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

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 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 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 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.

The last part (this document and §2 and §**Erreur ! Source du renvoi introuvable.**) start 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.

This document serves as the third deliverable in the BlockStand series. It focuses on translating the conceptual and regulatory frameworks presented in Deliverable 1, and the tools and guidelines in Deliverable 2, into concrete use cases. Each scenario is designed to illustrate how standards can be applied to real-world implementations of the European Digital Identity

Wallet (EUDIW), and 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 Business Opportunities

2.1 Digital Services

Existing or recent players could position themselves in the following areas, capitalizing on their know-how and knowledge while integrating the new situation created by the wallet:

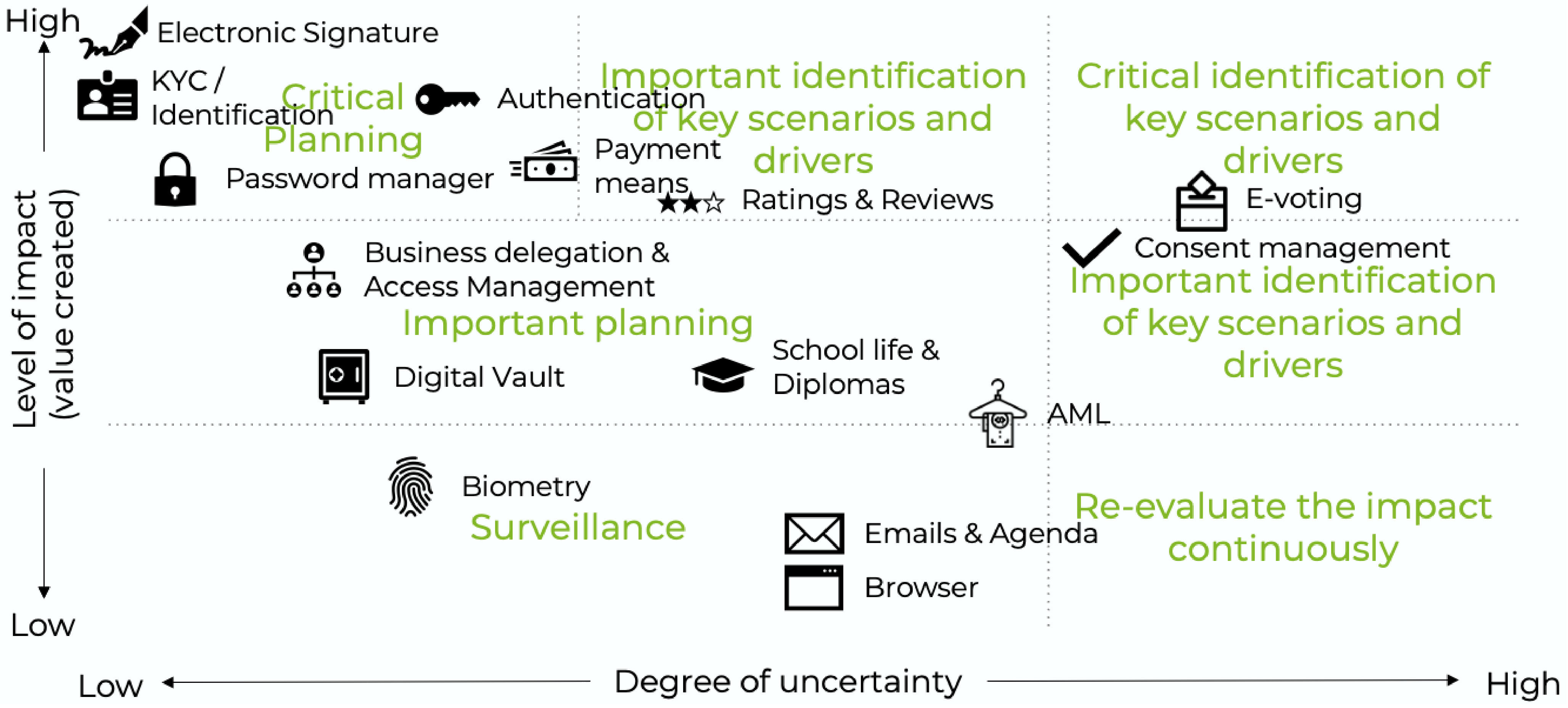
- As a private Wallet provider: alongside other non-sovereign Wallets coexisting in the market – in areas such as:
    - "Substantial" Wallet
    - "Low" Wallet for everyday use cases
    - Sectoral Wallets (Education Wallet, etc.)
    - Professional Wallet
- As an integrator to enable the deployment of white-label professional Wallets (for regulated professions, etc.)
- As a platform operator to:
    - Operate identity HUBs and trusted registries
    - Provide delegated verifier services on behalf of our clients
- As a consulting service provider, offering technical and regulatory support to our clients on this topic.

