even when using third-party identity stacks, developers benefit from simplified APIs. Abstraction layers that hide identity-specific complexity (e.g., credential presentations) are essential to accelerate adoption and reduce integration friction.

8) Regulation clarity is required for implementation at scale

The key assumptions agreed for the pilot were that the solution enables PSD2 compliance and that no outsourcing agreement between the bank and the wallet provider is needed. The bank remained liable but with a limited number of users the risk was deemed acceptable.

Co-funded by the European Union

Moving forward, eIDAS2 and PSD2/PSR interplay need to be clarified before the market can implement at scale (and time is running out - see Regulatory considerations)

9) Consumer education and technical support: critical enablers for EUDI Wallet usage

The pilot clearly demonstrated that **comprehensive user education** and **proactive technical support** are not optional—they are essential.

- **Education Needs**:
  - During the pilot, the bank's call center engaged directly with end-users, providing hands-on assistance for registration of the wallet, adding passports, understanding wallet functionalities, and addressing security concerns.
  - Users required clear, accessible information about what the EUDI Wallet is, how it differs from the bank's existing app, and the benefits of using it.
  - Many participants lacked awareness of the wallet's capabilities and needed reassurance about data privacy and security.
  - To support pilot users, a WhatsApp group was created by University of the Aegean for real-time communication. Participants received step-by-step instructions on wallet setup and credential issuance (e.g. Student attestation). Despite written guidance, ongoing support was necessary throughout the pilot to ensure users could navigate the payment flow successfully.

- **Technical Support Challenges**:
  - Adding a passport, particularly via NFC on iOS devices, proved difficult for many users. A detailed instructional video by iGrant was instrumental in overcoming this hurdle. However, this step will not be managed by the bank in real life, and should be replaced by the issuance of the PID by member states.
  - The SCA Attestation issuance process was not fully automated, leading to confusion. Some users attempted to scan the QR code before completing passport enrolment, resulting in errors.Notifications within the Wallet were sometimes overlooked, causing users to miss critical steps like accepting the SCA Attestation.

Most of the complexity came from the preparation of the wallet before the payment: downloading and setting up the wallet, adding a Passport and derive a PhotoID, adding a Student attestation, adding a CFF Loyalty card. In real-life, we expect those steps to be already completed, so that the experience with payments really starts with the registration of the EUDI Wallet with the bank.

We anticipate that in real life, the banks would need to play a key role in educating customers about the benefits and functionality of the wallet, providing reassurance in using it, and providing technical support when payment authentication fails with the EUDI Wallet.

10) Managing end-users pilot for payment requires significant efforts

Co-funded by the European Union

Recruiting end-users and getting them to complete the payment has required important efforts from Banca Transilvania and University of the Aegean.

Despite significant compensations being offered (e.g. headsets), from those users that expressed interest by registering to the pilot, less than half actively participated.

This may be due to 1) complexity of the wallet setup 2) difficulty to understand the concept 3) fear in doing a real payment with risk of not being refunded

Payment is indeed a sensitive use case, it is about people's money. If we want to pilot at scale in the next LSPs, we need to have the right resourcing and focused approach in pilot users management to obtain relevant insights.

4.9 Recommendations

Before being able to move to a commercial grade launch, more work is needed for the next LSPs to ensure the readiness of EUDI Wallet as an SCA method for online payments:

- **Work in close collaboration with the European Commission**
  - to finalize the Payment Rulebook and Use Case Manual. Identity the industry body in charge of maintaining this Rulebook beyond LSPs, as well as certification body and framework for payments
  - to solve for open regulatory issues
  - to ensure that necessary standards are referenced in the Implementing Acts (e.g. OIDV4VP)
  - to develop UX guidelines for the "Fast checkout with EUDI Wallet" feature
- **Continue to improve specifications**
  - UX optimisation (card tokenization, DC APIs)
  - Merchant integration (Payment method acceptance settings, PSP-side integration, iFrame issue)
  - In addition to card, continue to develop for account online payments (Open Banking PIS)
- **Continue to evolve standards**
  - EMV 3DS for cards
  - Berlin Group (and other Open Banking standardisation bodies) for account payments PIS
- **Implement a V2 of the pilot** with features that we could not implement in due time
  - EUDI Wallet Registration from the bank portal (Online / Mobile banking integration) with real-time issuance of the SCA attestation
  - Synergies with the use of EUDI Wallet for login into the portal (e.g. single registration for both login and SCA) and opening a bank account using the wallet for KYC (automatic issuance of an SCA attestation after opening the bank account)
  - Payment credentials implementation variants: multiple cards (from multiple schemes) & accounts, basic SCA attestation without any payment credential

