etonec

November 2026

EUDI is coming - don't just accept it!

EUDI wallets will change how payments are authorized and processed. In order to leverage the EUDI opportunity, PSPs should avoid four common pitfalls when they design their EUDI strategy.



Executive summary

Most payment service providers (PSPs) regard the European Digital Identity (EUDI) initiative as another regulatory obligation. But its impact goes far beyond the regulatory requirement to accept EUDI wallets for authentication if customers request. A PSP that only meets the minimum regulatory requirements may lose the customer interface to competitors and miss substantial revenue opportunities.

PSPs are broadly affected by the EUDI initiative as they process payments in the back end and are involved in the authorization processes in the front end. At the same time, existing processes will be challenged by the EUDI initiative, e.g. with dynamic linking moving from the PSP to the wallet and a race for the best user experience. This will impact existing payment processes and PSP risk assessments.

For this reason, PSPs have a lot to lose if they neglect the EUDI opportunity, but potentially have even more to win. The value they can derive depends on the role a PSP takes on in the ecosystem, e.g. becoming (only) a relying party, becoming an intermediary or an issuer. For PSPs, it is crucial to define and execute a proper EUDI strategy and avoid common pitfalls.

This Etonec white paper discusses four common pitfalls and how to address them and provides an exemplary checklist for PSPs' EUDI readiness.

Common EUDI pitfalls

Pitfall No. 1: Treat EUDI as just another identity project.

Pitfall No. 2: Settle for being a passive participant in the EUDI ecosystem.

Pitfall No. 3: Miss the opportunity to rethink the payment experience.

Pitfall No. 4: Limit your strategy to mandatory use cases.

Pitfall No. 1: Treat EUDI as just another identity project.

Indeed, EUDI wallets can help support identity-related processes, but limiting EUDI to identity data would miss wider opportunities or risk jeopardizing a PSP's customer interface.

The Basis

The eIDAS 2.0 regulation provides the regulatory foundation for the EUDI wallet, requiring each EU member state to provide an EUDI wallet to citizens by December 24, 2026. Within 12 months thereafter, private-sector entities, including PSPs, must accept EUDI wallets as a means of authentication when users request it, e.g. for login use cases. This applies to all entities that are required by law or by contract to use strong user authentication[1] for online identification. Importantly, **EUDI wallets will also become payment wallets, where users can store and manage payment methods, use the wallet for paying for goods and services and authorizing payments.** This creates massive opportunities for PSPs.

Combination as the success factor

Considering EUDI solely as an eIDAS 2.0 regulatory obligation risks missing the wider picture. A multitude of European regulations will shape the roadmap of PSPs in the next couple of years, providing further use cases for EUDI wallets.

Within the context of identity, accepting EUDI wallets as a means of identification can be one way of complying with the Anti-Money Laundering Regulation (AMLR), applicable from July 10, 2027. Accepting EUDI wallets can also help meet the requirements from the Consumer Credit Directive (CCD2) to perform creditworthiness assessments via verified identity attributes or age verification from the EUDI wallet.

On the payment side, the European Payments Council is undertaking efforts to standardize payment authentication via EUDI wallets as part of its SCARLET initiative, creating a clear framework for acceptance by PSPs. The Payment Services Regulation (PSR) is also considering strong customer authentication via EUDI wallets and would extend authorization requirements.

The real value appears where payments and identity meet: one seamless interaction that combines government-backed digital identity rails and attributes with strong customer authentication (SCA) for payment initiation. PSPs need to design this customer interface carefully.

Implications

Analyze EUDI fit
Identify how the EUDI initiative can help comply with other regulatory requirements.

Think big
Assess whether a platform build could be useful if multiple use cases or verticals are impacted.

Consider positioning
Examine your strategic positioning towards customers to design the future customer interface.



Did you know?
According to Worldpay's Global Payments Report 2026, **63%** of global ecommerce value is expected to be transacted with digital wallets by 2030.[2]

[1] Whilst the eIDAS 2.0 regulation refers to "strong user authentication" in article 5f, this white paper will use the term "strong customer authentication (SCA)" instead, utilizing the payment-specific term introduced by the Payment Services Directive 2 (PSD2).
[2] https://www.globalpayments.com/insights/gpr

Pitfall No. 2: Settle for being a passive participant in the EUDI ecosystem.

By focusing solely on mandatory regulatory requirements, PSPs may take on a limited role whilst overlooking wider opportunities in the ecosystem.

A novel 4-corner model

The EUDI ecosystem comes with various roles and responsibilities - some of them newly introduced by the eIDAS 2.0 regulation. Readers familiar with existing 3- and 4-corner models will recognize familiar elements. The EUDI ecosystem distributes distinct roles across issuers, holders, and verifiers of attestations and the infrastructure that establishes trust between them. Payment processing will see new actors emerge, fulfilling specific services along the value chain. The main actors in this new 4-corner model are shown in the following table.