Finally, a business model (verifier/payer and issuer/paid) must be devised to guarantee ecosystem's sustainability over the long term

2.2 Trusted Digital Products

Thanks to their footprint within trusted digital solutions market and their ability to ensure compliance with various regulations, software providers and industry leaders should be able to redesign their solutions with the goal of enhancing national or individual sovereignty while simplifying and securing B2B, B2C, and B2G use cases:

- Electronic Signature
- KYC/Identification
- Authentication/IAM/SSO
- Password manager
- Payment means
- Rating and Reviews
- E-voting
- Consent management
- Business delegation & Access Management
- Digital Vault
- School life & Diplomas
- AML
- Biometry
- Emails & Agendas
- Browser



An Uncertainty Matrix helps visualize and prioritize industry transformations by mapping potential changes based on their impact (value created, ranging from low/bottom to high/top) and degree of uncertainty (ranging from low/left to high/right), enabling strategic planning, risk assessment, and informed decision-making.

By structuring the matrix this way, it becomes a strategic tool to guide software providers and industry leaders in enhancing digital sovereignty, ensuring compliance, and optimizing solutions for B2B, B2C, and B2G use cases.

The following section outlines also applicable standards for core trusted digital functionalities commonly integrated into EUDI-compatible products and services. Each subsection identifies the most relevant standard(s) and explains their practical purpose.

2.2.1 High Impact & Low Uncertainty (Critical & Strategic Area)

These are well-established and highly valuable digital solutions that provide strong regulatory compliance and security benefits. Their adoption is widespread, making their uncertainty relatively low:

- Electronic Signature:
  - Enables legally binding transactions, crucial for digital contracts and B2B/B2G/B2C interactions.
  - Standards applied to ensure legal validity and trustworthiness of signatures aligned with eIDAS regulation:
    - ETSI EN 319 411-1/-2 – Trust service provider certification for qualified electronic signature issuance.
    - ETSI EN 319 421 – Policy and security requirements for remote signature creation.
- KYC / Identification:
  - Mandatory in finance, healthcare, and government services; essential for fraud prevention.
  - Standards applied to enable harmonized identity verification for onboarding and compliance processes:
    - ETSI TS 119 461 – Identity proofing policy and security requirements.
    - ISO/IEC 29115 – Entity authentication assurance framework.
- Authentication / IAM / SSO:
  - Core to cybersecurity, ensuring secure access management in enterprises and digital services.
  - Standards applied to ensure interoperable and secure identity and access control mechanisms:
    - OIDC (OpenID Connect) – for federated authentication.
    - SAML 2.0 – standard for secure SSO and identity federation.
    - ISO/IEC 24760 – Framework for identity management.
- Password Manager:
  - Increasingly used due to security concerns, but its value is well understood.
  - Standards applied to promote secure storage, usage, and passwordless alternatives:
    - ISO/IEC 27002 – Controls for information security, including credentials management.
    - FIDO2 / WebAuthn – Phasing out of passwords with strong authentication.