Co-funded by the European Union

    - Lifecycle management of the SCA attestation (delete, suspend, …) alongside with the bank's customer lifecycle management (eg open a new card or bank account, changes device, leaves bank, …) including Card Art management to display visual of the actual card in wallet
    - Transaction log in the wallet, connected to payment receipts
    - Update the platforms with the future Payment Rulebook specifications
    - in addition to cards, implement for account-based online payments (Open Banking PIS)
    - Unhappy flows
    - Cross-wallet validation through interop test beds
- **Gather further benefits for citizens and the payment industry**
    - Run an end-user survey at scale to collect insights representative to the actual EU citizen diversity
    - Evaluate the potential how EUDI wallets can help fighting fraud and improve security for the benefits of banks and merchants - e.g. trust acceptance mark, fraud signals, step up for high-risk transactions
- **Explore all payment online types** including recurring payments and subscriptions, and emerging ones like agentic commerce.

In addition, the payment industry should also start reviewing and preparing for 2027 those non-technical domains that would be impacted:

- **Dispute management and fraud reporting platforms updates**
- **Marketing and Communication**: pilot has shown that communication is key for such an emerging topic. Consumer banks, wallets and merchants need to build messaging, value propositions to drive awareness and usage of the EUDI Wallet for SCA and login.
- **Customer Support**: Consumer banks, wallets and merchants need to update their support channels (eg call center, FAQs, …) processes and train their CSR.
- **Legal**: Consumer banks, wallet providers and merchants need to update their consumer's T&Cs to include the necessary GDPR and Payment regulation (eg PSD2/PSR/RTS) provisions to support the use of the EUDI Wallet for authenticating online payments and/or sharing identity credentials

Co-funded by the European Union

4.10 Key drivers and headwinds for the EUDI Wallet in the online payment SCA space

DRIVERS FOR ADOPTION OR BENEFITS

1. **A single trusted authentication tool for online login and payments**: consumers now have a single authentication tool not only for login securely to multiple online services, but also to authenticate online payments whatever their bank is. Moreover, the EUDI Wallet simplifies the way they shop online (share payment credentials and other attestation and authenticate for payment in one tap) and provides reassurance that they are paying at a trusted merchant
2. **Innovation at online checkout:** merchants can build innovative and seamless fast checkout capabilities by combining payment and verifiable credentials, optimizing their conversion rates and providing high quality verifiable data about buyers. Furthermore, the EUDI Wallet can act as an instrument to streamline the issuance of e-receipts or other digital goods e.g. ticket concert or boarding pass
3. Digital authentication with EUDI Wallet enables faster and simple product pan-EU interoperable sign-up for banks (e.g. opening a bank account or applying for a loan). The EUDI Wallet as an SCA method for online payments use case could be **implemented jointly by banks with low incremental efforts**.
4. EUDI Wallet has also the potential to bring **more security and help fighting against fraud.** In particular, the relying party **access certificate** will ensure that the user is paying at a trusted merchant by checking its trust mark, which is a USP compared to existing authentication solutions - which **will reduce the risk of Authorized Push Payment Fraud (APP)**. Although not piloted, EUDI Wallet could also provide fraud signals during an online payment and step up authentication for high-risk transactions.
5. **Payment use case drives adoption and usage of the EUDI Wallet**: in a context of European digital commerce expansion, governments may be interested in payment as this is a high-frequency use case anchored in European citizens' (almost) daily lives that requires trust, convenience and security. Governments could start accepting the EUDI Wallet to pay at their own government online services.

Headwinds

1. **Consumer adoption**: despite very encouraging customer feedback, changing consumer habits for payment is difficult and will also depend on how banks and governments will educate / promote the EUDI Wallet for payments.
2. **Fast Checkout acceptance**: this optional feature requires significant changes at merchants' checkout and is likely to face a 'chicken and egg' problem as merchant may wait for EUDI Wallets wide adoption before prioritizing implementation.
3. **Bank readiness by end 2027**: the target of 100% EU bank technical readiness by end 2027 is a major challenge. There is still today a lack of awareness from the banking industry, and for banks that are more advanced, we will likely be in a **wait-and-see situation until regulatory clarification is provided**. And upgrading platforms for introducing a new authentication method for both card and account payments represent a significant amount of work.

