From fragmentation to sovereign interoperability

The digital future of Europe: a unique and secure identity

May 2026

gradiant

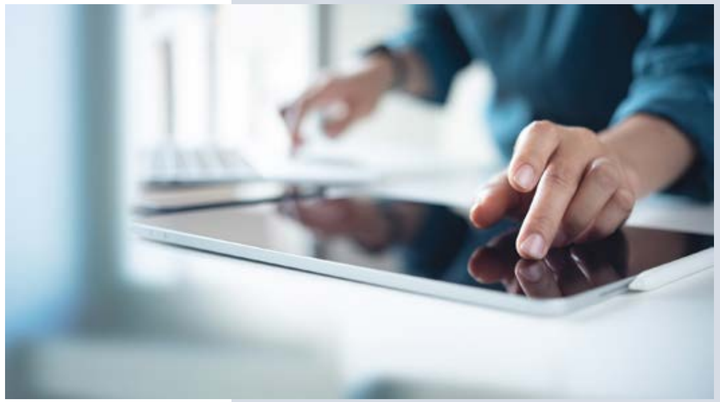
1.

From a mosaic of digital identities to a single, secure European solution

Last year, seven out of ten Europeans aged between 16 and 74 used a public authority's website or app. Most did so to look up information on:

- Services, benefits, laws or opening hours **(44%)**
- Access to personal data **(40%)**
- Downloading or printing forms **(38.1%)**.

At the other end of the scale, just 5.3% used this channel to submit applications, claims or complaints.