2.2.2 High Impact & High Uncertainty (Critical Scenario Identification)

These solutions have the potential to bring significant value but face regulatory, technological, or adoption challenges.

- E-voting:
  - High impact for democracy and digital governance but faces trust, security, and legal challenges.

    - Standards applied to guarantees integrity, anonymity, and verifiability in voting scenarios
        - EN 419 261-1 – Requirements for e-voting systems.
        - W3C VC + ZKP – Anonymous credential-based voting.
- Consent Management:
    - Essential for privacy and data protection (e.g., GDPR, CCPA) but evolving regulatory landscape creates uncertainty.
    - Standards applied to support GDPR compliance through structured consent collection and documentation:
        - ISO/IEC 29184 – Privacy notices and consent.
        - ISO/IEC 27560 – Consent record management.

2.2.3 Moderate Impact & Low Uncertainty (Important Planning Area)

These solutions provide value in niche areas and are well-defined, though their impact is not as high as the previous categories.

- Business Delegation & Access Management:
    - Important for corporate structures and secure workflow delegation.
    - Standards applied to facilitate fine-grained, contextualized role and delegation enforcement:
        - ISO/IEC 29146 – Access control framework.
        - ISO/IEC 22600 – Privilege management infrastructure.
- Digital Vault:
    - Useful for secure document storage and archiving but not as critical as identification or authentication.
    - Standards applied to ensure integrity, retention, and legal reliability of long-term digital storage
        - ISO 14641 – Electronic archiving requirements.
        - ETSI TS 119 511 – Preservation of qualified electronic signatures.

2.2.4 Moderate Impact & Moderate Uncertainty (Key Scenario Identification)

These solutions are useful but require further evaluation regarding their long-term impact and adoption potential.

- Payment Means:
    - Digital payments are well-established, but regulatory frameworks and new technologies (crypto, CBDCs) add complexity.
    - Standards applied to enable secure and interoperable payments integration in wallet contexts:
        - ISO 20022 – Financial messaging interoperability.
        - EMVCo 3DS & PCI-DSS – Secure transaction and card data management.
- Ratings & Reviews:
    - A valuable tool for e-commerce and services, but their integrity and regulatory oversight remain uncertain.

    - Standards applied to ensure transparency, credibility, and auditability of digital feedback.
        - ISO 20488 – Guidelines for online consumer reviews.
- School Life & Diplomas:
    - Digitization of academic records is beneficial but depends on government and institutional adoption.
    - Standards applied to enable trusted learning credential issuance and verification across borders:
        - EDCI & Europass – Credential schema and metadata.
        - W3C Verifiable Credentials – Portable, verifiable academic records.
- AML (Anti-Money Laundering):
    - Critical for compliance in finance but constantly evolving due to regulatory shifts.
    - Standards applied to enable risk-based screening and regulatory alignment:
        - FATF Recommendations – Global AML compliance.
        - ETSI TS 119 461 – Identity verification controls.

