

# The future of digital identity: Standards, Features, Opportunities, Use Cases

Deliverable 1: Reference Material

Deliverable 2: Envisioned Wallet with  
Useful materials for stakeholders

Deliverable 3: Practical Implementation of  
EUDI Wallet Standards: Use Cases and  
Application Scenarios

Scope:  
Standards  
EU Digital Identity Wallet  
Distributed Ledger Technologies  
Identity Proofing  
Verifiable Credential

Writer: [Mickaël Gaborit](#)

## Agenda

<b>1</b>	<b>INTRODUCTION.....</b>	<b>4</b>
1.1	RATIONALE.....	4
1.2	WHY BLOCKSTAND?.....	5
1.2.1	BLOCKCHAIN STANDARDIZATION EXPERTISE.....	5
1.2.2	SUPPORT FOR EUROPEAN STRATEGIC AUTONOMY.....	5
1.2.3	ENGAGEMENT AND COLLABORATION PLATFORM.....	5
1.2.4	INNOVATION AND FUTURE-PROOFING .....	6
1.2.5	ENSURING INTEROPERABILITY AND COMPLIANCE.....	6
1.3	IMPACT.....	6
1.4	PURPOSE OF THE FINAL DOCUMENT .....	7
<b>2</b>	<b>ENVISIONED WALLET FOR STAKEHOLDERS.....</b>	<b>9</b>
2.1	EVOLUTION OF WEB AUTHENTICATION: A WALLET BUTTON TO DO IT ALL, AUTHENTICATION AND IDENTIFICATION.....	9
2.1.1	WEB 1.0 .....	9
2.1.2	WEB 2.0 .....	9
2.1.3	WEB 3.0 .....	10
2.2	DECENTRALIZATION OF DIGITAL IDENTITY TEMPLATE: SIMPLICITY, SECURITY, SOVEREIGNTY, SOBRIETY .....	11
2.2.1	IDENTITY SCHEMA.....	11
2.2.2	KEY STANDARDS.....	13
2.3	COMPLIANCE WITH A NEW ECOSYSTEM OF TRUST BASED ON EBSI.....	14
2.3.1	KEY PRINCIPLES CHECKLIST .....	14
2.3.2	INTEROPERABILITY.....	14
2.3.3	KEY STANDARDS.....	15
2.4	OUR DIGITAL IDENTITIES GO BEYOND THE PIVOT IDENTITY .....	16
2.4.1	MOBILITY & TRAVEL .....	18
2.4.2	FOOD INDUSTRY.....	18
2.4.3	SOCIAL MEDIA .....	18
2.4.4	LEGAL ENTITY IDENTITY.....	18
2.4.5	E-GOVERNMENT .....	18
2.4.6	HUMANITARIAN BANKING .....	19
2.4.7	FINANCIAL SERVICES.....	19
2.4.8	HEALTH INDUSTRY .....	19
2.4.9	TELECOMMUNICATIONS.....	19
2.4.10	E-COMMERCE.....	19
2.4.11	SMART CITIES .....	20
2.4.12	INDUSTRY USES CASES AND STANDARDS MAPPING.....	20
2.5	COMPLIANCE WITH A NEW ECOSYSTEM OF TRUST BASED ON EUDIW .....	20
2.5.1	WHAT IS A CITIZEN WALLET? .....	21
2.5.2	ENROLMENT: ESTABLISHING A TRUSTED DIGITAL IDENTITY .....	23
2.5.3	TRUST FEATURES: ENABLING SECURE DATA SHARING & TRANSACTIONS .....	23
2.5.4	PRESENTATION TO END SERVICES: SEAMLESS & SECURE AUTHENTICATION .....	24
2.5.5	KEY BENEFITS .....	24

## The future of digital identity: Standards, Features, Opportunities, Use Cases

2.5.6	COMPLIANCE CHECKLIST FOR DIGITAL IDENTITY WALLETS (EUDIW).....	24
2.5.7	COMPLIANCE GUIDELINES.....	25
2.6	ENVISIONED WALLET FEATURES TEMPLATES.....	25
2.6.1	WALLET AUTHENTICATION .....	27
2.6.2	USER INTERFACE OPTIONS.....	27
2.6.3	SECURITY FEATURES .....	27
2.6.4	VC MANAGER (VERIFIABLE CREDENTIALS LIFECYCLE MANAGEMENT) .....	28
2.6.5	STORAGE OPTIONS.....	28
2.6.6	SECURE ENCLAVE OPTIONS.....	28
2.6.7	API FEATURES .....	29
2.6.8	CORE FEATURES.....	29
2.6.9	WALLET FEATURES AND STANDARDS MAPPING .....	31
2.7	3 SECURE STORAGE OPTIONS TO HELP STAKEHOLDERS CHOICE.....	31
3	<u>IMPLEMENTATION STEPS AND COMPLIANCE CHECKLISTS FOR STAKEHOLDERS.....</u>	<u>33</u>
3.1	IDENTIFY YOUR ROLE AND SCOPE WITHIN THE EUDI WALLET ECOSYSTEM.....	33
3.2	DEFINE INFORMATION SECURITY OBJECTIVES AND RESPONSIBILITIES .....	33
3.3	CONDUCT A RISK ASSESSMENT .....	34
3.4	DEFINE DATA CLASSIFICATION AND LIFECYCLE POLICIES.....	34
3.5	IMPLEMENT ACCESS CONTROL POLICIES .....	35
3.6	ENSURE SECURE DEVELOPMENT AND MAINTENANCE.....	35
3.7	ADDRESS DATA PROTECTION AND PRIVACY COMPLIANCE.....	35
3.8	MANAGE THIRD-PARTY AND INTEROPERABILITY RISKS .....	36
3.9	ENSURE INCIDENT MANAGEMENT AND BUSINESS CONTINUITY.....	36
3.10	MONITOR AND AUDIT COMPLIANCE CONTINUOUSLY.....	37
3.11	ALIGN PRODUCT FEATURES WITH FUNCTIONAL AND LEGAL EXPECTATIONS .....	37

# 1 Introduction

## 1.1 Rationale

Digital Identity will be totally transformed (law, usages, standards), and every public or private organization should be aware about which standards are the basis to evaluate which standards will be transformed.

Consequently, they need a standard Inventory considering the future eIDAS rules and Wallet ARF (Architecture and Reference Framework) to ensure consistency, interoperability, and security in the implementation of electronic identification and authentication systems. This ARF is open to DLT.

Having a standard Inventory or set of standardized guidelines and best practices helps in the following ways:

- **Consistency:** A standard Inventory ensures that all organizations follow a common set of rules and practices, leading to consistent and uniform approaches to electronic identification and authentication. This consistency is crucial for seamless interactions between different systems and services.
- **Interoperability:** Standardization facilitates interoperability between various eIDAS-compliant systems, enabling smooth information exchange and interactions across different platforms. This interoperability is vital for public and private organizations to collaborate effectively and provide services to users seamlessly.
- **Security:** Adhering to standardized security measures helps organizations protect sensitive user data and ensures a higher level of cybersecurity. A standard Inventory can provide guidelines for implementing robust security protocols and safeguards against potential threats and vulnerabilities.
- **Compliance:** With future eIDAS rules and Reference Architecture Framework in mind, a standard Inventory can help organizations align with regulatory requirements and ensure compliance with relevant laws and guidelines. It provides a clear roadmap for organizations to follow while developing and deploying electronic identification and authentication systems.
- **Efficiency:** By following standardized practices, organizations can streamline their processes, reduce duplication of efforts, and achieve greater operational efficiency. This efficiency ultimately benefits both the organization and the users accessing their services.
- **Future-Proofing:** A standard Inventory can consider emerging technologies and evolving regulatory requirements, allowing organizations to future-proof their electronic identification and authentication systems. It enables organizations to stay ahead of the curve and adapt to changes in the digital landscape.

In summary, a standard Inventory is essential for public and private organizations to create a cohesive and robust ecosystem of electronic

The future of digital identity: Standards, Features, Opportunities, Use Cases

identification and authentication solutions. It fosters consistency, interoperability, security, compliance, efficiency, and future readiness, all of which are vital for the successful implementation of eIDAS rules and Reference Architecture Framework.

## 1.2 Why Blockstand?

Blockstand is a pivotal initiative aimed at reinforcing the European Union's leadership in the global landscape of blockchain standardization. This project underscores the significance of blockchain technology for the EU's industrial dominance on the international stage.

Blockstand's core mission is to ensure that the internationally applied standards in blockchain not only bolster European leadership in this cutting-edge domain but also reflect the continent's values and requirements. By coordinating the inputs of experts, Blockstand serves as a crucial instrument for supporting Europe's strategic autonomy, emphasizing the importance of blockchain standards that align with European principles and needs.