	Relying party	Issuer	Intermediary	Wallet provider
Description	Connect with wallets to receive & verify credentials	Connect with wallets to issue credentials	Connect with wallets on behalf of relying parties	Provide EUDI wallet (instance) to users
Likely actors	PSPs, merchants	PSPs	PSPs, card networks, acquirers	PSPs, wallet or mobile platform providers

Trust as the connective tissue

To enable business processes based on credentials issued by one entity, held by another and processed by a third, the ecosystem has to be built on trust. This trust is embedded in the technical setup of EUDI and by the European Commission maintaining trust lists for the different roles. In every EUDI wallet interaction the different actors can enable the trust as:

- wallets can verify the identity of the requesting party and whether or not it is registered to ask for or provide the information
- attestation providers can verify whether the wallet solution has undergone a formal EUDI-related certification
- users can see the relying party requesting the information and that it was validated as trusted

While the legal role is fixed for many, the operating model is a choice.

In this emerging ecosystem, PSPs can take on multiple roles:

1. **Relying party:** for verifying users' credentials during checkout
2. **Issuer** of own credentials (e.g. payment credentials)
3. **Intermediary** providing EUDI services to merchants
4. **Wallet provider** for own EUDI wallet (instance) in the existing PSP payment app

Call to action for PSPs

PSPs sit at the intersection of payments and identity. Rather than settling for the relying party role, they should also consider becoming issuers, intermediaries or wallet providers.



Did you know?

PSPs must adapt their payment processing in order to accept EUDI wallet-based payments.

This white paper is a strategic analysis for general information. It is not legal advice and does not replace an assessment of your institution's specific obligations. Regulatory status reflects publicly available information as of October 2026; PSD3 and the PSR were not yet published at that date.

Pitfall No. 3: Miss the opportunity to rethink the payment experience.

While authorization remains an essential part of payments, EUDI wallets allow for a complete redesign of the user journey - in the front end and the back end.

The payment credential[3]

The concept of SCA was introduced with the Payment Services Directive 2 (PSD2) and requires the following for payment authorizations:

1. two of the following three elements: knowledge, inherence or possession
2. a clear display of payment amount and beneficiary

At the moment, PSPs dynamically link these two inputs to create a secure and legally safe payment authorization.

Specifications for EUDI wallet payment credentials to perform SCA are underway (namely PASO and TS12). They foresee the ability for PSPs to issue payment credentials into wallets, which can be an account identifier or the account information itself. These credentials are securely signed and bound to the user's device.

An SCA request shown in an EUDI wallet will display the amount and beneficiary followed by the actual payment authorization via two factors embedded in the wallet. The signed response from the wallet includes a hash of the data. The dynamic linking moves from the PSPs to the wallet. Subsequently, the PSPs involved in the payment transaction should each verify these payment credentials to establish the required legal basis for the payment.

Two authorization flows

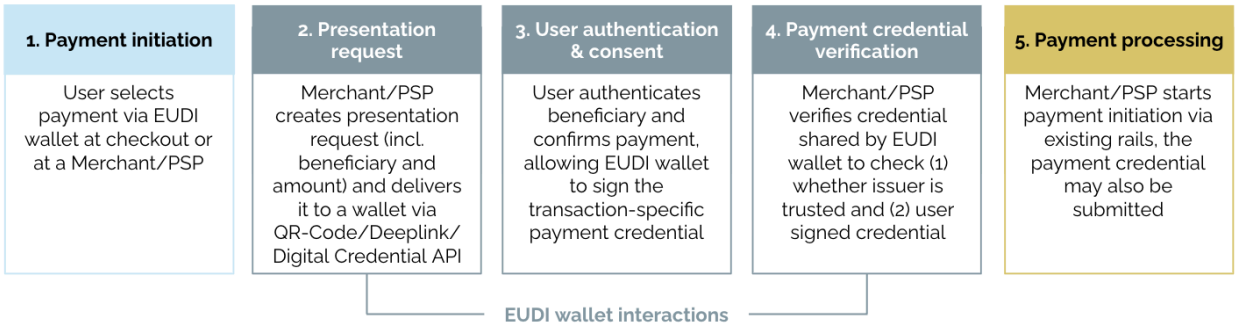
Issuer-requested
A payment credential is verified by the same PSP that issued it.

The flow is similar to existing authentication mechanisms: the PSP receives the credential from the wallet, verifies it and initiates the payment.

Third-party-requested
A payment credential is verified by a merchant or a PSP that did not issue it.

