Capgemini invent

in collaboration with

ABE EBA
EURO BANKING ASSOCIATION

Potential of the *EUDI-Wallet for Financial Institutions*

Whitepaper



"This whitepaper has been developed jointly by Capgemini and the Euro Banking Association to provide insights into the potential of the European Digital Identity Wallet for financial institutions and to support the ongoing discussion on its regulatory, operational and strategic implications for the European financial sector."

Contents

Executive summary 02

01 EUDI-ecosystem fundamentals 03

1.1 Regulatory foundation 04
1.2 EUDI-Wallet as the functional basis 05
1.3 Ecosystem participants and trust framework roles 05
1.4 Extension towards a European Business Wallet 06

02 Implications for the financial sector 07

2.1 Legal obligation 08
2.2 Pan-European acceptance 08

03 High-value financial sector use cases 09

3.1 Value framework for the financial sector 10
3.2 Use case clusters 10

3.2.1 Client onboarding and compliance 11
3.2.2 Financing and funding processes 11
3.2.3 Credential issuance 12
3.2.4 Identity based payment authorisation 13
3.2.5 Cross-platform and ecosystem integration 14

04 Technical integration requirements 15

05 Implementation approach and rollout plan 17

06 From planning to execution - strategic positioning and outlook 19

Executive Summary

The European Digital Identity (EUDI) ecosystem enables secure digital verification of identities and attributes across the European Union. Its core instrument is the EUDI-Wallet, which allows natural persons to store and present personal identification data and electronic attestations of attributes in a standardised and user controlled way. Organisations can verify data presented from the wallet and, where authorised, issue verifiable credentials into the wallet.

The EUDI-Wallet establishes a harmonised European trust framework under Regulation (EU) 910/2014 (eIDAS) as amended by Regulation (EU) 2024/1183, introducing a shift from document based verification to structured, cryptographically secured credentials. This reduces manual effort, accelerates onboarding, improves auditability, and lowers fraud exposure, while responsibility for regulated decisions remains fully with the financial institution. Organisations verifying credentials presented from a wallet act as relying-parties within the ecosystem. Organisations issuing credentials into the wallet act as issuers – a distinct role that additionally includes relying-party functions where wallet-held data is verified prior to issuance. Under the amended eIDAS framework, such regulated relying-parties in sectors such as financial services are required to accept wallet based online identification where strong user authentication is legally required. Based on the current implementation timeline defined in the regulation and supporting acts, this obligation applies from 24 December 2027, defining a binding implementation horizon for the financial sector.

Beyond compliance, the primary impact lies in high value financial sector use cases:

- **Onboarding & Compliance:** instant credential-based identity verification reduces manual effort, accelerates onboarding, and improves auditability, while maintaining full regulatory accountability.
- **Financing & Funding:** reusable verified evidence simplifies income, employment, and eligibility checks, reducing friction and duplication across customer, financial institutions, and public processes.
- **Proof Economy:** financial institutions can evolve from verifiers to issuers of reusable credentials (e.g. guarantees, confirmations), enabling new roles in digital ecosystems.
- **Identity based Payment Authorisation:** reduces fraud and improves customer experience while enabling a consistent, cross channel authentication solution.
- **Platform Integration:** standardised, cross-border identity enables seamless interaction across financial institutions, corporates, and public institutions.

A pragmatic implementation approach starts with establishing a compliant relying-party capability for those online identification processes that fall under the EUDI-Wallet acceptance obligation. Once this baseline is in place, financial institutions can extend wallet usage to additional verification use cases that create operational or customer value, even where no immediate regulatory obligation exists. A further, optional step is participation as a credential issuer, where this supports high-value downstream processes.

The priority now is to move from awareness to implementation. Financial institutions should identify in-scope journeys, establish reusable relying-party capabilities, and align governance for registration, attribute usage, and consent handling across markets and entities. Institutions that plan, focus and act around these strategic considerations can reduce implementation complexity, strengthen control consistency, and build the foundation for scalable participation in a European digital trust ecosystem.