2.2.5 Low Impact & Low Uncertainty (Surveillance & Continuous Evaluation Area)

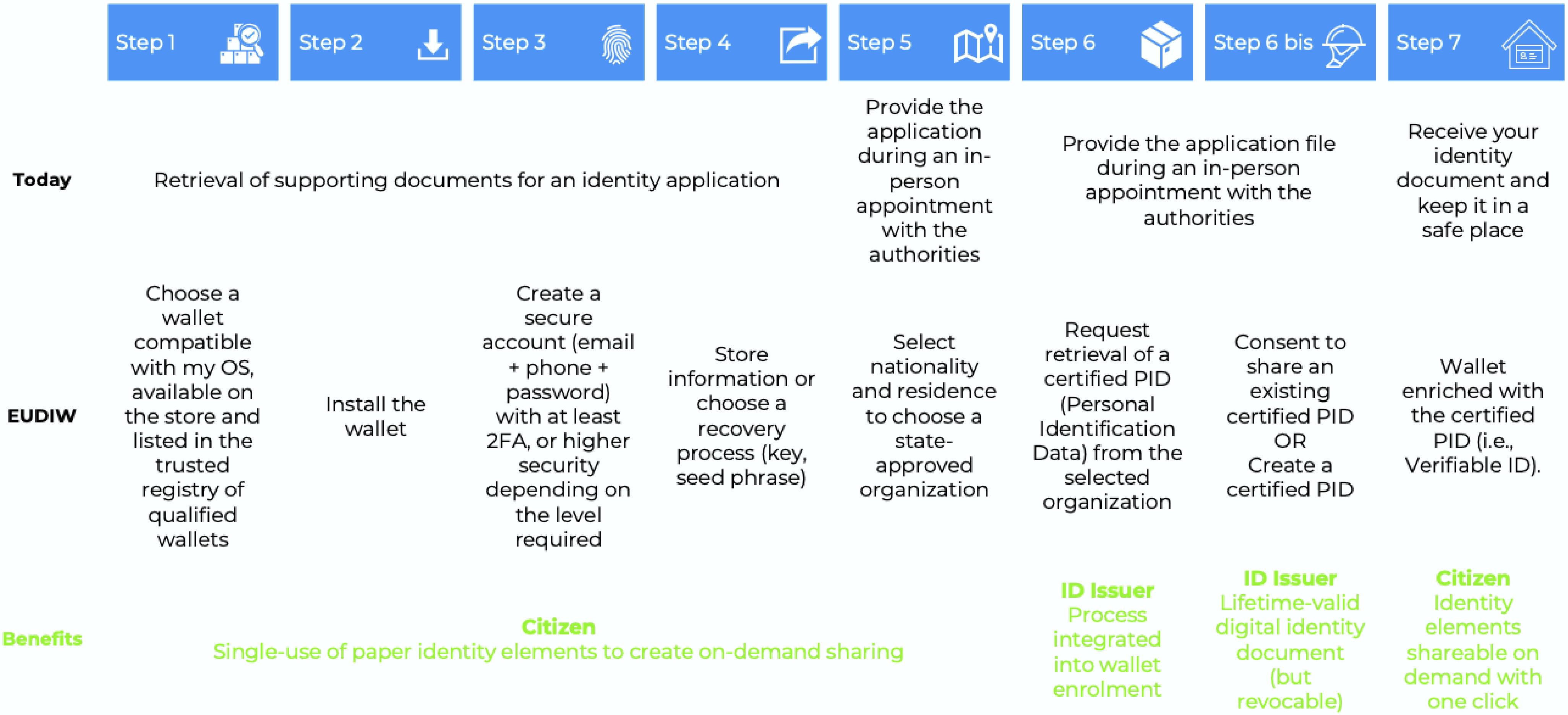
These solutions are useful but do not create substantial independent value. Their importance lies in integration within broader ecosystems.

- Biometry:
    - Enhances security but also raises privacy concerns, limiting its standalone value.
    - Standards applied to ensure accuracy and robustness of biometric authentication mechanisms:
        - ISO/IEC 19794-5 – Facial image data formats.
        - ISO/IEC 30107-3 – Presentation attack detection (PAD).
- Emails & Agendas:
    - Everyday tools with little direct impact on digital sovereignty but useful in identity-linked applications.
    - Standards applied to guarantee secure communications and scheduling interoperability:
        - RFC 5322 / iCalendar (RFC 5545) – Standardized messaging and scheduling.
        - S/MIME – Secure email encryption and signature.
- Browser:
    - A fundamental tool but not a direct driver of digital sovereignty on its own.
    - Standards applied to enable secure, standards-compliant wallet-browser integration with authentication support:
        - W3C WebAuthn / FIDO2 – Secure login without passwords.
        - ISO/IEC 27001 – Baseline browser session security management.