Co-funded by the European Union

4. **Impact on bank Customer Relationship** if their clients don't use their banking app anymore for online SCA. This could be mitigated from a brand perspective by including the bank logo in the EUDI Wallet (in the pilot the bank logo was visible in both the SCA Attestation and the Card Art)

Co-funded by the European Union

5. Payment Initiation: potential role for the EUDI Wallet

Beyond SCA, EWC has started to explore Payment Initiation where EUDI Wallets can become a true Payment wallet, holding payment credentials (card or account) and initiate a payment for both proximity and remote payments.

5.1 Card payments

The card tokenization technology is widely adopted by the most prominent digital wallets to facilitate both remote/eCommerce/in-app and proximity/NFC card payments.

1) For eCommerce, EUDI Wallets could hold card tokens to streamline the Fast Checkout option by removing the need to type in manually any card details (see Learnings section - Future Outlook). This sounds very promising and could be the first step for the EUDI Wallet to start tokenizing cards - but would need to build a merchant acceptance network.
2) For proximity / in-store payments, EUDI Wallets could benefit from HCE (Host Card Emulation) technology now available on both Android and iOS platforms in Europe, and from the wide acceptance network in-store (Contactless NFC payments) - but will need to convince citizens to switch from the legacy payment wallets.

The HCE/tokenization technology however does not include any Digital Identity technology (e.g. card tokens are not verifiable credentials, and contactless protocol uses different standards than mDL/ISO1813 or OID4VC/VP) but the payment feature could coexist as a separate “card payment stack” in the EUDI Wallet app, alongside with the “eIDAS2 stack”. Much work is needed to unify or develop interactions between both stacks to start creating value with for example combining identity and payment credentials.

We have developed in EWC an Implementation Guide that describes the high-level flows for provisioning card tokens and using it for payment in-store or online using the existing tokenization standards.

5.2 Account payments

We have also developed in EWC a Rulebook, a Data Schema and an Implementation Guide that describe how Natural Persons IBANs can be provisioned as a Verifiable Credentials in the EUDI Wallet and used for a pull payment (Direct Debit), primarily for subscription-based or recurring payments.

We will continue to develop more of those aspects for both card and account payments in the next LSPs.

Co-funded by the European Union

APPENDIX 1 List of payment specific abbreviations

- **3-D Secure (3DS)** – An authentication protocol for online card payments (e.g. "Visa Secure" or "Mastercard Identity Check") that requires the cardholder to complete an extra identity verification step during checkout. 3-D Secure is often used to implement **SCA** on e-commerce transactions (commonly via a one-time code or bank app approval).
- **A2A** – *Account-to-Account* payments, meaning money is transferred directly from the payer's bank account to the payee's bank account. These payments bypass card networks and typically use bank transfer networks (like instant SEPA transfers or open banking payment initiation).
- **AISP** – *Account Information Service Provider*, a type of third-party service introduced by **PSD2**. An AISP (with user consent) can access bank account data to provide services like personal finance dashboards or creditworthiness checks.
- **AML/CFT** – *Anti-Money Laundering / Countering the Financing of Terrorism*. This refers to laws, regulations, and procedures aimed at preventing criminals from legitimizing illicit funds (money laundering) and stopping funds from being used for terrorist activities. Banks and payment providers must follow strict AML/CFT rules (e.g. customer identity verification, transaction monitoring).
- **AMLA** – *Anti-Money Laundering Authority*. A new EU authority established in 2024 to oversee and enforce AML/CFT compliance across member states. AMLA will harmonize how AML rules are supervised, ensuring consistent standards throughout the EU.
- **API** – *Application Programming Interface*. In payments, APIs are the technical interfaces through which software applications communicate. Under **PSD2's** open banking, banks expose APIs to allow **TPPs** (third-party providers) to access accounts or initiate payments securely.
- **ATM** – *Automated Teller Machine*, a cash machine that allows bank customers to withdraw cash and perform basic transactions using a card.
- **BNPL** – *Buy Now, Pay Later*. A payment option that lets consumers split purchases into instalment payments (often interest-free) over time. BNPL services (e.g. Klarna, Afterpay) have grown popular in online shopping, making up an estimated ~5% of global e-commerce spend in 2022.
- **CNP** – *Card-Not-Present*, referring to transactions where the physical card is not present (e.g. online or phone purchases). These typically require extra security steps (like a CVV or SCA) since they carry higher fraud risk.
- **CVV** – *Card Verification Value*, the 3- or 4-digit security code on credit/debit cards (e.g. the number on the back of a Visa/Mastercard). It's used to verify that the customer has the physical card during **CNP** transactions, adding a layer of fraud protection.
- **e-commerce** – *Electronic commerce*, referring to buying and selling goods or services over the internet (online shopping via websites or apps). In this report, it includes desktop and **mobile commerce** transactions.