Utilizing Blockstand to create an inventory of standards impacting or impacted by the new eIDAS regulation was a logical step for several strategic and operational reasons, grounded in both the objectives of Blockstand and the significance of the eIDAS regulation in the context of Europe's digital transformation:

### 1.2.1 Blockchain Standardization Expertise

Blockstand focuses on enhancing European leadership in global blockchain standardization. Since the eIDAS regulation plays a crucial role in establishing a regulatory framework for electronic identification and trust services across Europe, Blockstand's expertise in blockchain standardization could facilitate the integration of new blockchain standards and technologies within the eIDAS framework. This is particularly pertinent for aspects related to security, trust, and interoperability, which are fundamental to both the blockchain ecosystem and the eIDAS regulatory landscape.

### 1.2.2 Support for European Strategic Autonomy

Blockstand aims to support European strategic autonomy in blockchain standardization, ensuring that international standards reflect European values and needs. The eIDAS regulation is central to the European Digital Single Market, aiming to enhance trust in electronic transactions. By aligning with Blockstand, there's an opportunity to ensure that the development and update of eIDAS-related standards are in harmony with European strategies and autonomy, especially in areas where blockchain technologies intersect with digital identity and trust services.

### 1.2.3 Engagement and Collaboration Platform

Blockstand provides a platform for stakeholders to engage in standardization activities, offering a collaborative environment for experts, policymakers, and industry representatives. The eIDAS regulation

The future of digital identity: Standards, Features, Opportunities, Use Cases necessitates broad consensus and alignment across different sectors and countries within the EU. Blockstand's infrastructure and community could serve as a crucial meeting ground for facilitating discussions, sharing best practices, and developing consensus on standards relevant to eIDAS.

#### 1.2.4 Innovation and Future-Proofing

The eIDAS regulation is set to evolve with technological advancements and the changing needs of the digital economy. Blockstand's focus on blockchain implies a forward-looking approach to standardization, crucial for incorporating innovative solutions into the eIDAS framework. This includes exploring how distributed ledger technologies can enhance the security, efficiency, and interoperability of electronic identification and trust services.

#### 1.2.5 Ensuring Interoperability and Compliance

Finally, Blockstand's work on creating a comprehensive inventory of blockchain standards can directly contribute to ensuring that new and existing eIDAS services are interoperable and compliant with emerging blockchain technologies. This is essential for the seamless operation of cross-border electronic transactions and services within the EU, promoting a cohesive and integrated Digital Single Market.

In summary, leveraging Blockstand's resources, expertise, and community platform for developing an inventory of eIDAS-impacting standards was a strategic choice to align blockchain innovation with EU regulatory frameworks, thereby supporting the digital and strategic autonomy of the European Union in the global digital landscape.

### 1.3 Impact

Having a standard Inventory covering identity, certificates, e-signature, and secure elements in Europe can have several positive impacts:

- **Interoperability:** Standardization ensures that different systems and services across Europe can interact seamlessly, promoting cross-border interoperability. This facilitates the exchange of information and services, fostering a more connected and efficient digital environment.
- **Security:** A standardized approach enhances the security of digital identities, certificates, and e-signatures. It establishes consistent security measures and protocols, reducing vulnerabilities and enhancing protection against cyber threats and fraudulent activities.
- **Legal and Regulatory Compliance:** A standard Inventory ensures alignment with legal and regulatory requirements, such as those specified in eIDAS (Electronic Identification, Authentication, and Trust Services) Regulation. Compliance with such standards enhances trust and confidence in digital transactions within Europe.
- **User Trust and Confidence:** Standardization helps build trust and confidence among users in digital services and transactions. Users are



more likely to adopt and use digital identity and signature solutions when they are backed by recognized and standardized frameworks.

- **Market Growth and Innovation:** A common standard encourages the growth and innovation of digital identity and signature solutions. Companies and startups can develop products and services more efficiently, knowing they conform to established standards, and this can foster healthy competition and spur technological advancements.
- **Cross-Border Services:** Standardization facilitates the provision of cross-border services within the EU. Users can access digital services across member states with greater ease, leading to improved efficiency and accessibility.
- **Economic Benefits:** A harmonized approach to digital identity, certificates, e-signature, and secure elements can generate economic benefits. It streamlines processes, reduces operational costs, and encourages the adoption of digital services, contributing to overall economic growth.
- **Simplified User Experience:** Users benefit from a simplified and consistent user experience when interacting with various digital services across Europe.
- **Standardized processes** reduce confusion and friction, making it easier for individuals and businesses to engage in digital transactions.

In summary, having a standard Inventory for identity, certificates, e-signature, and secure elements in Europe creates a more secure, trusted, and efficient digital ecosystem. It promotes innovation, fosters cross-border services, and contributes to the growth of the European digital economy.

### 1.4 Purpose of the final document

This first part is a curated collection of reference materials, including relevant standards organizations and technical specifications, to support further learning and understanding of the subject matter.

The second part (this document and the §2) envisions a future where digital identities are decentralized, secure, interoperable, and seamlessly integrated into various services while maintaining user control and privacy. It will be useful for quick reference and to introduce stakeholders to the main principles. This document complements Deliverable 1 by translating the theoretical inventory of standards into practical resources for stakeholders. It is designed to assist policy makers, project managers, legal and technical stakeholders in the design and deployment of compliant, interoperable, and secure digital identity solutions in line with the European Digital Identity Wallet (EUDIW) and the eIDAS 2.0 regulation.

The last part starts with an exploration of the business potential of digital identity wallets, highlighting key areas for growth, risk assessment, and strategic implementation. The adoption of digital wallets enhances authentication, verification, and trust management, leading to new business models across Digital Services and Trusted Digital Products.

The future of digital identity: Standards, Features, Opportunities, Use Cases

It finishes with some concrete use cases demonstrating how digital identity wallets can streamline identity verification, reduce fraud, and improve user experience across different domains, like Health, Mobility, Education and Employment.

This structured approach ensures that digital identity wallets are positioned as a game-changer for secure, interoperable, and efficient identity verification!



## 2 Envisioned wallet for Stakeholders

### 2.1 Evolution of web authentication: A Wallet button to do it all, authentication and identification

Web 1.0 / 1990	Web 2.0 / 2005	Web 3.0
<ul style="list-style-type: none"><li>• Basic web pages</li><li>• html</li><li>• E-commerce</li><li>• Java &amp; Javascript</li></ul>	<ul style="list-style-type: none"><li>• Generalization/Globalization of Internet Access, Fast Communications, Mobile Access, High-Quality Video (Visio, VOD, Camera)</li><li>• User generation of social media content</li><li>• Monetization of user data by Platforms and Applications then GDPR</li></ul>	<ul style="list-style-type: none"><li>• Semantic Web, AI, Decentralized Governance, Architectures and Distributed Applications</li><li>• Self-sovereign wallet (currencies, NFTs, Metaverse)</li><li>• eIDAS V2 in decentralized mode (EBSI or even public blockchains (few legal guarantees) inspired by the W3C DID standards</li><li>• Paradigm shift on the data economy: users monetize their data, transaction commissions replace subscriptions</li></ul>
<div>Username</div> <div>Password</div>	<div>Sign in with Google</div> <div>Sign in with Facebook</div>	<div>Connect wallet</div>

#### 2.1.1 Web 1.0

Web 1.0 (1990 – 2005) was the first generation of the Internet: static web pages that were accessible and commercialized for the first time. Protocols such as HTTP, HTML, and XML are the birthplace of the World Wide Web. The first web browsers appeared, the first internet service providers to log in, and the first web development tools. Software languages such as Java and Javascript were also created at this time. Overall, these were the early days of the internet.

#### 2.1.2 Web 2.0

Invented in 1999 by Darcy DiNucci, Web 2.0 refers to the participatory culture that has developed on the Internet thanks to user-generated content, social media, and widespread accessibility. Web 2.0 has brought about a change in the way we access the World Wide Web. We can now use our phones, and we have tons of apps at our fingertips, with hundreds of new ones added every day. Our phones have built-in cameras that are of higher quality than most real cameras in the 1.0 web. Today, anyone can be a content creator and share their content 24/7. This is a fundamental part of Web 2.0.

The current generation has also led the social media frenzy with Facebook, Instagram, Twitter, and all the others bursting onto the scene, following the

pioneers like MySpace and Bebo. Digital communication has also reached new heights with people choosing to use apps like WhatsApp or FB Messenger on old-school texts. Despite all this, the main distinction between web 1.0 and web 2.0 is the widespread mobile internet access. It's global. Nearly 4 billion people have access to the Internet today, compared to only 1 billion in 2005.

It's hard not to mention that Web 2.0 is also responsible for **putting our personal data in the hands of large, centralized companies**. Large companies make money from our personal data by selling it to marketers who do targeted advertising, focusing closely on their specific niche audience. While this means you may see more ads for things you're interested in, you've never seen a dime of the sale of your data. This is why we so often talk about abusive advertising. Web 2.0 seems trapped in a destructive and oppressive cycle. He lost touch with the original concept of the Internet – a decentralized website where network participants are equal, and central control ceases to exist. A paradigm shift seems necessary to get back on track.

### 2.1.3 Web 3.0

The top three Google searches attribute this term to three different people; however, it was Tim Berners-Lee who originally spoke about the concept of a semantic web. In 1999, describing his vision of the future, Berners-Lee stated:

"I have a dream for the Web [in which computers] become capable of analyzing all the Web's data—the content, links, and transactions between people and computers. A 'Semantic Web,' which makes this possible, has yet to emerge, but when it does, the everyday mechanisms of commerce, bureaucracy, and our daily lives will be handled by machines talking to machines. The 'intelligent agents' that people have been touting for ages will finally become a reality."