3 Use Cases

3.1 Use Case #1: Citizen Wallet Initialization: A complete enrollment process that includes installing the wallet and retrieving certified identity attributes.

3.1.1 Today and EUDIW’s process



	Step 1	Step 2	Step 3	Step 4	Step 5	Step 6	Step 6 bis	Step 7
Today	Retrieval of supporting documents for an identity application				Provide the application during an in-person appointment with the authorities	Provide the application file during an in-person appointment with the authorities		Receive your identity document and keep it in a safe place
EUDIW	Choose a wallet compatible with my OS, available on the store and listed in the trusted registry of qualified wallets	Install the wallet	Create a secure account (email + phone + password) with at least 2FA, or higher security depending on the level required	Store information or choose a recovery process (key, seed phrase)	Select nationality and residence to choose a state-approved organization	Request retrieval of a certified PID (Personal Identification Data) from the selected organization	Consent to share an existing certified PID OR Create a certified PID	Wallet enriched with the certified PID (i.e., Verifiable ID).
Benefits	**Citizen** Single-use of paper identity elements to create on-demand sharing					**ID Issuer** Process integrated into wallet enrolment	**ID Issuer** Lifetime-valid digital identity document (but revocable)	**Citizen** Identity elements shareable on demand with one click

Today's process is an example based on the French system. Today, in France, obtaining and using a **digital identity document** follows a well-defined process, mainly based on national systems such as **France Identité** and eIDAS. Here's a comparison with the **European Digital Identity Wallet (EUDIW)** and the benefits it brings.

- 1. Choosing and Installing a National Wallet
    - In France, citizens can use **France Identité**, an official app to store their **Electronic National Identity Card (CNIe)**.
    - Available on app stores (Google Play, App Store), **but limited to national use**.
    - Registration with **email, phone number, and activation via NFC** using the CNIe, secured with a **6-digit PIN code**, or even **biometric authentication**.
    - **No multi-device recovery option yet**.
    - The CNIe **is issued by the French State**, acting as the **sole identity provider**.
    - **No interoperability with other EU countries**.
- 5. Obtaining a Verified Identity
    - If the user has an **activated CNIe**, they can generate **verifiable attestations** (age, residence...).
    - **Limited use** for French public services and some private entities (banks, administration...).
- 6. Provide the application file during an in-person appointment with the authorities
- 7. Sharing and Using the Identity
    - Information can be shared via **QR codes and NFC**, but **only with services compatible with France Identité**.
    - **Not yet fully integrated with other countries or European services**.

With the **European Digital Identity Wallet (EUDIW)**, the process becomes **smoother, more secure, and most importantly, interoperable** across Europe.

- 1. Choosing and Installing a European Wallet
    - The user downloads a qualified wallet from app stores (Google Play, Huawei, Apple).
    - The wallet is listed in a trusted registry and compatible with all EU member states.
- 2. Install the wallet
- 3. Creating an Ultra-Secure Account
    - Registration with **higher security standards** (minimum 2FA, biometric authentication possible).
    - **Secure storage and recovery options** using a private key or seed phrase.
- 4. Storing and Managing Data Across Devices
    - The digital identity is synchronized and recoverable on multiple devices.
    - Advanced protection in case of device loss or theft.
- 5. Choosing a Certified Identity Provider

  - The user can select a qualified identity provider, validated by both the national government and the EU.
  - Compatible across different countries—no need for separate accounts for different national services.
- 6. Obtaining a Verified PID
  - The user can retrieve a certified PID (e.g., CNIe, Digital Passport, PVID...).
  - Or generate a verified identity using official documents.
  - One-click identity sharing with administrations, banks, and private services.
- 7. Full control over what data is shared (age, nationality, driver's license...).
  - Works in all EU countries without the need for multiple verifications.