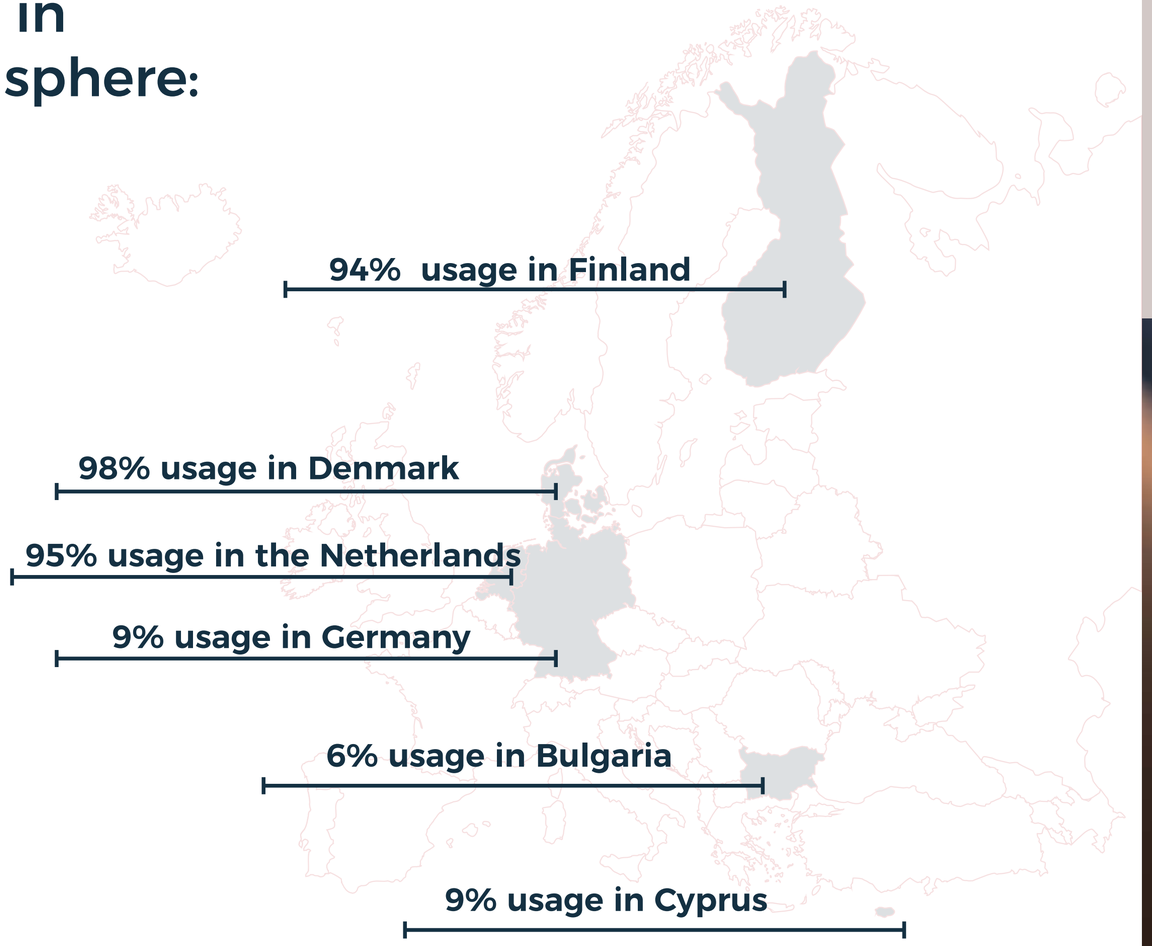
86%

Government services in the European Union are now available online, according to the eGovernment Benchmark 2024 report produced by Capgemini.

41%

People aged between 16 and 74 in the EU reported having used their eID to access online services for private purposes. According to Eurostat data from 2023.

Inequality between countries in its application in the private sphere:



The rise of digital services entails new challenges:

Identity theft

Data breaches

Fraud

For this reason, ensuring the protection of electronic procedures is key:

Not only to safeguarding citizens, but also to maintaining trust in public administration.

With this aim in mind, the **European Union** is moving towards a **personal and secure digital identity**, valid in all Member States

electronic IDentification Authentication and trust Services

To date, electronic identification in Europe has been marked by fragmentation: each country had its own national system, with limited interoperability and very restricted cross-border reach. This situation, governed by the 2014 eIDAS Regulation, left European citizens with uneven experiences, little confidence in the security of their data and few guarantees of use beyond their borders.

eIDAS laid the foundations for the legal framework for digital identification in the EU and regulated trust services such as electronic signatures and electronic seals. However, its practical application proved insufficient.

14 Member States

formally notified a digital identity scheme, and acceptance beyond national borders was minimal.

Result

Electronic transactions that were uneven, friction in identity verification - often dependent on manual processes or private intermediaries - and growing concerns about privacy.

Private sector

Integrating eID and trust services makes it possible to replace in-person procedures with secure digital operations, such as **opening accounts, signing contracts and onboarding customers**. This delivers significant savings in time and resources by reducing the administrative burden and the cost of manual identity verification.

MAY 2024: a turning point

- New European Regulation **(UE 2024/1183)**
- Launch of the European Digital Identity Wallet **(EUDI Wallet)**

THIS MARKS A TURNING POINT, SEEKING TO REVOLUTIONISE THE WAY CITIZENS AND BUSINESSES IDENTIFY THEMSELVES ONLINE.

It is **intended** to be:

✓ Secure ✓ Portable ✓ Valid

It aims to:

1.- Reduce costs
2.- Reduce frictions
3.- Reduce risks in access to both public and private services

Objective

From a mosaic of national solutions → **to a single European digital identity**

It will mark a before and after in the relationship between citizens, businesses and administrations.

Deadline

28 November 2024:
Implementing acts are adopted

Start of the period:
The maximum period begins to run from that date.

Length of the period:
24 months.

Resulting deadline:
December 2026.

Obligation on Member States:
To offer at least one wallet free of charge.

The challenge goes beyond a simple regulatory update, and achieving the objective will depend on coordination between governments, the private sector and the technology ecosystem.

This report analyses the key aspects of the **EUDI Wallet** deployment strategy**:**

Implementing acts

Wallet certification

Large-scale pilots (LSP)

Technological challenges and solutions

Triple perspective

Technology

Policies

Market needs

2.

eIDAS 2: the pillars of the new paradigm

eIDAS 2.0 is an update to the European regulation on electronic identification and trust services. It came into force in May 2024, introducing the **European Digital Identity Wallet (EUDI Wallet)**, a unified and sovereign digital identity that will mark a before and after in the relationship between citizens, businesses and administrations.

This regulation represents a paradigm shift. Its key elements are:

1

European Digital Identity Wallet (EUDI Wallet)

Each Member State will be required to make at least one digital wallet available free of charge before the end of next year. It may be used by citizens, residents and also by businesses. This tool will be valid and recognised throughout the European Union, thanks to a technical and legal interoperability framework that guarantees its use without border barriers. The European Commission has also left open the possibility for private providers to offer their own EUDI Wallet.

2

Interoperability and security

The wallet must be interoperable between national systems and comply with high security standards, including cybersecurity certification by the European Union Agency for Cybersecurity (ENISA).