Although the "Semantic Web" envisioned by Berners-Lee and "Web 3.0" are not exactly the same, they are often used interchangeably. The Semantic Web is an extension of the World Wide Web where machines can read and interpret data on the internet. It is essentially the everyday use of artificial intelligence on search engines, social media platforms, and other Web 3.0 sites, enabling them to read, learn, and understand user data and automatically respond accordingly. Smart search engines will be able to understand your search queries far more precisely than they do today, generating results that could save you countless hours of manual work—for example, delivering tailored vacation plans.

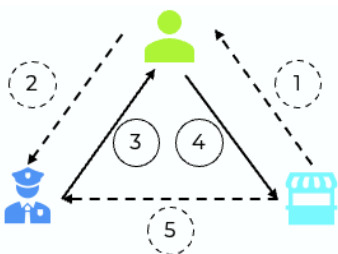
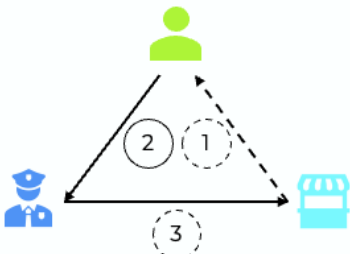
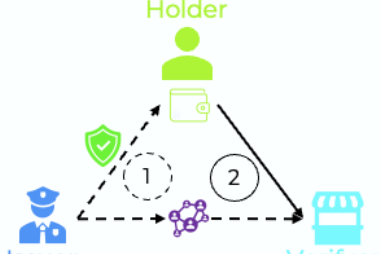
Tim Berners-Lee himself suggested that the Semantic Web would be part of Web 3.0, stating that it was just one element of the Web 3.0 design, not the same thing or a competing entity. In other words, the next generation of the internet will **combine machine-learning-based AI (the Semantic Web) with blockchain technology and other cutting-edge technologies**. Web 3.0 will be the term used to encapsulate this generation.

## 2.2 Decentralization of digital identity template: Simplicity, Security, Sovereignty, Sobriety

### 2.2.1 Identity schema

The 3 identity schemas always involve User/Citizen, Identity Providers/Issuer, and Service Providers/Verifiers:

- User: Natural or legal person (generally prospect, customer, supplier or partner) wishing to access a set of services, while limiting the risk of fraud (in particular identity theft)
- Issuer: Operator guaranteeing the user's identity to the service provider. It ensures the veracity of the attributes presented by the user (e.g. pivot identity, login and password, home) and confirms them with the service provider
- Verifiers: Public or private actor that must authenticate the user through a trusted third party, to allow him or her to access its services

Physical	Centralized digital	Decentralized with wallet
		
<ol style="list-style-type: none"> <li>1. Request for proof</li> <li>2. Transfer of the application</li> <li>3. Receipt of paper receipt</li> <li>4. Paper Voucher Transfer</li> <li>5. Supporting verification</li> </ol>	<ol style="list-style-type: none"> <li>1. Request for proof</li> <li>2. Transfer of the application</li> <li>3. Receipt of paper receipt</li> <li>4. Paper Voucher Transfer</li> <li>5. Supporting verification</li> </ol>	<ol style="list-style-type: none"> <li>1. Issuance of a <b>certified attribute</b> after identity verification, storage in the user's <b>wallet</b>, and proof (hash) recorded on a <b>ledger</b></li> <li>2. User consent to share attributes with the end service, which verifies on the ledger independently of the issuer</li> </ol>
<ul style="list-style-type: none"> <li>• Travel</li> <li>• Paper Procedures</li> <li>• Mailings</li> </ul> <p>Risks: delays &amp; oversights</p>	<ul style="list-style-type: none"> <li>• Less travel, paper, courier</li> <li>• Centralization of access to personal data</li> </ul> <p>Risks: security and citizen sovereignty</p>	<ul style="list-style-type: none"> <li>• Less forgery, duplication or theft of certificates, unnecessary duplication</li> <li>• Fine management of consent see Null disclosure evidence</li> <li>• Transmitter isn't central</li> </ul>

The arrows represent steps in the authentication process (not data flows).

To sum up:

- a. Physical identity was necessary in paper processes, physical appointments, with all the risks of delays, or errors, or forgetfulness that this entails. The first step of the authentication request which could be numbered zero, is not displayed for more readability.
- b. The digitization of services has accelerated the digitization of our identity, consisting of a set of attributes, identifiers, and credentials captured in electronic format, and credited by a government or commercial authority acting as a trusted third party. In response to this multiplication of identity elements, actors federate them with risks on:
  - confidentiality regarding commercial services (e.g. resale of customer data, leakage of data from an insecure system)
  - citizen sovereignty, if a country is hacked or takes an authoritarian turn (today warrants to access data may be required, but through the judiciary, not only with the means of the executive)

Centralized digital identity has made identification and authentication process more fluid but remains unimproved on the rest of the user journeys, and risks remain on the confidentiality and individual sovereignty of data.

- c. Decentralized identity digitizes the attributes extracted from the data of organizations issuing certificates, which certify (sign) them. These certified attributes are kept in the holder's portfolio, which can be used sovereignly with one click to access new services.

With a decentralized identity, the user is the only one who can share his data, which is why he is called "Holder". It even has the possibility of proving information without revealing the underlying certified information. For example, it is possible to prove:

- his or her majority without giving his or her date of birth or nationality
- the possession of a valid health pass without revealing whether it is thanks to a test or a vaccine
- prove your level of education without giving the graduate school or the date of graduation

Decentralized identity is often associated with sovereign identity (SSI), which goes further by allowing the bearer to be the only one to store their data. It involves 2 key elements in the architecture:

- The user's "wallet": a digital element (application or physical storage space) that holds the private keys to control the digital identities stored there.

## The future of digital identity: Standards, Features, Opportunities, Use Cases

- Verifiable credentials, which are inviolable claims that can be verified through cryptography, including the signature of the authority that issued it.

Historical models of identity management put identity providers at the center, **decentralized ones put the user at the center**. Upstream, the issuer signs the attributes. Downstream, the final service verifies the signatures.

### 2.2.2 Key Standards






These standards ensure trustless architecture, privacy-by-design, and global interoperability for identity models.

- W3C DID Core & VC Data Model: foundational for decentralized ID and credential portability.
- ISO/IEC 29100: privacy framework, ensuring user control.
- DIF & Aries RFC 0281: Rich schemas enabling semantic interoperability.

## 2.3 Compliance with a new ecosystem of trust based on EBSI

### 2.3.1 Key principles checklist

EBSI is designed as a market-friendly distributed blockchain ecosystem based on open standards and a transparent governance model. The EBP has approved five key principles.

				
Public Good	Governance	Harmonization	Open Source	EU Values & regulatory framework
EBSI's administration must be in the public good, and it is responsible for limiting its usage to public and private services that provide a net public good to the citizens of the Member States as a whole	The EBSI governance system shall ensure that decisions are reached through building consensus among stakeholders	EBSI governance should encourage and maintain the harmonization of technical requirements and architecture to prevent the proliferation of protocols supported or conflicting architectural assumptions.	Codebase for all EBSI services should be open source to allow maximal auditing, security, and healthy competition between service providers, vendors, and private sector concerns building on top of the infrastructure.	EBSI must not only comply with, but model compliance with the GDPR's current interpretation and ongoing refinement, align with eIDAS and other regulations

### 2.3.2 Interoperability

Requested by Europe and a guarantee of new markets, interoperability requires an informed choice of standards to follow. Which?

Type	Description
<b>Legal</b>	Ensure that organizations operating in different legal, policy and policy frameworks can work together. In concrete terms, this means (at the very least) aligning the "foundations" with the GDPR and eIDAS principles.
<b>Organizational</b>	Ensure that relevant business processes and information exchanges (including meeting the requirements of the user community) are aligned and executed in the same manner. In concrete terms, this means "instantiating" the functioning of the courses: business functions and technical flows (for example W3C).
<b>Semantics</b>	Ensure that the format and precise meaning of the data and information exchanged are preserved and understood throughout the exchanges between the parties, in other words "what is sent is what is understood". In concrete terms, this means, for example, being clear about how identification/authentication can be done correctly, how VCs and VPs must be precisely constructed so that parties can deal with them in a predictable way, such as DIF/W3C standards



### Technique

Ensure that applications and infrastructures connecting systems and services are all identified and understood in the same way (this includes interface specifications, interconnection services, data integration services, data presentation and exchange, and secure communication protocols).

In concrete terms, this means being clear about which components/services need to be available to have a compliant implementation and how these need to interact correctly.

Interoperability will be key to facilitate network effect.