Key Benefits of EUDIW Compared to the Current French System:

Criteria	□□ France Identité (Current)	□ EUDIW (Future)
Interoperability	Limited to France	Usable across the EU
Security	6-digit PIN	2FA, biometrics, private keys
Data Recovery	Local storage only	Backup and multi-device recovery
Identity Sharing	QR code, NFC	One-click sharing with data control
Service Access	Only for French services	Public and private services across the EU
Identity Provider	Only the French State	Multiple qualified providers

Today, in France, the digital identity process is still national, with solutions like France Identité, which offer high security but **limited interoperability**. **With EUDIW**, citizens will have a **single, secure wallet** that is **valid across Europe**. They will be able to manage their **personal data**, access **public and private services** in multiple countries, and **instantly and securely share their identity**. The EUDIW represents a **revolution in digital identity management** and will significantly simplify administrative and commercial processes across Europe.

3.1.2 Standards

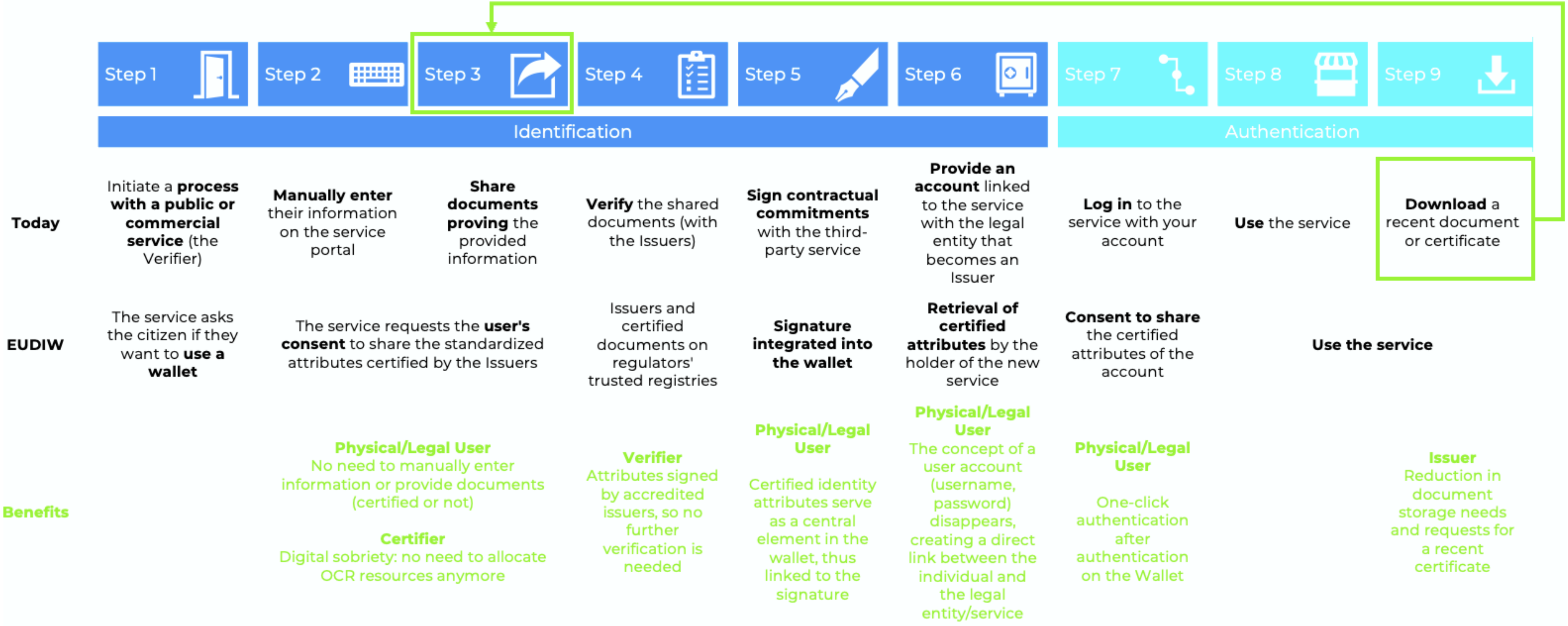
These standards provide a secure and compliant process for onboarding individuals, guaranteeing the reliability and integrity of the attributes issued to the wallet:

- ETSI TS 119 461 – for identity proofing and assurance levels.
- ISO/IEC 29115 – to define authentication levels and requirements.

