DIGITALSIGN - CERTIFICADORA DIGITAL, SA.

THE EUROPEAN DIGITAL IDENTITY WALLET
WHAT CHANGES FOR ORGANISATIONS

CONTEXT, USE CASES AND THE ROLE OF QUALIFIED TRUST SERVICE PROVIDERS

CONTENTS

Executive Summary

The way we prove who we are is about to change. For decades, digital identification has relied on fragmented national systems, on manual processes and on the digitisation of physical documents. With Regulation (EU) 2024/1183, eIDAS 2.0, which established the European Digital Identity Framework, the European Union sets a new standard: the European Digital Identity Wallet.

Each Member State is required to provide at least one certified Wallet within 24 months of the entry into force of the relevant implementing acts, that is, foreseeably by the end of 2026. And, at the latest 36 months after those acts, therefore by around 24 December 2027, organisations in regulated sectors will be required to accept the Wallet as a means of identification, at the request of the holder, under Article 5f of eIDAS 2.0.

In this white paper, we explain what the European Digital Identity Wallet is, what role it plays in the digital transformation of citizens and, above all, of organisations, and we present the main use cases, with a natural emphasis on the financial sector without overlooking other high-value domains. The European Digital Identity Wallet does not render Qualified Trust Service Providers (QTSPs) redundant: on the contrary, it industrialises demand for precisely what a QTSP is authorised to do, namely to verify identities, certify attributes and sign or seal with legal value.

1. What is the European Digital Identity Wallet

The European Digital Identity Wallet is, as defined in Article 3, point (42), of eIDAS 2.0, an electronic identification means that allows its holder to securely store, manage and validate their person identification data and electronic attestations of attributes, to provide them to those who require them and, further, to sign by means of a qualified electronic signature and to apply qualified electronic seals.

In simple terms, it is a mobile application in which the citizen, resident or business comes to hold, in a single place and under their control, their digital identity and a set of verified attributes: academic qualifications, professional certifications, licences, powers of representation, among many others.

One principle sets the European Digital Identity Wallet apart from current identification systems: the selective disclosure of attributes, expressly enshrined in Article 5a(4)(a). The holder shares only the information strictly necessary for each interaction. Thus, to prove that they are of age, the holder need not reveal their date of birth; to prove a professional qualification, they need not disclose the full identity document. Control over the data therefore remains at all times with the holder.

The legal basis is Regulation (EU) 2024/1183, which amended Regulation (EU) No 910/2014 and entered into force in May 2024.

> **Selective Disclosure**
>
> With the European Digital Identity Wallet, proving a fact no longer requires disclosing an entire document. The holder shares only the strictly necessary attribute, for example 'over 18', without revealing the date of birth or the full identity. This is a gain in both convenience and privacy at once.

2. The Architecture of Trust

Three elements underpin trust in the European Digital Identity Wallet, and it is important to distinguish them: (i) the *person identification data* (PID), defined in Article 3, point (3), which make it possible to determine the identity of the holder and constitute the identity core of the Wallet; (ii) the *electronic attestations of attributes*, which attest specific facts about the holder, such as an address, a tax identification number, a qualification or a power of representation, and which, where issued by a QTSP and where the requirements of Annex V to the Regulation are met, take the form of a qualified electronic attestation of attributes (QEAA), defined in Article 3, point (45); (iii) the *qualified electronic signature* and the *qualified electronic seal*, which the Wallet integrates natively and which confer, on the natural person and the legal person respectively, the ability to sign and to seal documents with full legal value.

As regards the rigour of identification, eIDAS defines three assurance levels, 'low', 'substantial' and 'high' (Article 8), which express the evidential weight of an electronic identification means. It should be stressed that the Wallet is provided, as required by Article 5a(11), under an electronic identification scheme with a high assurance level, the most demanding. It is important, nonetheless, not to conflate the two planes: the assurance level relates to the identification means; attestations of attributes, in turn, are trust services and derive their legal value from their qualified status, and not from a grading by assurance levels.