### 2.3.3 Key Standards

These standards guarantee adherence to pan-European decentralized governance, auditability, and public good usage:

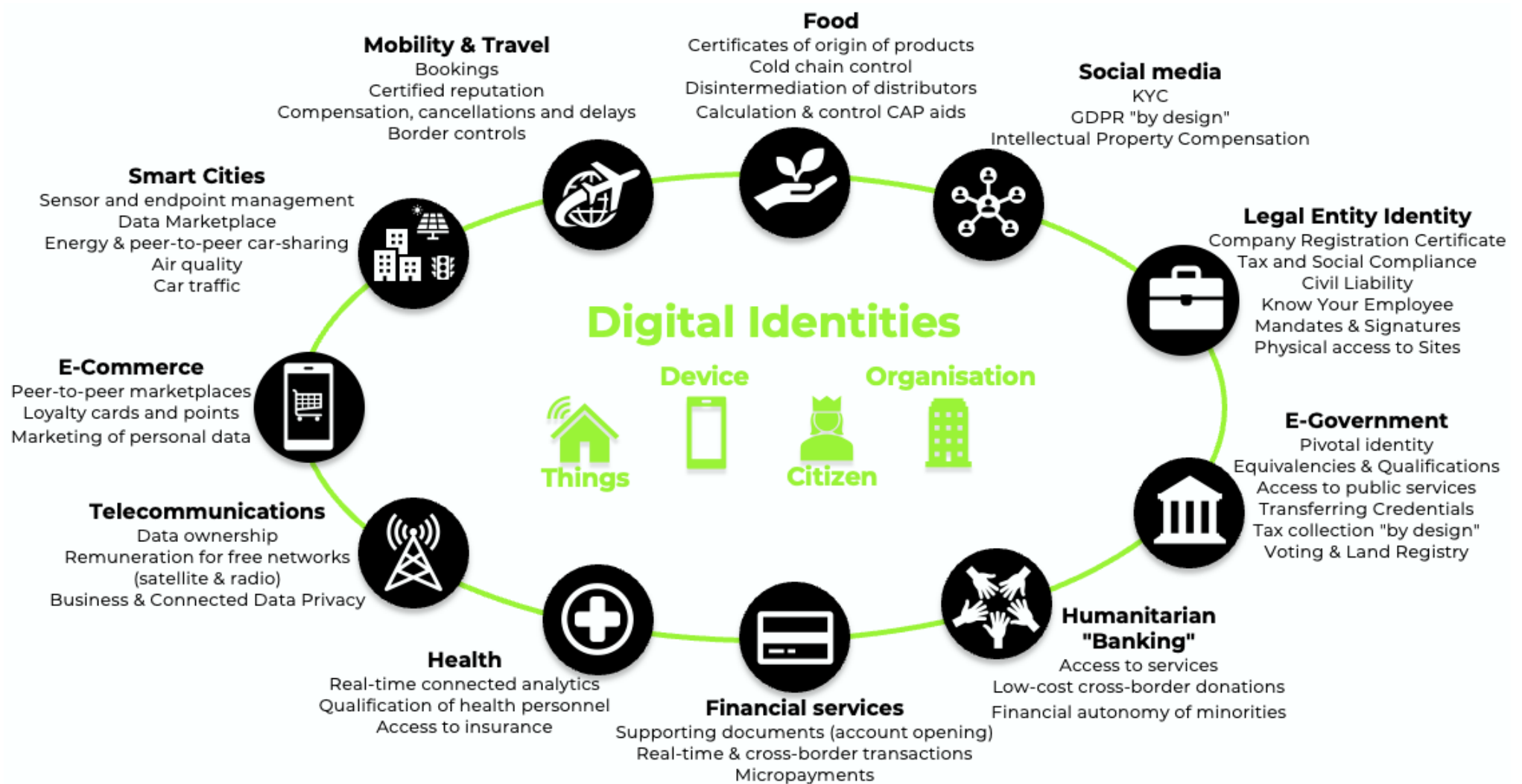
- ETSI EN 319 401 and ENISA framework: for trust service provider and cybersecurity compliance.
- CEN/CLC JTC 19 & EBSI API standards: ensure technical interoperability.

## 2.4 OUR Digital Identities go beyond the Pivot Identity

Industries often talk about the digital twin, but this concept is also valid for citizens: pivotal identity or simple authentication, certificates or tickets for shows or transport, skills or experience. So we should rather talk about OUR digital identities in the plural.

eIDAS aims to make the Wallet our **digital administrative twin**. By extension, eIDAS anticipates the management of the identity of legal entities for B2B uses.

Various industries use Digital Identities for Devices, Organizations, and Citizens. A Digital Wallet could significantly transform each industry by enhancing security, accessibility, and efficiency. Below is an industry-wise breakdown:



#### 2.4.1 Mobility & Travel

Digital wallets could store boarding passes, travel documents (passports, visas), and vaccination certificates, allowing seamless check-ins and cross-border travel.

Secure authentication for car rentals, ride-sharing, and public transport using biometric verification.

Standards: ICAO Doc 9303, ISO/IEC 18013-5: for travel document integration and mobile licenses.

#### 2.4.2 Food Industry

Digital wallets could securely store certificates of origin and traceability for food items, ensuring authenticity and compliance with regulatory standards.

Farmers and suppliers can digitally sign smart contracts, ensuring transparent and automated transactions.

Standards: ISO 22000 & Blockchain provenance: ensures traceability, authenticity.

#### 2.4.3 Social Media

Secure self-sovereign identity (SSI) within digital wallets can help users control their personal data and prevent identity theft.

Intellectual property protection through digital signatures or NFT-based content ownership.

Standards: ISO/IEC 29100 & GDPR ZKP methods: for data privacy and user control.

#### 2.4.4 Legal Entity Identity

Digital wallets could enable instant identity verification for businesses, ensuring compliance with Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations.

Secure, verifiable storage of business licenses, tax documents, and legal contracts.

Standards: ISO 17442 (LEI), AMLD standards, eIDAS for legal entity verification.

#### 2.4.5 E-Government

Citizens could store digital IDs, social security numbers, and tax records securely in their digital wallets.

Digital voting systems leveraging biometric authentication could prevent election fraud.

The future of digital identity: Standards, Features, Opportunities, Use Cases  
Standards: eIDAS 910/2014, OIDC, SAML via OASIS: for secure authentication and credential federation.

#### 2.4.6 Humanitarian Banking

Digital wallets can facilitate direct aid distribution in disaster relief areas by securely storing financial assistance vouchers.

Enables refugees and displaced individuals to access financial services without traditional documentation.

Standards: FATF KYC, W3C VC+ZKP: ensure aid compliance with minimal exposure.

#### 2.4.7 Financial Services

Users can store and manage digital bank accounts, insurance policies, and investment portfolios securely.

Digital wallets enable instant cross-border payments, decentralized finance (DeFi) access, and micro-payments.

Standards: ISO 20022, ETSI TS 119 461: for transaction and identity trust.

#### 2.4.8 Health Industry

Patients can store medical records, prescriptions, and vaccination certificates securely for seamless healthcare access.

AI-driven health monitoring tools could link real-time connected analytics to patient profiles for improved care.

Standards: ISO/HL7 FHIR, EN 17269: for cross-border, privacy-preserving health data.

#### 2.4.9 Telecommunications

Digital wallets can store eSIM profiles for seamless carrier switching.

Secure authentication for business communications and remote work access.

Standards: ETSI GS NFV, GSMA eSIM: for device identity and service access.

#### 2.4.10 E-Commerce

Users can store loyalty points, digital receipts, and payment credentials in one place for a seamless shopping experience.

Enhanced fraud prevention with biometrics and blockchain-based verification.

Standards: ISO/IEC 27001 + OAuth2/OpenID: for secure payment and privacy.

#### 2.4.11 Smart Cities

Digital wallets can enable access to public services, energy distribution tracking, and digital IDs for residents.

Facilitate secure and automated parking payments, traffic management, and environmental data access.

Standards:

- ISO/IEC 30182 (smart city concept model)
- W3C DID: to align identity use with IoT & civic access.

#### 2.4.12 Industry uses cases and standards mapping

Industry uses cases	Relevant Standards
Mobility & Travel	ICAO Doc 9303 ISO/IEC 18013-5
Food Industry	ISO 22000
Social Media	ISO/IEC 29100 GDPR ZKP methods
Legal Entity Identity	ISO 17442 (LEI) AMLD standards eIDAS for legal entity verification.
E-Government	eIDAS 910/2014 OIDC SAML via OASIS
Humanitarian Banking	FATF KYC W3C VC ZKP
Financial Services	ISO 20022 ETSI TS 119 461
Health Industry	ISO/HL7 FHIR EN 17269
Telecommunications	ETSI GS NFV GSMA eSIM
E-Commerce	ISO/IEC 27001 OAuth2/OpenID
Smart Cities	ISO/IEC 30182 (smart city concept model) W3C DID:

#### 2.5 Compliance with a new ecosystem of trust based on EUDIW

The European Digital Identity Wallet is an initiative to develop a secure and interoperable digital identity wallet that allows EU citizens, residents, and businesses to securely store and share identity-related information, such as electronic identification (eID), certificates, and credentials, for both public and private sector services.