- W3C Verifiable Credentials – to encode identity attributes.
- EBSI Trusted Issuers Registry – to ensure issuer validity and trust linkage.

3.2 The Wallet: the key enabling a looped lifecycle of VCs.

Today, many documents issued by public or commercial services are used for enrollment in other public or commercial services. Thus, it is possible to define a common framework for this use of documents issued by one service and required for the opening of others. The table in the image outlines the identification and authentication process when enrolling in a new service, comparing today's manual process with the EU Digital Identity Wallet (EUDIW) approach. It highlights the benefits of using the wallet for different stakeholders. Here's a structured breakdown:

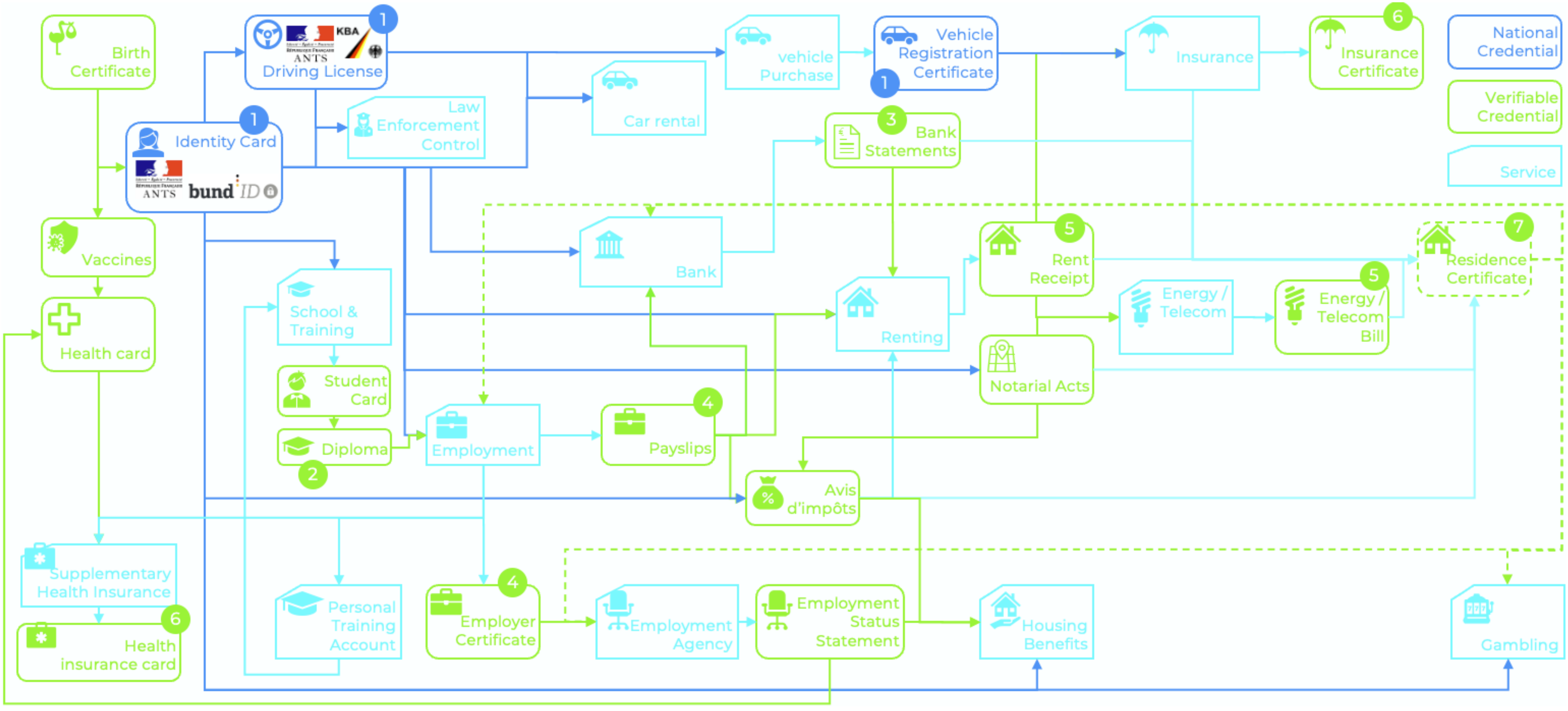


	Step 1	Step 2	Step 3	Step 4	Step 5	Step 6	Step 7	Step 8	Step 9
	Identification						Authentication		
Today	Initiate a **process with a public or commercial service** (the Verifier)	**Manually enter** their information on the service portal	**Share documents proving** the provided information	**Verify** the shared documents (with the Issuers)	**Sign contractual commitments** with the third-party service	**Provide an account** linked to the service with the legal entity that becomes an Issuer	**Log in** to the service with your account	**Use** the service	**Download** a recent document or certificate
EUDIW	The service asks the citizen if they want to **use a wallet**	The service requests the **user's consent** to share the standardized attributes certified by the Issuers		Issuers and certified documents on regulators' trusted registries	**Signature integrated into the wallet**	**Retrieval of certified attributes** by the holder of the new service	**Consent to share** the certified attributes of the account	**Use the service**	
Benefits		**Physical/Legal User** No need to manually enter information or provide documents (certified or not) **Certifier** Digital sobriety: no need to allocate OCR resources anymore		**Verifier** Attributes signed by accredited issuers, so no further verification is needed	**Physical/Legal User** Certified identity attributes