3. Who Issues the Wallet, and Why It Matters

The Wallet may be provided by the Member State itself, by an entity mandated by it, or through the recognition of a private solution. Moreover, the Regulation provides that person identification data be issued by a public authority or by a party to whom it delegates, which opens the door for a duly certified QTSP to act in that role.

This distinction matters. A private QTSP, such as DigitalSign, operates under European regulatory supervision, subject to stringent obligations of security, auditability and data protection, but with the agility, capacity for innovation and market proximity that a public body can rarely ensure. It is this combination that makes QTSPs central actors in the implementation of the Wallet, not merely as integrators, but as issuers of qualified trust.

Trust in the system as a whole is, finally, signalled by a dedicated mark: Article 3, point (50), establishes the 'EU Digital Identity Wallet Trust Mark', a verifiable and recognisable indication that a given Wallet has been provided in accordance with the Regulation.

4. Timeline

When	Milestone
May 2024	Entry into force of eIDAS 2.0, Regulation (EU) 2024/1183.
By around 24 Dec. 2026	Each Member State provides at least one certified Wallet, within 24 months of the implementing acts (Art. 5a(1)).
10 Jul. 2027	The Anti-Money Laundering Regulation (AMLR) becomes applicable.
By around 24 Dec. 2027	Organisations in regulated sectors become required to accept the Wallet, at the holder's request, within 36 months of the implementing acts (Art. 5f(2)).

The 24-month and 36-month periods run, under the Regulation, from the entry into force of the relevant implementing acts; the dates indicated result from that calculation, assuming their entry into force on 24 December 2024.

5. What Changes for Citizens

For the citizen, the European Digital Identity Wallet represents convenience with control. A single application will make it possible to identify oneself to public and private services, in any Member State, to sign contracts with legal value, to access healthcare services or to prove qualifications, revealing on each occasion only what is strictly necessary. Selective disclosure returns to the holder command over their data, reversing the current logic, in which proving a simple fact most often requires exposing an entire document.

6. What Changes for Organisations

This is where the essence lies. From the time limit in Article 5f(2), organisations that are required, by law or by contract, to use strong user authentication, a category that includes, in particular, banking, financial services, insurance, telecommunications, energy, crypto-asset service providers and very large online platforms, will have to accept the European Digital Identity Wallet as a means of identification, at the holder's request.
A terminological note is warranted here: the Regulation refers to the organisation that accepts and relies on the European Digital Identity Wallet as the 'relying party', and reserves the term 'user' for the holder. For clarity, we use 'organisation' and 'holder' here.

Acceptance Obligation (Article 5f of eIDAS 2.0)
Acceptance of the Wallet is not a commercial option; it is a legal obligation for organisations in regulated sectors subject to strong user authentication, to be complied with at the holder's request, within 36 months of the entry into force of the implementing acts, foreseeably by 24 December 2027.

Nevertheless, the implications go well beyond mere compliance:

- Faster and less costly onboarding. The customer's identity has already been verified and certified at source. The organisation receives the attributes it needs instantly, with no manual collection of documents and no redundant checks, reducing integration time and operational costs.
- A truly pan-European operation. An identity verified in one Member State is recognised in all the others. One of the greatest points of friction, the re-verification of identity in each new market, is eliminated, and a single integration comes to serve all 27 markets.
- Contracts with full legal value at a distance. The European Digital Identity Wallet natively integrates the qualified electronic signature, which has the same legal value as a handwritten signature throughout the Union. Concluding contracts remotely, securely and paper-free, ceases to be the exception and becomes the norm.
- Less data, less risk. Selective disclosure means that the organisation collects only what is strictly necessary for each transaction. Less data stored means lower exposure in the event

of a security incident and less effort to comply with the GDPR, not least through data minimisation.