A new flow evolves: the PSP receives the credential from the wallet, verifies it and ideally passes it on to the original credential issuer during payment initiation. This requires adaptations.

Payment initiation & SCA via EUDI wallets



Did you know?
A shift is underway, with dynamic linking moving from the PSPs to the wallet.

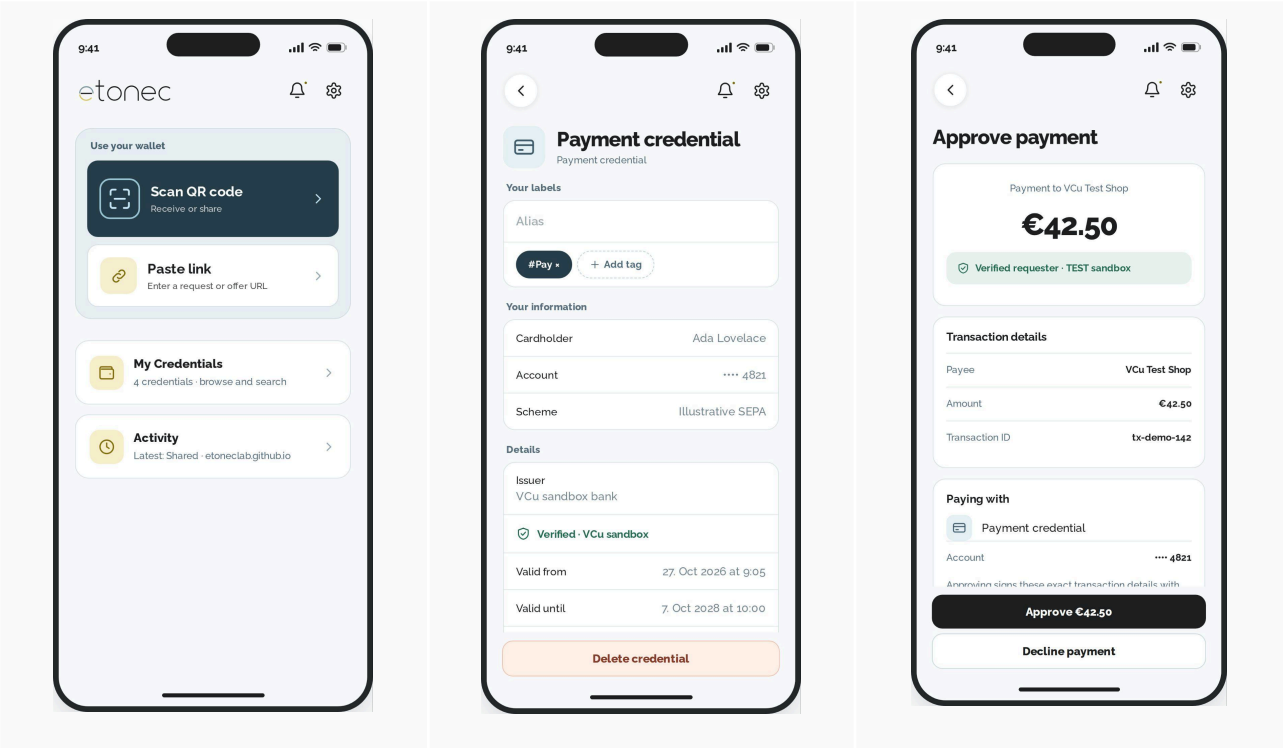
[3] This white paper uses the term "payment credential" whilst other publications refer to it as "SCA credential".

End-to-end EUDI payment journey

Step 1: Use an EUDI wallet to scan a QR code, provided by the PSP, to receive a payment credential.

Step 2: Store the payment credential in the EUDI wallet - whether this is a bank account, a credit card, a payment wallet or a future digital euro account credential.

Step 3: Use the payment credential for a purchase: scan QR code, authorize payment by reviewing and approving the amount and the beneficiary in the EUDI wallet.



Step 4 (not pictured): The merchant hands the payment credential over to the PSP for payment processing

PSP benefits

- Cost saving opportunities (e.g. reduction of 3DS fees)
- Unified implementation and user experience across the EU
- Stronger identity binding could create fraud reduction opportunities
- Ability to request additional attestations together with a payment attestation
- Simplified and streamlined technical integration of payment methods
- Control over positioning

User benefits

- One-click SCA replaces out-of-context procedures (e.g. 3DS)
- Passwordless authentication
- Payment and SCA in one wallet with universal usage across an emerging acceptance base
- Consistent user experience across different platforms and payment methods
- Streamlined user experience aligned with current market practices (in particular when utilizing technologies such as the Digital Credentials API)

EUDI introduces new third-party-requested SCA flows and wallet-based dynamic linking. PSPs must adapt to keep the customer relationship. Payments will continue to be processed on the same conventional rails, where PSPs remain essential. A clear EUDI strategy lets PSPs protect their business and possibly extend it.