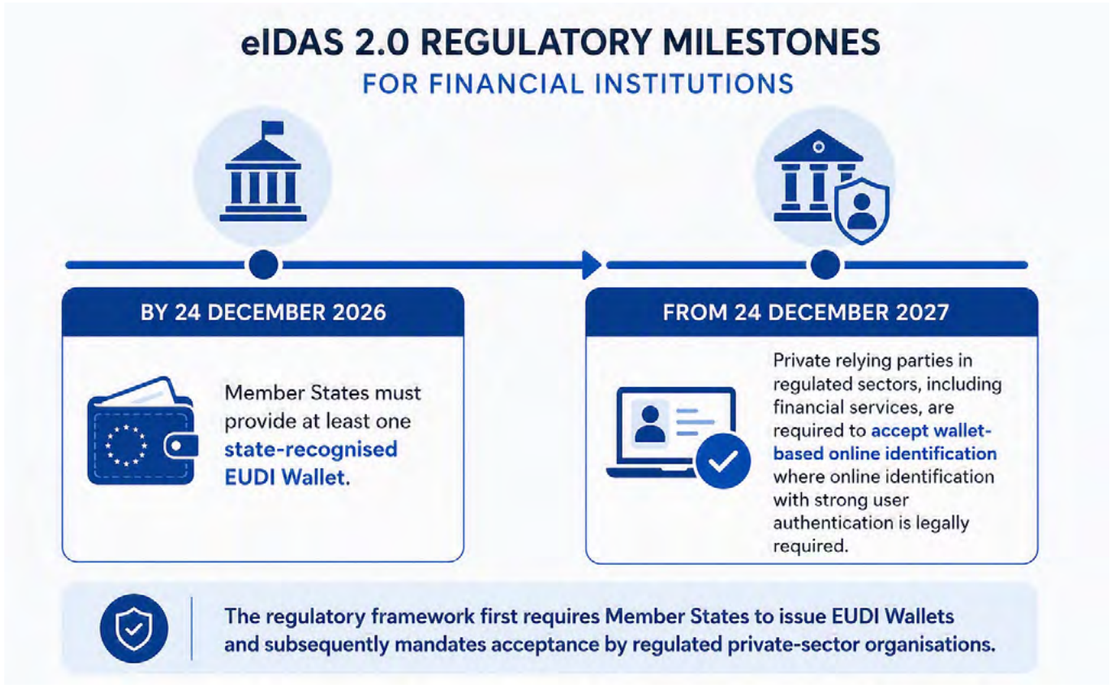
01

EUDI-ecosystem fundamentals



1.1 Regulatory Foundation

The legal basis of the EUDI-ecosystem is the amended eIDAS Regulation (EU) 910/2014, specifically Regulation (EU) 2024/1183, together with its implementing acts. This framework establishes directly applicable EU law for electronic identification and trust services and defines a harmonised trust framework across EU Member States. The regulatory framework contains two dates of particular importance:

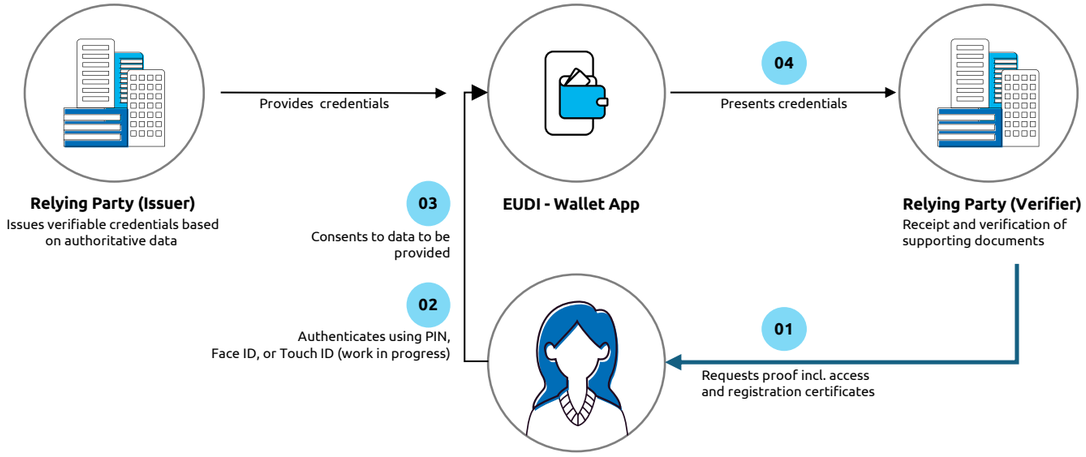


Picture 1: *critical dates for financial institutions*

1.2 EUDI-Wallet as the functional basis

The EUDI-Wallet acts as a user-controlled holding component for identity data and electronic attestations of attributes. It enables users to receive, store, and share such data. Credentials in the EUDI-Wallet can be issued by both public authorities and private-sector entities. At a minimum, EU Member States provide the core digital identity, enabling individuals to identify and authenticate themselves with legal certainty and a high level of assurance.

Electronic attestations of attributes document specific facts or characteristics of a person and can be verified by relying-parties for a defined purpose. The eIDAS framework regulates the issuance, presentation, and verification of such attestations, but does not prescribe how verified information is used within downstream business or regulatory processes. For financial institutions, wallet-based credentials therefore serve as verified evidence inputs that can be integrated into existing processes in accordance with applicable sector-specific rules. Wallet-based identification follows consent-driven and purpose-bound principles. Only attributes that are necessary for a defined purpose may be requested, and credential interactions must support transparency and auditability.



Picture 2: *EUDI-ecosystem simplified visualisation*

1.3 Ecosystem participants and trust framework roles

The EUDI-ecosystem defines a set of functional roles centred around the lifecycle of electronic attestations of attributes. These roles include issuers, verifiers, and wallet holders. Financial institutions primarily participate as relying-parties, requesting electronic attestations of attributes for a defined purpose and verifying their authenticity, integrity, and validity before using the verified information as input to internal processes.