## The future of digital identity: Standards, Features, Opportunities, Use Cases

The EUDIW is a key component of the eIDAS 2.0 regulation, aiming to enhance digital identity adoption across Europe by ensuring privacy, security, and interoperability while enabling seamless authentication and digital transactions.

The EUDIW ecosystem will be structured around 3 actors (described on § 2.2).

### 2.5.1 What is a citizen wallet?

In general, the wallet covers the functions of a digital safe, identity federator, password manager, etc. It is an essential building block in the rationalization of:

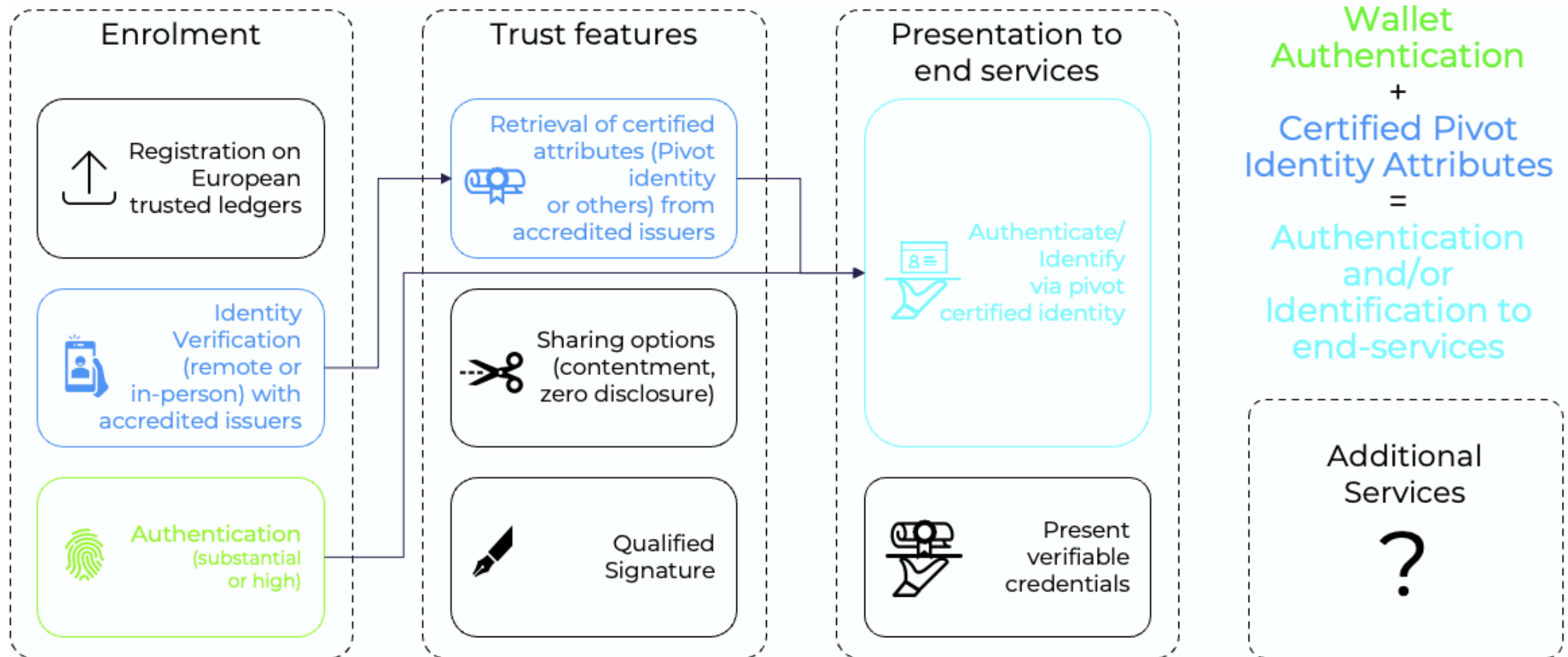
- Requests from issuers, who can value a dormant asset by feeding this new chain of trust,
- Final Service Audits.

The classic certificates (of identity, address, income, insurance) which are documents, which often require manual verifications on the side of the end services, are replaced by attributes signed by their issuers. Among the advantages: Data Minimization and Structured Data (rather than an OCR that extracts data from a pdf) standardize exchanges and indirectly make the chain of trust more sober (hosting and computing capacity).

Some points of focus:

- Terminology: the business talks about PID for Personal Identification Data, the IS also talks about VID for Verifiable ID, which is a Verifiable Credential standard,
- Qualified signature query: currently does not exist in a mobile version, only via remote server
- Standards: eIDAS 2.0, W3C VC, ISO/IEC 23220: foundation for wallet architecture.

We could define 3 macro features that will transform Authentication & Identification:



## 2.5.2 Enrolment: Establishing a Trusted Digital Identity

Key functionalities:

- Registration on European trusted ledgers: Ensures compliance with eIDAS 2.0 and enhances trust.
- Identity Verification (remote or in-person) with accredited issuers: Allows users to establish their digital identity securely, reducing fraud risks.
- Authentication (substantial or high): Ensures a high level of security from the start, setting the foundation for reliable digital interactions.

Market Transformation Impact:

- Standardizes identity verification across the EU, reducing the reliance on proprietary login systems.
- Increases user autonomy over their own identity, limiting the power of centralized identity providers like Google or Facebook.
- Strengthens cross-border interoperability and trust in digital transactions.

Standards:

- ETSI TS 119 461
- ISO/IEC 29115

## 2.5.3 Trust Features: Enabling Secure Data Sharing & Transactions

Key functionalities:

- Retrieval of certified attributes (Pivot identity or others) from accredited issuers: Ensures users can prove their identity without constant re-verification.
- Sharing options (consent management, zero disclosure): Users can control what they share, enhancing privacy.
- Qualified Signature: Allows users to sign legally binding documents using their verified identity.

Market Transformation Impact:

- Reduces friction in authentication: Users don't need to enter credentials manually every time.
- Enhances privacy: Zero-knowledge proofs (ZKPs) can validate identity without exposing unnecessary data.
- Boosts legal compliance: Supports GDPR and eIDAS, making digital signatures legally equivalent to handwritten ones.
- Expands new use cases: Can power decentralized identity wallets, digital contracts, and trusted KYC solutions.

Standards:

- W3C ZKP
- ISO/IEC 29100 for privacy
- ETSI TS 119 432 for signatures

## 2.5.4 Presentation to End Services: Seamless & Secure Authentication

Key functionalities:

- Authenticate / Identify via Pivot certified identity: Enables instant, strong authentication without passwords.
- Present certified attributes: Users can selectively share identity attributes (e.g., age verification, professional credentials).

Market Transformation Impact:

- Replaces passwords: Moves towards passwordless authentication, reducing phishing risks.
- Streamlines onboarding & access management: No need for businesses to store user credentials.
- Improves user experience: Authentication becomes faster, smoother, and more secure.
- Overall Market Disruption & Key Benefits

Standards:

- DIF Presentation Exchange 2.0
- OIDF Self-Issued OP: for verified credential use.

## 2.5.5 Key Benefits

<b>Decentralization &amp; User Control:</b>	<b>Security &amp; Compliance:</b>	<b>Business &amp; Government Adoption:</b>	<b>Expansion of Digital Wallet Ecosystem:</b>
Users manage their identity, shifting control away from centralized identity providers (e.g., Google, Microsoft).	Higher assurance levels for authentication (aligned with eIDAS 2.0, GDPR, and AML regulations).	Enables seamless B2C, B2B, and B2G digital interactions (banking, e-government, healthcare, etc.).	Interoperable wallets allow users to authenticate across multiple services with one verified identity.

Standards:

- Wallet ARF, EBSI Trust Model: ensure verified trust loops and ledger anchoring

## 2.5.6 Compliance Checklist for Digital Identity Wallets (EUDIW)

This section provides a structured overview of core requirements for compliance with EUDIW and eIDAS 2.0. Each item in the checklist aligns with a specific technical or regulatory standard and can be used as a verification tool during solution design, development, or audit phases.