Co-funded by the European Union

- **EMV** – *Europay, Mastercard, and Visa*, the global standard for chip-based payment cards and terminals. An **EMV** "chip-and-PIN" card contains a secure chip that, together with a PIN or signature, dramatically reduces counterfeit card fraud
- **IBAN** – *International Bank Account Number*. A standardized international format for bank account identifiers used across Europe (and beyond) to facilitate cross-border transfers. An IBAN includes a country code, two check digits, and the domestic bank account number; for example, a French IBAN looks like "FR76….etc." Banks use IBANs for routing payments through systems like **SEPA**.
- **KYC** – *Know Your Customer*. The process by which financial institutions verify the identity and background of their customers (e.g. confirming name, ID documents, address). KYC checks are a fundamental part of **AML/CFT** compliance to prevent fraud and illicit activity.
- **NFC** – *Near Field Communication*. A short-range wireless technology used in contactless payments. NFC enables devices like credit cards, smartphones, or smartwatches to transmit payment information by simply being held near a reader (tap-to-pay).
- **OTP** – *One-Time Password*. A single-use security code, often sent via SMS or generated in an authenticator app, used to verify a user's identity.
- **P2P** – *Peer-to-Peer* (or Person-to-Person). Typically describes direct payments between private individuals.
- **PIN** – *Personal Identification Number*, a secret numeric code (usually 4-6 digits) that cardholders enter to verify their identity for card transactions (e.g. at ATMs or point-of-sale terminals).
- **PISP** – *Payment Initiation Service Provider*. A third-party service (under **PSD2** open banking) that can initiate a payment directly from a user's bank account to a merchant's account with the user's consent. This enables **A2A** payments for online purchases (sometimes seen as "Pay by Bank" options at checkout).
- **PoS** – *Point-of-Sale*. The physical location or system where a retail transaction is completed (e.g. the checkout counter in a store, or the card reader where you tap or insert your card). In the report, "in-store (PoS) payments" refer to face-to-face transactions at physical merchants.
- **PSD2** – *Second Payment Services Directive*. An EU Directive in effect since 2018 that updated payment regulations across Europe. PSD2 is known for **opening up banking (Open Banking)** – requiring banks to provide APIs to licensed third parties (AISPs/PISPs) – and for introducing **SCA** (strong two-factor authentication for electronic payments) to enhance security.
- **PSD3** – *Third Payment Services Directive*. A proposed EU Directive (announced in 2023) that will update and refine PSD2. PSD3 is planned alongside a new **Payment Services Regulation (PSR)**; together these will address issues like improving open banking adoption, further reducing fraud, and harmonizing rules across EU countries. (Expected no earlier than ~2025–2027 for implementation.)
- **PSR** – *Payment Services Regulation*. The companion regulation proposed with **PSD3**. Unlike a directive, a regulation would be directly applicable in all EU member states. The PSR is set to include operational rules on security (like SCA), rights and obligations of providers and users, and other technical aspects to ensure consistent application of payment laws EU-wide
- **PSP** – *Payment Service Provider*. A broad term for any entity that provides payment services. This includes banks, e-money institutions, payment processors, etc. In the

Co-funded by the European Union

context of EU directives, PSPs are the regulated companies subject to PSD2/PSD3 rules (for example, a fintech offering a payment app is a PSP, as is a traditional bank's payments division).

- **SCA** – *Strong Customer Authentication*. A requirement under **PSD2** that electronic payments and account access be authenticated using at least two independent factors (out of: something you know, something you have, something you are). SCA is essentially Europe's two-factor authentication mandate for payments, aimed at reducing fraud. For instance, when you receive a text code or push notification to confirm an online purchase, that's SCA in action.
- **SEPA** – *Single Euro Payments Area*. An EU-driven initiative that harmonized euro-denominated bank transfers and direct debits across 36 European countries. SEPA allows cross-border euro transfers to be as fast and cost-effective as domestic transfers. It includes the **SEPA Instant Credit Transfer** scheme for near-instant bank payments, which many **A2A** services leverage.
- **TPP** – *Third-Party Provider*. In payments, this refers to authorized fintech companies that are not banks but offer services via bank connectivity. Under open banking, TPPs include **AISPs** (account info services) and **PISPs** (payment initiation services) that connect to your bank through **APIs**. Essentially, a TPP is any non-bank provider accessing bank accounts to render financial services (with user permission).

Co-funded by the European Union