Issuer and relying-party are distinct functional roles under eIDAS 2.0: issuers create and cryptographically secure attestations, while relying-parties (verifiers) validate presented attestations prior to use. Wallet holders store and present electronic attestations under their control. An institution may combine both roles. For example, when an issuer verifies personal identification data or attributes from the wallet before issuing a new attestation, it acts as a relying-party for that verification step, without the issuer role becoming a sub-category of the relying-party role. This flexibility allows financial institutions to start as consumers of verified evidence and, where appropriate, extend their role to issuing attestations.

A central governance element for relying-parties is registration. Participation in the EUDI-ecosystem requires formal registration that documents the intended use of requested data and the attributes that may be requested for that purpose. This registration is not a technical formality. It functions as a governance mechanism that enforces transparency, data minimisation, and accountability by making declared purposes and attribute scopes explicit and externally visible.

In this context, two types of certificates are relevant for relying-party registration. The access certificate is used to authenticate the relying-party technically when interacting with the EUDI-Wallet, ensuring that only authorised parties can request and receive wallet-based data. The registration certificate, by contrast, serves a governance function: it documents the intended use cases and the attributes that may be requested for those purposes. Together, these certificates link technical access with formalised purpose definition, ensuring that credential requests are both securely authenticated and transparently governed within the EUDI trust framework.

1.4 Extension towards a European Business Wallet

The European Business Wallet (EBW) is intended to extend the EUDI-approach from natural persons to organisations by enabling organisations to be identified and to exchange verifiable organisational data. The corresponding regulation is currently (at the time of publication of this whitepaper) under negotiation, based on a draft proposal from the European Commission for a regulation on an EBW (COM (2025) 838). Conceptually, the EBW can be seen as a natural extension of the relying-party components of the EUDI-ecosystem, as it would enable structured and trusted B2B and B2G interactions in addition to B2C use cases. In this context, the EBW is expected to support the management and presentation of verified company identity data, mandates and representation rights, as well as licences, certificates, and sector-specific credentials. This enables new forms of secure B2B and B2G interactions, such as digital onboarding of corporate clients, automated verification of representation rights, or cross border business processes with reduced manual validation effort.

However, from a present regulatory perspective, the EBW remains a forward looking extension rather than an immediate compliance requirement. For financial institutions, the EBW should therefore be understood as a strategic, forward-looking topic: in the short term, the focus is on integrating EUDI-Wallet capabilities for retail based processes. In the mid to long term, EBW capabilities may become highly relevant for corporate banking, particularly in areas such as Know Your Business, trade finance, and cross border business relationships. The exact regulatory timeline, scope of obligations, and technical specifications for the EBW are still evolving. As such, financial institutions should monitor developments closely and consider early positioning, but without assuming immediate implementation requirements.