Item	Requirement	Standard/Reference
Identity Proofing	Substantial/High assurance levels	ETSI TS 119 461, eIDAS CIR 2015/1502
Verifiable Credentials (VC) format	Must support W3C VC Data Model	W3C VC 1.1
Qualified Electronic Signatures	Support QSCD mechanisms	CEN EN 419 241-1, ETSI EN 319 401
Interoperability	Use standard protocols for VC exchange	EBSI VC Framework, ISO/IEC 18013-5
Privacy & Consent	Compliance with GDPR and selective disclosure	ISO/IEC 29100, ZKP, W3C VC ZCAP-LD

### 2.5.7 Compliance Guidelines

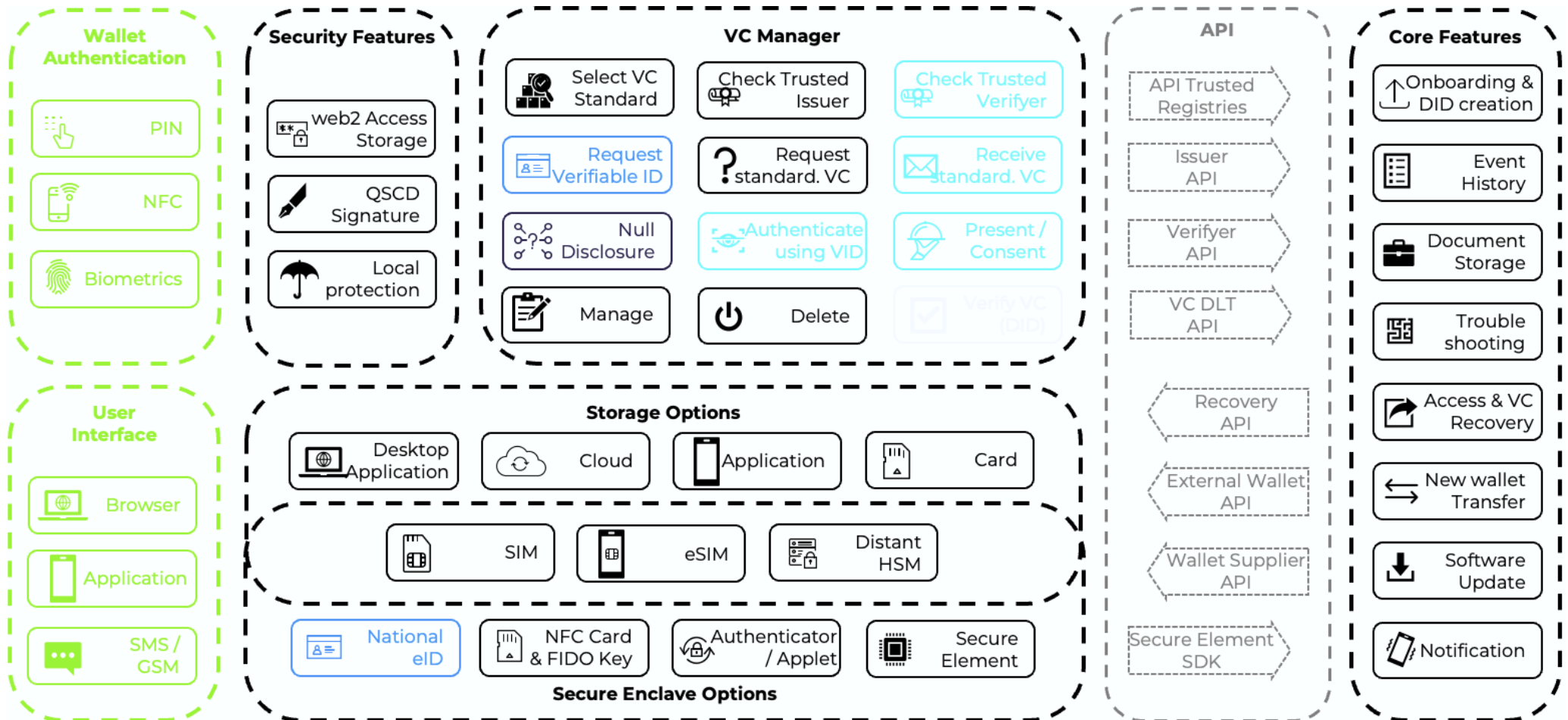
This section outlines implementation-focused recommendations to help stakeholders ensure their digital identity solution meets regulatory, technical, and ethical best practices. These guidelines are intended to complement the checklist by supporting long-term compliance and operational excellence.

- Trust Framework Integration: Ensure participation in or alignment with an EU-recognized Trust Framework (e.g., EBSI).
- Data Minimization: Follow ISO/IEC 29101 principles to only collect what is necessary.
- Selective Disclosure: Utilize ZKPs or BBS+ Signatures to minimize data exposure.
- Security Protocols: Adopt ETSI EN 319 401 and ISO/IEC 27001 for TSP compliance and ISMS security.
- Standard API Use: Integrate with EBSI and OIDF protocols for wallet communication.

## 2.6 Envisioned wallet features Templates

Wallet could cover a huge scope of features:

# The future of digital identity: Standards, Features, Opportunities, Use Cases





### 2.6.1 Wallet Authentication

- PIN: Traditional security mechanism requiring a user-defined code.
- NFC: Contactless authentication using an NFC-enabled device or smart card.
- Biometrics: Fingerprint, facial recognition, or other biometric authentication methods.

#### Functional Impact:

- Provides multi-factor authentication (MFA) for enhanced security.
- Supports user-friendly, passwordless access to the wallet.

#### Standards:

- FIDO2, ISO/IEC 18013-5: strong MFA and biometric mobile ID.

### 2.6.2 User Interface Options

- Browser: Web-based access to the wallet and its functions.
- Application: Dedicated mobile or desktop apps for managing credentials.
- National GSM: Possibly referring to SIM-based authentication for mobile security.

#### Functional Impact:

- Ensures cross-platform compatibility (web, mobile, SIM-based).
- Enhances usability by offering multiple access channels.

#### Standards:

- WCAG 2.1 & ISO 9241: usability and accessibility.

### 2.6.3 Security Features

- Web3 Access Storage: Secure Web3-based credential and identity storage.
- QSCD Signature: Qualified Signature Creation Device (QSCD) for eIDAS-compliant digital signatures.
- Local Protection: On-device security mechanisms to protect stored credentials.

#### Functional Impact:

- Ensures compliance with eIDAS, GDPR, and AML regulations.
- Strengthens identity security with tamper-proof digital signatures.

#### Standards:

- ETSI EN 319 401
- ISO/IEC 27001
- QSCD

#### 2.6.4 VC Manager (Verifiable Credentials Lifecycle Management)

- Select VC Standard: Choose between different Verifiable Credentials (VC) standards.
- Request Verifiable ID: Obtain a digital identity credential from a trusted issuer.
- Request Endorsed VC: Ask for additional endorsements or attestations for a VC.
- Check Trusted Issuer: Validate that a credential was issued by an accredited entity.
- Request Verified VC: Obtain a VC that has undergone a validation process.
- Request Standard VC: Fetch a standard, non-verified VC.
- Manage & Delete VC: User-controlled credential management.
- Present & Consent: Allow users to share credentials based on consent.

##### Functional Impact:

- Ensures trustworthiness of identity credentials.
- Empowers users with full control over their digital identity.
- Enables selective disclosure & privacy-preserving authentication (e.g., Zero-Knowledge Proofs).

##### Standards:

- W3C VC
- DIF Credential Manifest

#### 2.6.5 Storage Options

- Desktop Application: On-device storage for PCs or workstations.
- Cloud: Remote storage accessible anywhere.
- Application: Mobile or web application-based storage.
- Card: Smart card storage (e.g., NFC-based identity cards).

##### Functional Impact:

- Flexible storage architecture allows users to select security vs. accessibility trade-offs.
- Supports decentralized identity models with cloud and on-device storage.

##### Standards:

- ISO/IEC 27018 (cloud privacy)
- ISO/IEC 24760 (identity management)

#### 2.6.6 Secure Enclave Options

- National HSM: Hardware Security Module (HSM) for national identity protection.

## The future of digital identity: Standards, Features, Opportunities, Use Cases

- NFC Card & Micro SD: Hardware-based storage solutions for credentials.
- Authentication & NFC: Combining contactless authentication with secure storage.
- Distant HSM: Remote hardware security modules for cloud-based solutions.

### Functional Impact:

- Enables tamper-resistant credential storage.
- Supports offline and online identity verification with NFC & HSM.
- Reduces dependency on software-based security, which can be more vulnerable.

### Standards:

- ISO/IEC 15408 (Common Criteria)
- EN 419 241

### 2.6.7 API Features

- Issuer API: Allows credential issuance by trusted authorities.
- Verifier API: Enables authentication and validation of credentials.
- Trust Registry API: Accesses decentralized registries to verify credential authenticity.
- Document Storage: Stores supporting documents linked to identities.

### Functional Impact:

- Enables seamless integration into third-party applications.
- Supports decentralized identity ecosystems via registries and APIs.

### Standards:

- EBSI APIs
- OIDF standards

### 2.6.8 Core Features

- Onboarding: User identity verification & wallet setup.
- Event Tracking: Logs key identity-related events for compliance.
- Secure Document Storage: Ensures encrypted, auditable identity records.
- Trustee Identity Storage: Secure custodianship of user credentials.
- New wallet Transfer: Enables a citizen to securely migrate their identity data to a new wallet while decommissioning the previous one.
  - Secure Export & Import of Identity Data: Allows users to transfer Verifiable Credentials (VCs), authentication keys, and settings to a new wallet.
  - Binding to a New Secure Element (HSM, NFC, SIM, or Cloud Vault): Ensures the new wallet is bound to a trusted environment before transfer.