Pitfall No. 4: Limit your strategy to mandatory use cases.

The real value creation is harder to spot initially and impacted by multiple factors, including ecosystem positioning, make-vs-buy decisions and integration activities. On closer inspection, substantial value becomes visible.

EUDI value creation

At first glance, it looks like sustainable commercial models in the EUDI ecosystem are hard to establish. For example, it is challenging for an issuer to receive a fee every time a relying party uses its credential. Instead, the value creation heavily depends on the ecosystem role adopted by the PSP.

Did you know?

The intermediary role creates revenue opportunities for PSPs with a large merchant base.

	Relying party	Issuer	Intermediary	Wallet provider
EUDI commercial impact	**Direct:** Cost savings for existing business processes[4]	**Indirect:** Improved user experience, reduced fraud/ lower return/ higher approval rates	**Direct:** Pay-per-use/ subscription revenue from customers	**Indirect:** Control of the customer interface

All EUDI roles provide direct or indirect business opportunities for PSPs. However, PSPs must carefully evaluate which approach fits their strategic agenda. Importantly, cost of service also impacts the business case. An in-house relying party platform build keeps control of data, customer journeys, roadmap prioritization and risk logic, at the cost of building and operating the service. Utilizing a vendor can reduce the build and operational burden, at the cost of being dependent on the vendor in terms of roadmap prioritization, data processing and customer journeys. Using an intermediary relying party as a service provider enables an abstraction of administrative and technical complexity for issuance and verifications, but comes at a cost.

Evolving commercial value

The business case will also depend on external factors outside the control of the PSP, such as national wallet rollout timelines and feature prioritization, user adoption and the alignment on specifications (especially for payment credentials). Early business cases must be built on pilot data instead of market benchmarks.

Test commercial models with sandboxes and pilots

With many opportunities and moving pieces in place, experimentation is key to success. Multiple EUDI sandboxes, testbeds and pilot implementations are available. PSPs can join these to experiment with user journeys to gain insights into:

- Success rates of the wallet journey versus your current flow
- Authentication success and failure reasons
- Fallback scenario testing
- Fraud and abuse signals compared with existing authenticators
- Operational cost per verified customer and per support contact

[4] Examples include the replacement of existing identity verification methods with EUDI-based know-your-customer (KYC) checks as well as fraud reduction.

This white paper is a strategic analysis for general information. It is not legal advice and does not replace an assessment of your institution's specific obligations. Regulatory status reflects publicly available information as of October 2026; PSD3 and the PSR were not yet published at that date.

PSPs can prevent common pitfalls while ensuring EUDI readiness by December 2027

With the technical specifications gaining maturity and wallets starting to enter the market, PSPs must put EUDI onto their roadmap and avoid common pitfalls from the beginning.

Exemplary EUDI checklist

Within the next 2 months - Strategy

- [ ] Set up EUDI project and a cross-functional EUDI project team
- [ ] Identify EUDI verification and issuance use cases (mandatory vs. optional, immediate vs. later)
- [ ] Identify suitable roles in the EUDI ecosystem (relying party, issuer, intermediary, wallet provider)
- [ ] Develop holistic EUDI strategy
- [ ] Define EUDI project roadmap
- [ ] Create a holistic business case

Within the next 4 months - Design

- [ ] Identify processes affected by EUDI as well as impacted teams
- [ ] Design technical architecture and platform capabilities
- [ ] Decide on make-vs-buy approach
- [ ] Design EUDI user journeys (incl. fallback flows)

Until launch date (December 2027 at the latest) - Build & test

- [ ] Define Go-to-market approach (timing, jurisdictions, etc.)
- [ ] Build platform (in-house, via a vendor or via an intermediary relying party)
- [ ] Register for EUDI roles
- [ ] Consider joining a sandbox/ pilot
- [ ] Test and validate EUDI user journeys (internally and/ or externally)

Post December 2027 - Monitor & adapt

- [ ] Monitor adoption
- [ ] Prioritize and implement use cases parked for later

About Etonec

Etonec helps financial institutions, payment service providers and technology companies turn digital identity, digital payments and digital money into strategy and products. The team supports you with everything from strategic decisions through architecture, prototypes and implementation, and contributes to the consortia and associations shaping the standards, including the WE BUILD and APTITUDE large-scale pilots, SPRIND Sandbox and the Digital Euro Association.



Marcus Nasarek
Architecture & Regulation



Nancy Timm
Product & Payments



Dr. Jonas Gross
Strategy & Public Policy



Jonathan Knoll
Commercial & Ecosystems

office@etonec-ds.com www.etonec.com