02

Implications for the financial sector

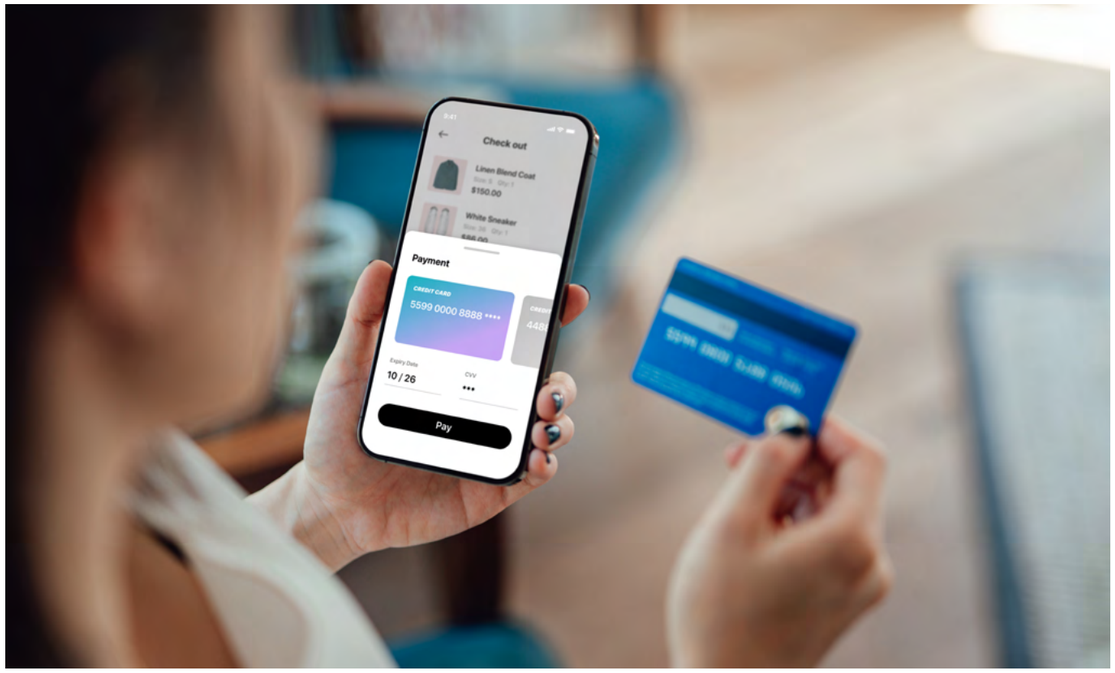
2.1 Legal obligation

As of December 2027, financial institutions are required to accept wallet-based online identification in all regulated financial institution processes where strong user authentication is legally required. This obligation is derived from Article 5f(2) of Regulation (EU) 910/2014 (eIDAS), as amended by Regulation (EU) 2024/1183, and applies upon the voluntary request of the user for the possibility to use the EUDI-Wallet. Financial institutions can no longer limit digital identification options to proprietary or nationally scoped solutions in these scenarios.

2.2 Pan-European acceptance

EUDI-Wallet acceptance must be designed as a cross-border, pan-European capability from the outset. Financial institutions are required to accept wallets issued by any EU Member State once the obligation applies, regardless of the national rollout status of the state-provided EUDI-Wallet. Therefore, the acceptance obligation is independent of the respective national status of the EUDI-Wallet. As a result, wallet acceptance should be implemented in line with the common technical and governance standards defined by the EUDI-ecosystem. When these standards are applied, cross-border interoperability is achieved by design. Country-specific or fragmented implementations risk deviating from this model and increase operational complexity. A consistent relying-party capability aligned with the EUDI-standards supports uniform verification, logging, and governance across entities and channels.

However, there is potential for divergence in national implementations, particularly at the governance level. While technical standards are harmonised, additional national requirements in areas such as registration, security, or audit may increase complexity for cross-border operations. Nevertheless, eIDAS requirements act as the sole reference regarding compliance and acceptance at EU level.

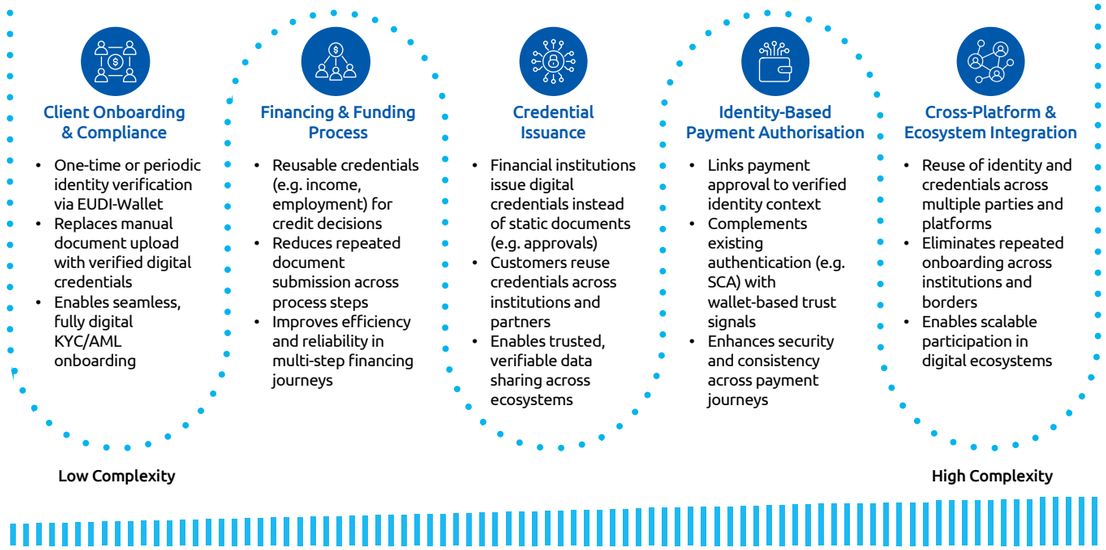


High-value financial sector use cases

3.1 Value framework for the financial sector

For the financial sector, “value” refers to use cases that combine regulatory relevance with measurable operational and customer impact, such as reduced onboarding effort, improved auditability, or lower fraud exposure. Value is not created by isolated wallet features but by capability clusters that can be scaled across products and channels. The following five clusters represent a relevant structure for the financial sector. This clustering is also consistent with the practical adoption path that starts with acceptance as a relying-party and can later expand into optional credential issuance.

3.2 Use case clusters



Picture 3: *overview of major use case clusters*

3.2.1 Client onboarding and compliance

Context

Client onboarding and compliance processes are core activities for financial institutions and represent the most immediate area in which the EUDI-Wallet has regulatory and operational relevance, particularly in Know Your Customer and Anti-Money Laundering contexts. These processes are characterised by one-time or periodic identification events, rather than recurring transaction-level authentication.