3

Full user control over their data

Users can decide what information to share and with whom, applying the principle of data minimisation.

4

Access to public and private services

From the end of 2027, all service providers that require strong authentication -such as banking, telecommunications, health, education, transport, energy and e-commerce- will be required to accept the EUDI Wallet as a valid means of identification and authentication.

5

Integrated trust services

The wallet will include services such as electronic signatures, electronic seals and electronic attestations of attributes.

6

Data protection and privacy

Technologies such as selective disclosure will be implemented to minimise the information exchanged, guaranteeing data protection in accordance with Regulation (EU) 2016/679 (GDPR).

EUDI Wallet

01

Full portability
A single identity valid throughout the EU.

02

Enhanced privacy
Granular control over shared information.

03

Certified security
Compliance with the highest cybersecurity standard.

04

Real interoperability
Mandatory acceptance across the European Union.

Immediate Opportunities

The European Digital Identity Wallet will allow every European citizen to access, identify themselves and act online with security, convenience and control, consolidating a more inclusive, interoperable and human-centred digital Europe.

In addition, attribute-issuing entities, such as universities, professional associations and administrations, will be able to issue compatible verifiable credentials from the outset.

Trust Service Providers, in turn, will need to adapt their validation, preservation and signature processes to the new legal and technical requirements.

Architecture and Reference Framework (ARF)

The ARF (Architecture and Reference Framework) is the common guide created by the European Union for developing the European Digital Wallet. It establishes the rules and standards that ensure different digital wallets are secure, compatible and valid in all EU countries.

Thanks to this framework, citizens will be able to identify themselves and carry out digital procedures in any Member State simply and securely.

The ARF is updated periodically to incorporate new technologies and improvements in interoperability.

3.

Roadmap: keys to full adoption

Five elements will shape the roadmap for the full adoption of the new regulation in the coming years. Each of them is also reflected in the political, market and technological spheres:

1.

The implementing acts that will define in detail how the regulation will be deployed.

2.

The architecture based on key principles that ensure its effectiveness and reliability, such as interoperability, security and privacy, and user control.

3.

The large-scale pilots (LSP), which will test the EUDI Wallet in real-life environments before its general roll-out.

4.

Wallet certification, which is essential to guarantee security and trust.

5.

The reference implementation, a technical solution developed by the European Commission and based on the Architecture and Reference Framework (ARF), which serves as a standard model for developing interoperable, secure digital wallets that comply with European regulation.

Implementing Acts: from legal text to operational reality

2024

20 May: Regulations enters into force.

December: First package of implementing acts covering technical requirements for the digital wallet, the ecosystem, interfaces and certification.

2025

May: Second package of implementing acts covering security breach management, registration and obligations of relying parties, the list of certified wallets and ID matching.

July: Third package of implementing acts covering electronic attestations of attributes, supervision and reporting rules, and review of eID schemes.

End of 2025: Implementing act for the interoperability framework for cross-border identification; specific date to be determined.

2026

24 Decemeber: Each Member State must provide at least one free digital wallet to citizens, residents and organisations.

2027

December: The requirement for certain public and private organisations to accept the wallet as a means of identification where strong authentication is required comes into force.

One of the key aspects of this regulation is the creation and implementation of detailed rules and procedures through a series of gradual implementing acts.

These acts seek to establish clear rules and procedures that guarantee the security and interoperability of the European Digital Identity Wallet and cybersecurity certification schemes. They define certification processes to ensure that wallets and other related services comply with European standards, promoting trust between Member States.

They also ensure operational compliance for trust services, such as electronic attestation of attributes - accreditation of a person’s identity in the digital sphere, and the electronic ledger transaction, records that ensure verifiable and secure traceability, thereby improving the reliability of digital transactions in the EU.

Implementing acts from a tri-axial perspective

The approval of the implementing acts requires coordinated progress on three levels.

Political and governance level

The key lies in harmonising criteria without losing sovereignty: Member States must build a common framework that avoids national dialects while ensuring effective supervision, with shared indicators and a clear circuit for sanctions and corrective measures.

Market level

The market, for its part, faces the challenge of incorporating the EUDI Wallet as a competitive standard. Financial institutions, e-commerce and healthcare must plan an adaptation timetable that allows them to integrate in advance, capitalising on the advantage of frictionless onboarding and reduced fraud.