## The future of digital identity: Standards, Features, Opportunities, Use Cases

- Wallet Decommissioning Protocol: Ensures the old wallet is revoked, preventing unauthorized access.
  - Recovery Authentication: Requires multi-factor authentication (MFA) before authorizing the migration (e.g., PIN, biometrics, secure backup key).
  - Revalidation with Trust Registries: The new wallet must revalidate identity and credentials with issuers and verifiers.
- Software Update: Ensures software compliance & integrity.
- Authentication: Strong identity verification mechanisms.
- Notification: Enables real-time alerts and updates related to digital identity events, credential usage, and security actions.
  - Credential Expiry Alerts: Notifies users when a Verifiable Credential (VC) is about to expire or requires renewal.
  - Transaction & Authentication Logs: Sends security alerts when the wallet is used for authentication, identity verification, or document signing.
  - Unauthorized Access Warnings: Detects and informs users of suspicious login attempts or credential access.
  - Policy Updates & Regulatory Compliance Alerts: Ensures users stay informed about changes in identity verification policies or compliance requirements.
  - Consent Requests & Approvals: Provides real-time notifications for consent management, allowing users to approve or deny data-sharing requests.
  - Cross-Wallet Notifications: In multi-wallet ecosystems, alerts users about pending credential transfers, issuer updates, or new identity verification requirements.

### Functional Impact:

- Provides full lifecycle management for digital identities.
- Facilitates compliance with international security standards.
- Solves device loss or theft scenarios, allowing users to recover their digital identity on a new wallet.
- Ensures data continuity and compliance with privacy regulations (e.g., GDPR).
- Enhances user control & transparency by keeping them informed about wallet activities.
- Improves security by detecting and preventing unauthorized actions in real time.

### Standards:

- ETSI TR 119 460 (logs)
- ISO/IEC 27035 (incident mgmt.)
- ISO 14641 (archiving)

## 2.6.9 Wallet features and standards mapping

Wallet Features	Relevant Standards
Wallet Authentication	FIDO2 ISO/IEC 18013-5
User Interface Options	WCAG 2.1 ISO 9241
Security Features	ETSI EN 319 401 ISO/IEC 27001 QSCD
VC Manager	W3C VC DIF Credential Manifest
Storage Options	ISO/IEC 27018 (cloud privacy) ISO/IEC 24760 (identity management)
Secure Enclave Options	ISO/IEC 15408 (Common Criteria) EN 419 241
API Features	EBSI APIs OIDF standards
Core Features	ETSI TR 119 460 (logs) ISO/IEC 27035 (incident mgmt.) ISO 14641 (archiving)

## 2.7 3 Secure Storage Options to help stakeholders choice

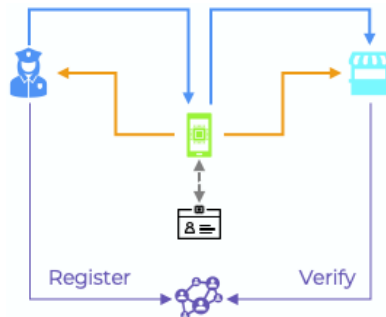
We need to separate two major storage needs: the storage of cryptographic keys, which secure the rest of the data, from the storage of that data itself, such as Verifiable Credentials (VCs). A Secure Element (SE) is a Secure Operating Systems (ROE firmware) running on a secure tamper-resistant microcontroller. The following chapter describe the options to store the cryptographic keys securing all the data. Store these keys on our personal eID is a discarded option for 3 reasons:

- It can be lost, and given that the time to reissue a new identity card can take several months, it seems impossible to leave a citizen without access to their wallet data,
- This type of physical standard is used for decades through massive public investments, while the capabilities to breach it evolve constantly,
- It can be useful for wallet onboarding. However, as of now, it is impossible for it to serve as a Secure Element (at least for the French eID, where the PID is hardcoded, lacking the memory needed to store certificates).

Then there are 3 options:

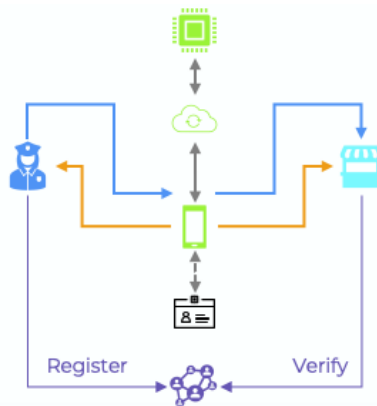
- Everything on your device (secure element or nearby via NFC, SIM, or eID cardCNle),
- Remote storage for the actual Secure Element, with the CNle used only for authentication,
  - All storage in the back-end.

## Fully on the device with authentication via eID



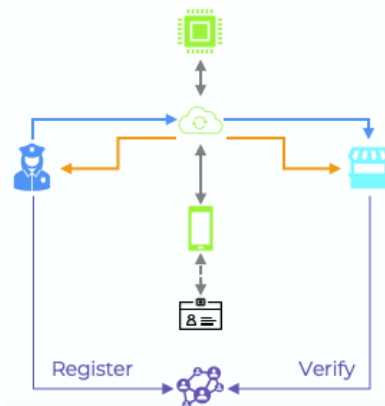
- Dependence on terminal providers and their Secure Element
- Dependence on eID (loss, manufacturing delay)
- Higher security requirements for the application
- Offline presentations (PID, EAA, QEEA) facilitated
- Massive attack (denial of service) unlikely (limited to the OS)
- Optimal processing time

## Remote with authentication via eID and interfaces through the device

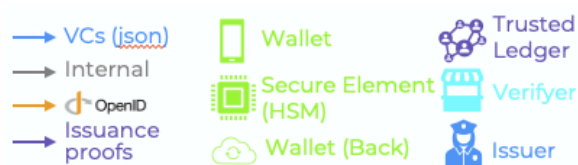


- Centralized + Single Point of Failure
- Degraded offline presentations (PID, EAA, QEEA)
- Potential weakness in terminal security
- Independence from terminal providers
- Backup & Recovery
- Control and robustness of the Secure Element (/ HSM)

## Remote (storage & interfaces)



- Centralized + Single Point of Failure
- Offline presentations (PID, EAA, QEEA) impossible
- Independence from terminal providers
- Backup & Recovery
- Control & robustness of the Secure Element (/ HSM)
- Full control over data flows (Certifier & Verifier) and simplified interfacing



To ensure secure device recovery, continuity, and compatibility with trust services, the applicable standards are:

- ISO/IEC 24760-3: Identity data lifecycle.
- ETSI TS 119 432 + EBSI secure storage modules.



### 3 Implementation Steps and Compliance Checklists for Stakeholders

This chapter provides a structured path to help organizations involved in the European Digital Identity Wallet (EUDI Wallet) ecosystem implement robust security, privacy, and governance controls. Each section aligns with a key step in the lifecycle of a secure digital identity system.

Whether you are a wallet issuer, verifier, governance authority, or technology provider, these steps are designed to help you assess your readiness, identify compliance gaps, and ensure that each decision is grounded in applicable standards and regulations. Each sub-section includes a targeted checklist to validate implementation progress across operational, legal, and technical domains.

By following these steps, stakeholders can ensure their systems are trustworthy, interoperable, and aligned with both EU regulatory expectations and international best practices.

#### 3.1 Identify Your Role and Scope within the EUDI Wallet Ecosystem

This step helps each organization determine their role(s) in the digital identity value chain and define the perimeter of their responsibilities.

Question	Requirement Type	Reference Type	Applicable Standards & Regulations
Have you identified whether your organization acts as an Issuer, Holder, Verifier, or Governance body within the EUDI Wallet ecosystem?	Governance Role Definition	Guideline	EUDIW Architecture & Reference Framework
Have you defined the legal and operational scope for your EUDI Wallet-related activities?	Scope Determination	Regulation	GDPR, eIDAS 2.0, ISO/IEC 27001 Clause 4.3
Have you documented all cross-border operations or data transfers within the scope?	Jurisdiction Management	Regulation	GDPR – Chapter V
Is the scope approved and regularly reviewed by governance leadership?	Governance Oversight	Standard	ISO/IEC 27001 – Clause 5.1

#### 3.2 Define Information Security Objectives and Responsibilities

This step ensures your identity-related operations are framed by clear governance and measurable objectives.

Question	Requirement Type	Reference Type	Applicable Standards & Regulations
----------	------------------	----------------	------------------------------------

## The future of digital identity: Standards, Features, Opportunities, Use Cases

Have you formally assigned security responsibilities across relevant roles (CISO, DPO, Product Lead, etc.)?	Role Management	Standard	ISO/IEC 27001 - Clause 5.3
Are information security objectives clearly defined, measurable, and aligned with regulatory requirements?	Governance Objectives	Regulation	GDPR, ISO/IEC 27001 - Clause 6.2
Is there a dedicated Data Protection Officer (DPO), and is the role clearly defined?	Data Protection Role	Regulation	GDPR - Article 37
Are responsibilities for identity data classified and traceable across roles and systems?	Accountability Mapping	Guideline	ISO/IEC 27701

### 3.3 Conduct a Risk Assessment

This step helps evaluate security and privacy risks relevant to digital identity operations and systems.