Use case description

In client onboarding and compliance scenarios, individuals use their EUDI-Wallet to prove their identity and relevant attributes as part of an initial or event-driven identification step within a digital journey. Instead of uploading documents or completing identification steps causing friction in the entire onboarding process (manual document handling, video-identification, etc.), the user consents to share verified identity data and, where applicable, additional attributes such as address or representation rights from the wallet. The financial institution receives these credentials in a structured and verifiable form and uses them to complete onboarding or compliance checks. This enables a fully digital, media-break-free and frictionless onboarding experience while ensuring that identity and compliance requirements are met with the highest level of assurance.

Process mechanics

The financial institution acts as a relying-party by requesting purpose-bound attributes, receiving credentials from the wallet, and verifying their authenticity, integrity, and validity before integrating the verified information into onboarding and compliance workflows. This replaces the collection and manual assessment of various documents.

Value drivers

Operational benefits include reduced manual verification effort, shorter client onboarding cycles, and improved auditability through consistent and traceable interactions. The use of standardised digital credentials improves evidence quality without changing existing regulatory responsibilities.

Key applications

A key high-value application is onboarding of natural persons acting in regulated roles, particularly the verification of identity and representation rights where individuals act on behalf of an organisation. Today, these checks are often document-heavy, burdensome and repetitive. Additional applications include age and identity verification for regulated products, where predefined attributes can be shared securely without full document disclosure.

Strategic relevance

This cluster represents the primary entry point for EUDI-Wallet adoption in the financial sector. It addresses mandatory identification requirements and creates the foundation for subsequent wallet-based use cases.

3.2.2 Financing and funding processes

Context

Financing and funding processes require repeated verification of customer and eligibility information, often involving multiple parties, including public institutions.

Use case description

In financing and funding processes, customers use the EUDI-Wallet to provide verified evidence required for credit, subsidy, or guarantee-related decisions. Instead of repeatedly submitting income statements, employment confirmations, or eligibility documents, the user presents relevant credentials from the wallet at specific points in the process. The issuer could therefore be, for example, the relevant employer or tax authority. These credentials can be reused across steps or even across different interactions, reducing repeated data requests. For the financial institution, this creates a more reliable and efficient way to obtain decision-relevant evidence while improving customer experience in often complex and multi-step financing journeys.

Process mechanics

Individuals present relevant credentials via the EUDI-Wallet. These credentials are verified by the financial institution as a relying-party and incorporated into credit or funding workflows. Credentials can be reused across multiple steps in a process chain.

Value drivers

Verified credentials reduce manual handling, lower the risk of fraud, and improve consistency of evidence used in risk assessment. Reuse of credentials reduces unnecessary duplication and streamlines interactions between financial institutions, customers, and third parties.

Key applications

Typical applications include credit assessment based on income or employment attestations, subsidy eligibility checks, and financing or guarantee-related workflows involving repeated verification.

Strategic relevance

This cluster extends wallet usage into additional business processes and increases the operational value of EUDI-Wallet integration. It also creates a natural transition towards credential issuance.

3.2.3 Credential issuance

Context

Financial institutions already generate authoritative artefacts such as approvals, confirmations, and guarantees as part of their core processes. Today, these artefacts are typically exchanged as static documents, which limits reuse, requires repeated verification, and creates friction in downstream processes involving multiple parties.

Use case description

In this cluster, financial institutions go beyond consuming credentials and begin issuing them. When a financing decision, guarantee, or confirmation is created, the institution issues a verifiable credential into the customer's EUDI-Wallet instead of providing a PDF or paper document. The customer can then reuse this credential in subsequent interactions with other financial institutions, business partners, or public authorities. This turns financial institution-generated artefacts into reusable digital proofs and enables downstream processes to rely on verified information without repeated document exchange.

Process mechanics

The financial institution issues a cryptographically secured credential into the wallet. This credential can later be presented to other relying-parties and independently and instantly verified, without repeated document exchange.

Value drivers

Credential issuance enables downstream reuse, reduces friction in multi-party processes, and positions financial institutions as trusted evidence providers within broader ecosystems.

Key applications

Examples include credit approvals, financing confirmations, guarantees, and payment confirmations, which today are typically exchanged as static documents.

Strategic relevance

Credential issuance is an optional, next-stage capability that builds on stable relying-party adoption. It offers strategic ecosystem value but requires additional governance, including lifecycle management and compliance alignment.





3.2.4. Identity based payment authorisation

Context

Payment authorisation in the financial sector is currently dominated by fragmented authentication mechanisms such as one-time passwords, device-bound factors, and channel-specific security solutions. These mechanisms provide transaction security, but they are often loosely coupled to verified identity information and lead to inconsistent user experiences across channels and markets. At the same time, fraud prevention increasingly depends on stronger and more reusable trust signals, creating pressure to better link payment authorisation to verified identity contexts.

Use case description

In identity-based payment authorisation scenarios, the EUDI-Wallet may be used to support or strengthen transaction authentication. When a customer initiates a payment or a sensitive transaction, the wallet can provide identity or attribute-based confirmation as part of the authorisation flow. Rather than relying solely on one-time passwords or device-bound factors, the transaction can be linked to a verified identity context. While this capability is still emerging, it illustrates how identity and payment processes may increasingly converge around wallet-based trust signals.