Technology level

From the technological perspective, success depends on consolidating API specifications, credential formats and cryptographic verification mechanisms that ensure resilience, minimal latency and robust cross-border operation.

Only **synchrony** between these **three areas** will allow the regulation to become an **interoperable and secure reality.**

Anticipating the deadlines set by the implementing acts can be a competitive advantage for companies.

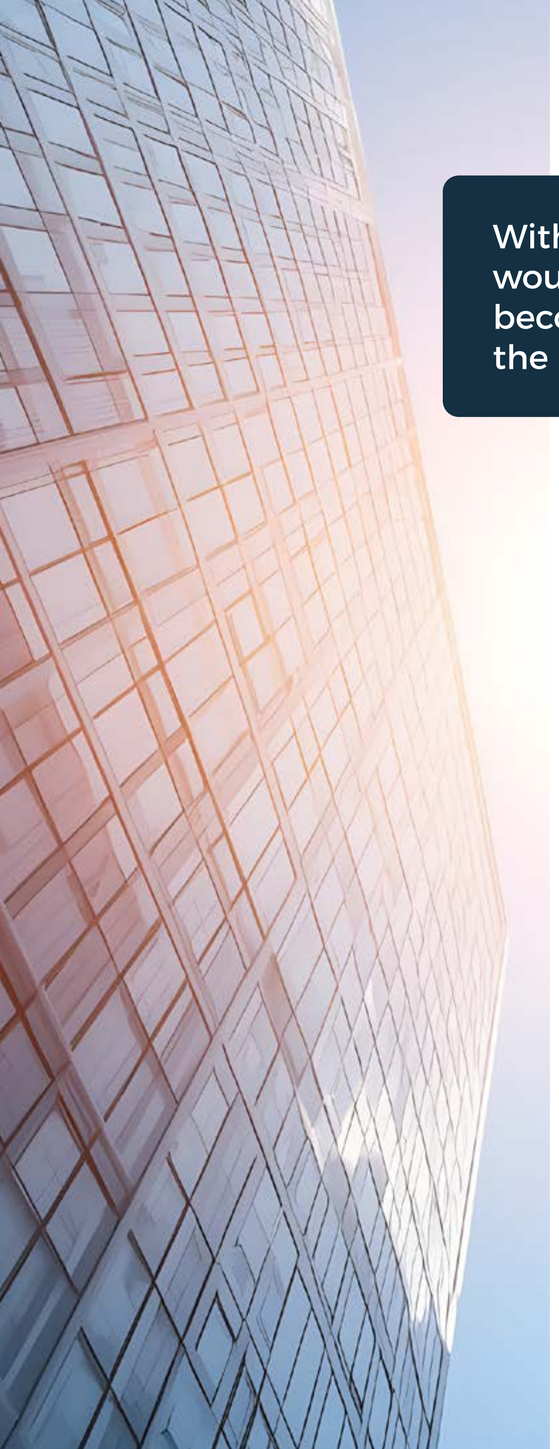
On the other hand, it is essential to take the market view into account. Companies need to see these acts not as a formality, but as a technical manual defining how they can integrate into the EUDI Wallet.

Each package brings opportunities - new forms of digital onboarding, authentication or signature - but also obligations, such as registration, mandatory acceptance and systems adaptation.

Wallet certification from a tri-axial perspective

- Homogeneous approval criteria.
- Accredited laboratories.
- Repeatable evaluation processes that guarantee trust in all Member States.

At the economic and market level, obtaining the certification mark becomes a brand asset. It is capable of conveying reliability to both end users and institutional clients, and of requiring the entire value chain - verifiers, issuers and trust entities - to document their compliance.



Without this convergence, certification would be a mere formality; with it, it becomes the real licence to operate in the European ecosystem.

The technological level completes the triangle

01

End-to-end encryption.

02

Hardware protection.

03

Secure key management.

04

Immediate revocation mechanisms, which are essential to uphold the promise of a “high” level of assurance.

05

Use of zero-knowledge proofs.

Large-scale pilots (LSP): validation in the real world

Large-scale pilots, or LSP, are initiatives funded by the European Commission that make it possible to test and improve the technical specifications of the digital wallet before its widespread implementation in the Member States. These projects cover a wide variety of everyday use cases, involving more than 350 public and private entities from 26 Member States, as well as Norway, Iceland and Ukraine.