Question	Requirement Type	Reference Type	Applicable Standards & Regulations
Have you conducted a comprehensive risk analysis specific to identity data and wallet functionalities?	Risk Assessment	Standard	ISO/IEC 27005, ISO/IEC 27001 - Clause 6.1.2
Are threats related to identity theft, impersonation, or unauthorized access evaluated?	Threat Modeling	Guideline	ENISA Threat Landscape for Digital Identity
Are probability and impact rated for each identified risk?	Risk Rating Framework	Guideline	ISO/IEC 31000
Are risks continuously reviewed following incidents or system changes?	Dynamic Risk Adjustment	Standard	ISO/IEC 27001 - A.16.1.2

### 3.4 Define Data Classification and Lifecycle Policies

This step focuses on organizing personal and sensitive data in structured ways, with controlled retention and disposal.

Question	Requirement Type	Reference Type	Applicable Standards & Regulations
Have you classified personal and sensitive data in accordance with legal obligations?	Data Classification	Regulation	GDPR - Recital 51, ISO/IEC 27001 - Control A.8
Are special categories of personal data (e.g., biometrics) identified and protected accordingly?	Sensitive Data Handling	Regulation	GDPR - Article 9

## The future of digital identity: Standards, Features, Opportunities, Use Cases

Do you define retention periods for each data type?	Data Retention Policy	Standard	ISO/IEC 27001 – A.8.3
Are there policies and mechanisms to guarantee secure deletion of identity-related data?	Secure Data Disposal	Standard	ISO/IEC 27001 – A.11.2.7

### 3.5 Implement Access Control Policies

This step helps ensure identity systems are accessible only to authorized and accountable individuals.

Question	Requirement Type	Reference Type	Applicable Standards & Regulations
Are role-based access controls in place to prevent unauthorized access to identity systems?	Access Management	Standard	ISO/IEC 27001 – A.9
Is strong authentication (e.g., MFA) required for access to sensitive systems?	Identity & Access Control	Standard	NIST 800-63B, ISO/IEC 27001 – A.9.4
Are access logs automatically generated and retained?	Logging & Traceability	Standard	ISO/IEC 27001 – A.12.4
Are default passwords or admin accounts disabled or secured upon deployment?	Secure Configuration	Guideline	OWASP ASVS, ISO/IEC 27001 – A.13.1.1

### 3.6 Ensure Secure Development and Maintenance

This step integrates security by design into the lifecycle of identity platforms.

Question	Requirement Type	Reference Type	Applicable Standards & Regulations
Are developers trained in secure coding practices and identity-specific risks?	Developer Training	Guideline	OWASP, ISO/IEC 27001 – A.7.2
Is a secure SDLC framework followed for EUDI Wallet-related components?	Development Lifecycle	Standard	ISO/IEC 27034, NIST SSDF
Are changes to wallet systems tracked and documented with rollback mechanisms?	Change Control	Standard	ISO/IEC 27001 – A.12.1
Is penetration testing regularly performed on critical identity features?	Security Testing	Guideline	OWASP, ENISA Guidance for SSI

### 3.7 Address Data Protection and Privacy Compliance

This step supports full alignment with personal data rights and obligations.

Question	Requirement Type	Reference Type	Applicable Standards & Regulations
Is data minimization implemented across all identity features?	Privacy by Design	Regulation	GDPR - Article 25
Are privacy impact assessments conducted for new identity products?	DPIA	Regulation	GDPR - Article 35
Are all consents explicit, granular, and auditable?	Consent Management	Regulation	GDPR - Article 7
Do identity users have transparent access to how their data is processed?	User Transparency	Regulation	GDPR - Articles 12-14

### 3.8 Manage Third-Party and Interoperability Risks

This step ensures external vendors and cross-system exchanges meet trust, security, and interoperability standards.

Question	Requirement Type	Reference Type	Applicable Standards & Regulations
Are all suppliers vetted via a standardized due diligence process?	Supplier Risk	Guideline	ISO/IEC 27036
Do your APIs and wallet components meet EUDI federation specifications?	Interoperability Compliance	Guideline	EUDIW Technical Specifications
Is contract language aligned with data protection and liability obligations?	Legal Safeguards	Regulation	GDPR - Articles 28, 32

### 3.9 Ensure Incident Management and Business Continuity

This step prepares your team to recover and respond to breaches or service interruptions in wallet systems.

Question	Requirement Type	Reference Type	Applicable Standards & Regulations
Is an identity-specific incident response playbook defined and tested?	Incident Response Policy	Standard	ISO/IEC 27035, ENISA Guidelines
Are critical wallet services covered by redundancy or failover plans?	Service Continuity	Standard	ISO/IEC 22301, ISO/IEC 27001 - A.17
Do users receive clear communication in case of data breaches?	Breach Notification	Regulation	GDPR - Article 33

### 3.10 Monitor and Audit Compliance Continuously

This step guarantees ongoing evaluation of policies and systems related to digital identity.

Question	Requirement Type	Reference Type	Applicable Standards & Regulations
Are automated systems in place to flag deviations from policy or expected behavior?	Continuous Monitoring	Standard	ISO/IEC 27001 – A.12.4
Are third-party audits or certification pathways planned or completed?	External Audit	Guideline	eIDAS 2.0 Conformity Assessment, ETSI standards
Are internal audits mapped against both legal and ISO frameworks?	Internal Compliance Review	Standard	ISO/IEC 27001 – Clause 9

### 3.11 Align Product Features with Functional and Legal Expectations

This step helps product teams evaluate each core feature in a digital identity system to ensure compliance with legal, technical, and security standards.

Question	Requirement Type	Reference Type	Applicable Standards & Regulations
Does the wallet support issuance of verifiable credentials in line with the W3C standard?	Credential Issuance	Standard	W3C Verifiable Credentials, eIDAS 2.0
Is credential revocation supported and traceable by both issuers and holders?	Credential Revocation	Guideline	ISO/IEC 23220-3, EUDIW Revocation Mechanisms
Can credentials be presented in a selective disclosure format?	Data Minimization	Regulation	GDPR – Article 5(1)(c), ISO/IEC 27551
Is user consent captured and auditable prior to sharing any credential?	Consent Management	Regulation	GDPR – Article 7, ISO/IEC 29184
Does the wallet provide offline verification of credentials?	Availability & Portability	Guideline	EUDIW Functional Specifications
Are user interface elements accessible for all users, including those with disabilities?	Accessibility Requirements	Regulation	EU Accessibility Act, WCAG 2.1

## The future of digital identity: Standards, Features, Opportunities, Use Cases

Are cryptographic keys stored in secure environments (e.g. secure elements, trusted execution environments)?	Key Management	Standard	ISO/IEC 11770, ETSI TS 119 312
Can users export, import, and back up their wallets securely?	Data Portability	Regulation	GDPR - Article 20, ISO/IEC 29100
Does the wallet log transactions such as issuance, updates, and revocations securely?	Event Logging	Standard	ISO/IEC 27001 - A.12.4, ETSI TS 119 512
Are mechanisms in place to detect and report anomalies in wallet usage?	Threat Detection	Guideline	ISO/IEC 27001 - A.12.6, ENISA Threat Modeling
Is credential status information accessible without compromising user privacy?	Status Querying	Standard	ISO/IEC 18013-5, EUDIW Architecture
Does the wallet restrict use of credentials by purpose and validity?	Usage Control	Regulation	GDPR - Article 5(1)(b), ISO/IEC 29100
Are updates to wallet software signed and verified before installation?	Secure Updates	Standard	ISO/IEC 30111, NIST 800-147
Can users delegate wallet management under secure and revocable conditions?	Delegation & Proxy Access	Guideline	EUDIW Use Cases, ENISA Guidelines
Are audit logs accessible only to authorized roles with separation of duties?	Log Access Control	Standard	ISO/IEC 27001 - A.12.4.2
Is the wallet compatible with multiple credential formats (e.g., mDL, PID, diplomas)?	Interoperability	Guideline	ISO/IEC 18013-7, W3C VC, EUDIW
Can users clearly understand the purpose, issuer, and verifier of each credential presented?	Transparency & UX	Regulation	GDPR - Articles 12-13, UX Guidelines for eIDAS
Are verification processes resistant to replay attacks and cloning?	Security & Anti-Fraud	Standard	ISO/IEC 29115, ETSI TS 119 461
Can credentials be grouped by categories (e.g., health, education) with privacy-friendly defaults?	Data Organization	Guideline	ISO/IEC 29100, Human-Centric Wallet Design
Are onboarding flows for identity creation and wallet activation secure and user-friendly?	Onboarding	Guideline	ENISA UX Guidelines,

## The future of digital identity: Standards, Features, Opportunities, Use Cases

			ISO/IEC 27550
Are credentials easily revocable by the user in case of compromise or theft?	User Revocation Control	Regulation	GDPR – Article 17, ISO/IEC 27555
Are fallback recovery procedures in place without compromising privacy?	Account Recovery	Guideline	EUDIW Best Practices, ISO/IEC 27552
Are biometric authentication methods privacy-preserving and voluntary?	Biometric Use	Regulation	GDPR – Article 9, ISO/IEC 24745
Are privacy settings configurable and understandable for non-technical users?	Privacy Controls	Guideline	ISO/IEC 29100, ISO/IEC 27550
Can users audit what credentials have been shared, with whom, and when?	User Auditing Capability	Regulation	GDPR – Articles 15, 30