Process mechanics

Wallet-based identity or attribute credentials could support authentication steps associated with payment approval, strengthening trust in transaction flows.

Value drivers

Potential benefits include improved security, reduced fraud exposure, and a more consistent user experience across authentication processes.

Key applications

Identity-based payment authorisation is most relevant in customer journeys where strong authentication is required under PSD2 and in the evolving PSD3 and PSR framework, including transaction approval and other high-risk authentication moments, as well as secure account access flows. In these contexts, the EUDI-Wallet could provide a reusable trust signal that complements existing SCA mechanisms.

Strategic relevance

This cluster is forward-looking in the sense that current eIDAS acceptance obligations focus on online identification, and available guidance does not indicate that payment authorisation is covered by the same acceptance obligation as wallet-based identification. At the same time, payment authorisation and account access are already shaped by SCA requirements under PSD2 and by the expected PSD3 and PSR evolution. For financial institutions, the strategic relevance is therefore to treat the EUDI-Wallet as a potential enabler for improving SCA-relevant user journeys, rather than as an additional standalone compliance requirement under eIDAS.

3.2.5. Cross-platform and ecosystem integration

Context

In platform and ecosystem scenarios, the EUDI-Wallet enables verified identity and credentials to be reused across multiple, independent parties based on a common European trust framework. Instead of establishing individual identity solutions for each partner or platform, financial institutions can rely on wallet-based identity and attribute verification that is anchored in shared trust lists, standardised protocols, and common governance rules. This allows customers or organisations to interact with financial institutions, corporate platforms, and public services using the same verified identity context, without repeated onboarding or bespoke integrations. Compared with the previously described clusters, this use case cluster is by far the most complex, as it connects the new EUDI-infrastructure with existing legacy systems on a deeper level. However, this has the potential to deliver the highest economic value, especially when combined with the EBW.

Use case description

In platform and ecosystem scenarios, the EUDI-Wallet enables individuals or organisations to reuse verified identity and credentials across multiple parties. A user can present the same wallet-based identity or attributes to different financial institutions, corporate platforms, or public services without repeating identification steps. This supports seamless interaction across institutional boundaries and enables financial institutions to participate in broader digital ecosystems where identity and trust are shared rather than recreated in each channel.

Process mechanics

Verified credentials are exchanged using standardised EUDI-protocols and validated against shared trust lists and mechanisms that confirm whether credentials are still valid, revoked, or expired. Relying-parties verify authenticity, integrity, and validity at transaction level, while governance elements such as intended use registration and attribute minimisation ensure consistent application across platforms and participants.

Value drivers

Platform integration reduces the need for bilateral identity integrations, lowers onboarding and verification effort across ecosystem partners, and supports scalable cross-border interactions. By relying on a shared trust infrastructure, financial institutions can participate in ecosystem-based processes without assuming central identity provider roles or duplicating verification logic for each platform.

Key applications

Typical applications include cross-border customer onboarding across multiple financial institutions, participation in funding or guarantee platforms involving public authorities, and verification of organisational data and mandates in corporate ecosystems where multiple parties rely on the same evidence.

Strategic relevance

Platform integration addresses the structural challenge of trust fragmentation in multi-party digital ecosystems. For financial institutions, the EUDI-Wallet provides a way to participate in platform-based and cross-border processes using a shared European trust infrastructure, without creating proprietary identity platforms or bespoke partner integrations. This supports long-term interoperability, scalability, and ecosystem participation beyond individual bilateral use cases.



04 Technical integration requirements

Implementation in the financial sector should start from the core requirement of relying-party capability. It includes the ability to request credentials for a defined purpose, receive and validate wallet presentations, and make verified attributes available to downstream processes under appropriate controls. This requires a financial institution-side integration layer that not only generates wallet requests and processes responses, but also maps verified attributes into internal onboarding, compliance, and decision-support systems in a structured and auditable manner.

From an architectural perspective, wallet integration therefore goes beyond a standalone technical component. Verified identity data and attestations must be consumed by existing Know Your Customer, Anti-Money Laundering, onboarding, and customer lifecycle systems, where they replace or complement document-based inputs. This integration layer is where operational efficiency and automation benefits materialise, as it determines how consistently verified data can be reused across processes and channels.

A central governance and integration requirement is relying-party registration and certificate handling. The ecosystem design distinguishes between an access certificate, used to authenticate the relying-party to the wallet, and a registration certificate, which documents the intended use and the attributes that may be requested for that purpose. These certificates must be obtained via designated relying-party registrars, which are typically operated or mandated by public authorities. While the regulatory framework for this registration is defined at EU level, the concrete registrar structures and operational processes are still being established in many EU Member States. For financial institutions, this means that technical onboarding must be aligned with external registration and governance processes, as intended use declarations and attribute scopes become externally visible representations of data processing purposes.