There are several key projects and consortia for the development of digital identity in Europe

Seeks to foster innovation in six strategic sectors: government services, banking, telecommunications, mobile driving licences, electronic signatures and health.

POTENTIAL

A multinational project that tests the European Digital Identity Wallet.

Digital Credentials for Europe (DC4EU)

TWorks on the implementation of digital travel credentials to facilitate secure cross-border mobility.

EU Digital Wallet Consortium (EWC)

Made up of Nordic and Baltic countries, Italy and Germany, and designed to test the use of the digital wallet when authorising payments and promoting interoperability in electronic transactions.

NOBID

Large-scale pilots (LSP) from a tri-axial perspective

Large-scale pilot projects (LSP) act as a reality filter for the whole system. From a governance perspective, they allow Member States to draw joint lessons and turn them into operational guidelines that facilitate later adoption, including in local administrations.

In the market arena, these pilots give organisations the advantage of being first movers: they can test onboarding, electronic signature and attribute verification processes with real users, measure conversion and abandonment rates, and adjust business models before general mandatory acceptance takes effect.

On the technological front, LSP are a genuine interoperability laboratory, where credentials, presentation flows and revocation mechanisms are validated across different platforms, operating systems and networks, identifying bottlenecks and guaranteeing service stability.

Joint experience across these three levels is what will make it possible to reach 2026 with controlled risks and infrastructure ready to scale.

LSP are essential for validating and verifying systems and detecting possible risks before mass deployment.

4.

Technological challenges and solutions

One of today's challenges is managing the vast amount of information generated in any production process, in public administration and public service systems, or in the different development phases of any company.

Technology centres such as **Gradiant**, a European leader in the development of **deep tech** in the field of ICT, work to provide solutions that enable all this data to be stored, managed and used efficiently with applied artificial intelligence techniques. The centre has extensive experience in the development and design of information-processing systems of different kinds and adapted to different environments.

These tools use applied artificial intelligence to extract relevant information that companies and public administrations can apply with full guarantees of security and privacy.

In parallel with the development of these solutions, **Gradiant** has also made progress in guaranteeing:

- Security
- Privacy
- Data anonymisation, extracting highly useful information from data to speed up processes in which time is a key factor.

Technologies such as **blockchain** can serve as a basis for building secure identity platforms, where companies, public administrations and citizens can verify identity attributes in a decentralised way.

Blockchain would act as an immutable and transparent register on which to build a trust anchor that entities can use to verify information coming from wallets.

In this regard, it is worth differentiating between credentials:

Qualified credentials

These may be issued by trust service providers or by public entities registered as qualified issuers. Above these sits PID (Person Identification Data), the credential that identifies a natural person as a citizen of the Union. PID may only be issued by organisations designated at national level, such as the police.

Non-qualified credentials

These are credentials that any entity wishing to perform an action with an e-wallet can issue.

5.
NovaWallet: the future of identity in the EU

Digital wallets have become one of the flagship products for users of mobile devices. Companies and public administrations are joining the use of this technology to facilitate access to online services, especially now that digital wallets will become an essential component of digital identities under the eIDAS2 framework.

Within the European digital identity ecosystem, Gradiant has NovaWallet, a simple, reliable e-wallet aligned with eIDAS2 and the EBSI (European Blockchain Services Infrastructure). It is a solution - available for iOS, Android and web - that allows European citizens to access the online services offered by public administrations more quickly and easily, while guaranteeing their security and privacy.

The wallet combines:

designed to facilitate business adoption of sovereign identity schemes.

NovaWallet is a Gradiant tool already available to facilitate an interoperable and sovereign European digital identity as required by eIDAS2.

This innovation, designed to replace current digital certificates, is one of the first e-wallets to receive the European EBSI seal of conformity, accrediting it as one of the secure proofs of identity compatible with its regulatory model for citizens' digital identification.

By incorporating blockchain technology into this digital wallet, Gradiant offers a complete service that enables user authentication in a fully secure and reliable way, for both individuals and organisations.

NovaWallet has been one of the first digital wallets to receive the European seal of conformity.

NovaWallet supports both same-device and cross-device flows and is prepared to offer cloud back-up with high levels of privacy and security.

It also includes a framework that enables the creation of ad hoc digital wallets, as well as future standardised wallets such as the EU Business Wallet (EUB Wallet) or other bespoke solutions that an organisation may want for its internal processes.