7. Use Cases: Where the Wallet Creates Value

7.1. Financial Services, the Immediate Focus

The financial sector is at once the most mature and the one with legally guaranteed demand, since it is there that the acceptance obligation of Article 5f intersects with identity verification duties. The following cases stand out:

- Account opening and onboarding (KYC): the customer presents their person identification data and the required attestations of attributes, with selective disclosure, reducing the process from days to minutes.
- Customer due diligence (CDD) in relation to money laundering: as we develop below, the AMLR expressly recognises the Wallet and qualified attestations of attributes as appropriate means of verification.
- Strong customer authentication (SCA): the Wallet natively supports strong authentication aligned with PSD2, and Article 5f requires banks and payment service providers to accept it, at the customer's request.
- Qualified signature of credit, loan, insurance or investment contracts: once the customer has been identified through the Wallet, the contracting is completed entirely at a distance, with a qualified electronic signature.
- Crypto-asset service providers (MiCA): these too are among those required to accept the Wallet, which standardises and reuses identity verification.

7.2. Other High-Value Sectors

- Health: cross-border electronic prescriptions and patient summaries, with the presentation of healthcare professional credentials and reimbursement entitlements.
- Education and professional qualifications: diplomas, micro-credentials and professional licences as verifiable credentials, with instant, fraud-proof verification by employers and regulators.
- Mobility and travel: mobile driving licence (mDL), travel credentials and streamlined check-in.
- Telecommunications: registration and activation of SIM cards with identity verification, in a sector likewise covered by the acceptance obligation.
- Public sector: identification and authentication with national and cross-border services, dovetailing, in Portugal, with Chave Móvel Digital and the gov.pt application.
- Age verification: cryptographic proof of majority without revealing the date of birth or the identity, a direct response to the duties to protect minors arising from the Digital Services Act.

- Business-to-business relations (B2B): immediate proof of powers of representation, of the legal person's identification number and of mandates, with relevance for public procurement, electronic invoicing and business-to-business contracting.

EVIDENCE OF MATURITY: THE LARGE-SCALE PILOTS

The European Digital Identity Wallet is not a theoretical exercise. Four large-scale European consortia have tested it, involving hundreds of public and private entities: POTENTIAL (public services, bank account opening, SIM registration, driving licences, qualified signatures and electronic prescriptions), EWC (travel credentials, payments and the business wallet), NOBID (payments) and DC4EU (education and social security).

8. The Role of QTSPs, and of DigitalSign, in This Transition

The Wallet multiplies, rather than eliminates, demand for qualified trust services. A QTSP such as DigitalSign intervenes, specifically, on four fronts:

- the issuance of qualified electronic attestations of attributes (QEAA), with legal value throughout the European Union;
- qualified electronic signatures and qualified electronic seals, the regulated product par excellence, now consumable from the European Digital Identity Wallet;
- remote identity proofing of persons, based on the ETSI TS 119 461 standard, for the onboarding of holders and the issuance of credentials at the high assurance level;
- integration and verification for organisations that accept the European Digital Identity Wallet, that is, a single route to securely accept any European Wallet;

DigitalSign is a Qualified Trust Service Provider, supervised by the Portuguese National Security Office (Gabinete Nacional de Segurança) and recognised at European level. With more than two decades of experience in digital identity and trust services, it is well positioned to support organisations and citizens across every dimension of this transition, from the issuance of qualified credentials to integration into business processes.

9. Convergence with the New Anti-Money Laundering Regulation

On 10 July 2027, Regulation (EU) 2024/1624, the AMLR, becomes applicable, harmonising customer due diligence duties throughout the Union. The Wallet and the AMLR work together: the Wallet provides the means of verification; the AMLR defines the degree of rigour required. Indeed, Article 22(6)(b) of the AMLR recognises electronic identification means at the substantial or high level and qualified trust services as appropriate methods of remote identity verification. And eIDAS 2.0 itself, in Recital 62, points to secure electronic identification and the provision of attestation of attributes as a solution enabling the financial services sector to fulfil customer due diligence. The same process that improves the customer experience thus satisfies regulation.

10. CONCLUSION

The European Digital Identity Wallet is not merely a technological change. It is the construction of a European trust infrastructure that redefines the relationship of organisations with their customers, employees and partners. For those who regard it as an opportunity, and not merely as an obligation, it brings more efficient processes, a truly European reach and a foundation of digital trust with measurable economic value.
For organisations that want to be prepared in 2027, the time to begin is now.

Would you like to know how DigitalSign can support your organisation in the transition to eIDAS 2.0? Talk to our team.