Consent and auditability need to be treated as first-class architectural concerns across the full integration chain. Wallet-based identification is consent-driven and purpose-bound. Financial institutions therefore require consent handling mechanisms embedded in customer journeys and audit-ready logging that captures the declared purpose, requested attributes, consent events, verification results, and downstream system usage. These elements must be integrated with existing compliance and audit frameworks rather than implemented as isolated features.

Operational readiness should be validated through appropriate test and pre-production environments. Financial institutions should ensure that relying-party registration, certificate handling, verification routines, and end-to-end integration into internal systems are exercised and validated before production rollout. Early testing is critical to ensure that wallet interactions, governance controls, and internal system integration function coherently before regulatory timelines apply.

Finally, channel and device constraints must be considered early in the design journey. Current planning for state-provided wallets indicates an app-based approach with an initial focus on same-device flows, while cross-device scenarios are expected to mature over time. This affects how wallet interactions are embedded into digital onboarding and authentication journeys, particularly for desktop-initiated processes. Financial institutions should therefore design mobile-first wallet interactions while ensuring that internal systems and processes can accommodate evolving cross-device patterns as the ecosystem matures.

05 Implementation approach and rollout plan

A pragmatic implementation approach should align with the regulatory scope while reducing delivery and operational risk. Given the inherent cross-border acceptance and interoperability requirements of the EUDI-ecosystem, implementation should not be approached on a Member-State-by-Member-State basis. Instead, financial institutions should design a single, scalable, pan-European solution that can be deployed consistently across markets, products, and channels, in line with the common standards defined by the implementing acts, while also considering a corresponding phase-out of national legacy solutions.

Implementation typically starts with regulatory scoping, retiring legacy solutions, and process mapping. Financial institutions should identify all online identification and authentication processes that are subject to a legal or contractual requirement for strong user authentication and therefore fall within the scope of EUDI-Wallet acceptance. This analysis should be performed across the full landscape, covering digital onboarding, account access, and other identification checkpoints embedded in customer journeys, with the explicit objective of supporting EU-wide acceptance rather than isolated national solutions.

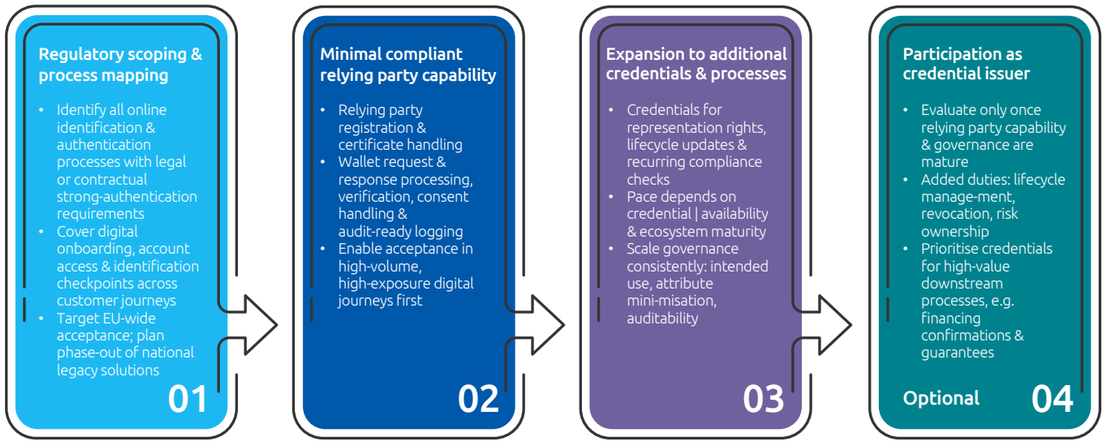
The next step is the establishment of a minimal compliant relying-party capability that can be reused across markets. This includes relying-party registration, certificate handling, wallet request and response processing, verification routines, consent handling, and audit-ready logging. At this stage, the focus should be on enabling acceptance in high-volume and high-exposure digital journeys, where failure to support wallet-based identification would have the greatest regulatory and operational impact once the acceptance obligation applies.

Once core identity acceptance is stable, financial institutions can expand the solution to additional credential types and more complex processes. This may include the use of credentials for representation rights, lifecycle updates, or recurring compliance checks, depending on credential availability and ecosystem maturity. Throughout this expansion, governance remains critical. Intended use definitions, attribute minimisation, and auditability must scale consistently, as uncontrolled expansion increases supervisory and privacy risk.

A further, optional stage is participation as a credential issuer. Issuance should only be evaluated after relying-party capabilities and governance processes are mature, as issuing credentials introduces additional responsibilities related to lifecycle management, revocation, and risk ownership. Where issuance is pursued, financial institutions should prioritise credentials that reduce friction in high-value downstream processes, such as financing confirmations or guarantees, and ensure alignment with regulatory, operational, and liability constraints.

Timeline alignment should follow the European legal framework rather than national rollout variability. Member State obligations to provide a state-recognised wallet precede the acceptance obligation for private relying-parties, which applies at a later stage. Financial institutions should use this sequencing to stage internal delivery, starting with early testing and sandbox participation (depending on the availability per EU Member State), followed by progressive rollout of production-ready capabilities across markets. Early validation of cross-market functionality is particularly important, as interoperability is an inherent property of the EUDI-ecosystem and should be reflected in implementation from the outset.