NovaWallet features

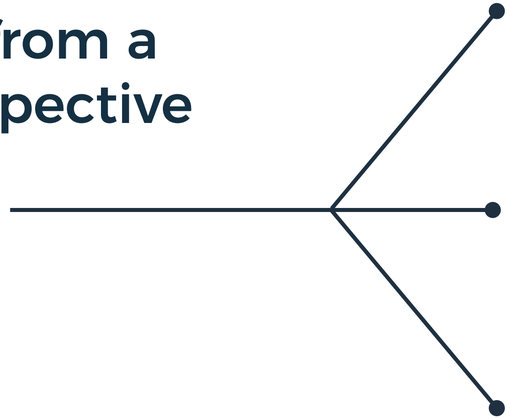
Integration with EBSI and eIDAS2
Adopts interoperability standards, verifiable credentials and exchange protocols aligned with European regulation.

Multiple roles
Companies can operate as a Trusted Accrediting Entity (TAE), Trusted Issuer (TI) or Verifier, facilitating the entire cycle of issuing, receiving and validating credentials.

Advanced privacy and security
Implements privacy-enhancing technologies (PET), trusted execution environments (TEE), selective disclosure and zero-knowledge proofs (ZKP), strengthening user control over their data.

Fluid experience
Its intuitive interface facilitates registration, onboarding, credential management and presentation, without compromising accessibility, including TEE support and cloud mobility

Analysis of NovaWallet from a tri-axial perspective



At the political and governance level, the solution aligns with the eIDAS2 regulation and with European Blockchain Services Infrastructure standards, offering administrations a tool that facilitates interoperability and the definition of credential management and revocation policies.

From the market perspective, its value proposition is clear: it reduces internal development costs, accelerates onboarding and verification processes, and opens opportunities in sectors as diverse as finance, education, health and public administration, backed by already validated use cases.

At the technological level, NovaWallet stands out for its secure architecture - with trusted execution enclaves, advanced privacy techniques and full compatibility with iOS, Android and web - its observability through detailed metrics and its strict adherence to EBSI standards, guaranteeing fast and reliable **integration.**

The combination of these three vectors turns the platform into a real accelerator for those who must meet the deadlines for European digital identity.

Real use cases

NovaWallet has already been validated in real-life scenarios such as:

- **Digital onboarding in public administration, financial security, telecommunications and mobility.**
- **Public administration procedures based on sovereign identity.**
- **Issuing and verifying educational and professional certificates.**
- **Pilots in EU-backed projects, especially within the ACID programme for decentralised identity for citizens.**

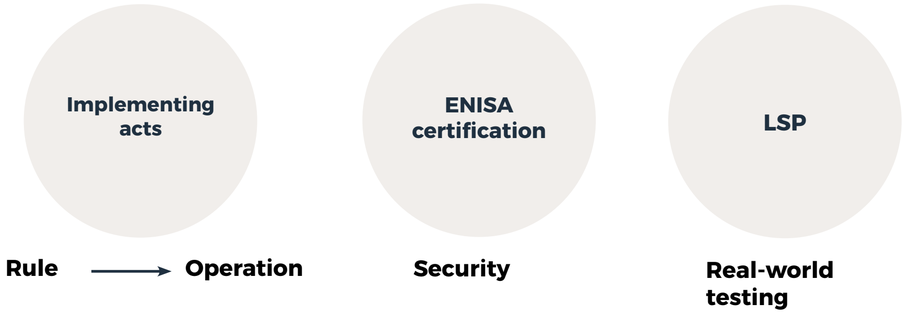
6.

Conclusions

European digital identity is entering a decisive phase:

Moving from fragmentation to sovereign interoperability.

eIDAS2 + EUDI Wallet



Transforming into operational reality.

Administrations

- Harmonisation and security.
- Common metrics.
- Effective supervision.
- Public trust.

Market / Companies

- Mandatory acceptance.
- Frictionless onboarding.
- Electronic signature.
- Attribute verification.

↓ Fraud ↑ UX

Technology ecosystem

- Stable APIs.
- Robust formats.
- Key management.
- Interoperability engineering.

Interoperability - Security - Trust.

NovaWallet
Gradiant

- EBSI conformity.
- Mature APIs.
- Advanced security.
- Technical certifications.
- Validated use cases.

- ✓ Meet regulatory deadlines.
- ✓ Scale trust.
- ✓ Accelerate adoption.

European Digital Identity

Interoperable, sovereign and operational from today.