From an organisational perspective, successful rollout requires coordinated ownership across technology, compliance, and business functions. Clear responsibility must be established for relying-party registration, certificate lifecycle management, and governance of intended use and attribute minimisation. Without this alignment, financial institutions risk implementing technically functional solutions that fail to meet supervisory expectations due to insufficient transparency, consistency, or control.



Picture 4: *implementation steps*

06 From planning to execution - strategic positioning and outlook

The EUDI-Wallet introduces a shared European infrastructure for digital verification. For the financial sector, this is a structural shift. Identity and attribute verification moves from fragmented, document-driven routines towards standardised credentials that can be verified across borders. Financial institutions that treat this as a core capability can simplify onboarding, compliance, and cross-border service delivery at scale.

The priority is execution. Wallet acceptance must become a reusable relying-party capability across all relevant online identification flows where strong user authentication is legally required. Institutions that implement this once and reuse it across products and markets gain significant operational advantages; they reduce regulatory exposure and they avoid parallel identity stacks that inflate cost and weaken control consistency. This is where financial institutions can create structural efficiency, because the same verification and governance layer can be reused across the customer lifecycle, including onboarding, periodic reviews, and recurring checks.

The larger opportunity is strategic positioning in a European trust ecosystem that will expand in scope and adoption. The financial sector already produces authoritative evidence in core processes, for example confirmations and guarantees. Over time, financial institutions can choose to issue verifiable credentials where this supports downstream reuse and reduces friction in multi-party process chains. This is not a mandatory step. It positions financial institutions as trust anchors that enable other market participants to rely on verified evidence without repeated document exchange.

In practical terms, the EUDI-Wallet can be treated as a compliance requirement and a transformation lever at the same time, without blending the two. Compliance defines the minimum acceptance capability. Strategy defines how far to extend into reuse, issuance, and ecosystem integration. Financial institutions can reduce structural costs, strengthen risk control, and secure a credible role in the digital trust layer that will shape European financial interactions over the coming years.

From a broader perspective, the evolution of the European trust ecosystem will also play a role in enabling identity-based interactions with digital AI agents and AI-driven services. In particular, the EBW extends these capabilities to organisational identities, enabling verified representation of mandates, roles, and authority in a structured and machine-readable form. This creates a foundation for trusted automated interactions across institutional boundaries, where both individuals and organisations can be represented in a verifiable way. While this development is still emerging, it highlights the longer-term importance of interoperable identity and credential infrastructures beyond human-centric use cases.

Coordinated industry action is now required. Financial institutions should align on the interpretation of eIDAS acceptance scope across jurisdictions and use cases, while establishing consistent relying-party capabilities and integration approaches across their organisations.

Ensuring interoperability depends on active participation in cross-border testing and validation initiatives, combined with aligned governance practices for registration, attribute usage, and consent handling. These elements need to be developed in a coordinated manner to avoid diverging national or institutional approaches.

Ultimately, financial institutions should focus on building a common, scalable operating model for EUDI-Wallet integration. Only sustained collaboration across the European financial sector will prevent fragmentation and enable a harmonised and scalable adoption of the EUDI-Wallet.



Thomas Egner

Secretary General
Euro Banking Association



Dr. Florian Forst

Vice President | Financial Services | Global Payments Domain Lead Capgemini Invent

About Capgemini Invent

As the digital innovation, design and transformation brand of the Capgemini Group, at Capgemini Invent we enable CxOs to envision and shape what's next for businesses. Located in over 40 studios and more than 70 offices around the world, we are a 13,500 strong team of strategists, data scientists, product and experience designers, brand experts and technologists who develop new digital services, products, experiences and business models for sustainable growth.

Capgemini is the business transformation partner for enterprises in the age of AI. We help organizations imagine and build an intelligent, sustainable future, combining AI, technology and human ingenuity to transform how they operate, innovate and grow. With unique end-to-end capabilities spanning strategy, technology, engineering and intelligent operations, we bring together deep industry expertise and market-leading capabilities in AI, cloud and data to turn ambition into measurable business outcomes at scale. Supported by a robust ecosystem of partners and nearly 60 years of expertise, Capgemini is a responsible and diverse global organization of over 410,000 team members in more than 50 countries. The Group reported 2025 revenues of €22.5 billion.

Make it real. | www.capgemini.com

About EBA

The Euro Banking Association (EBA) brings payments practitioners together to harmonise and advance Europe's payments ecosystem.

We assess the impact of regulation, new trends and technologies, create market practices and learn from one another.

This collaborative space helps our member and stakeholder community to drive progress, making payments better for European consumers and businesses.

The EBA has close to 180 members from the European Union and across the world.
For additional information about the Euro Banking Association, please visit our **website** or follow us on **LinkedIn**.

Capgemini invent

Copyright © 2026 Capgemini. All rights reserved.