serve as a central element in the wallet, thus linked to the signature	**Physical/Legal User** The concept of a user account (username, password) disappears, creating a direct link between the individual and the legal entity/service	**Physical/Legal User** One-click authentication after authentication on the Wallet		**Issuer** Reduction in document storage needs and requests for a recent certificate

The EUDIW model streamlines the entire process, reducing friction in service enrollment by leveraging trusted digital identity attributes. This eliminates manual inputs, document uploads, and redundant verifications, enhancing security, efficiency, and user experience.

3.3 The Impact of EUDIW on Everyday Life Events

Most events in our physical daily lives can be impacted by the arrival of the EU Digital Identity Wallet (EUDIW):



3.3.1 Birth Certificate & Identity Documents

- Our birth certificate allows us to request identity documents from national authorities, such as identity cards, driver's licenses, or vehicle registration certificates (e.g., ANTS in France, BundID or KBA in Germany).
- Standards applied to support legally recognized and verifiable issuance of identity base records, enabling portability and reuse.
    - W3C Verifiable Credentials – to issue verifiable birth certificates.
    - ISO/IEC 18013-5 – for mDL use.
    - ETSI TS 119 432 – for secure signature of civil documents.

3.3.2 Education & Professional Certifications

- We must verify our identity to enroll in school or training programs, enabling us to obtain diplomas, certifications, and professional cards (e.g., healthcare professional cards).
- Standards applied to ensure interoperable educational claims and verification of professional skills across Europe:
    - EDCI / Europass Schema – for structured academic credentials.
    - W3C VC + BBS+ Signatures – to support credential reuse and privacy.
    - ETSI EN 319 401 – to certify institutional integrity.

3.3.3 Banking & Financial Services

- Our identity and proof of residence allow us to open bank accounts and receive bank statements.
- Standards applied to enables automated compliance with Anti-Money Laundering (AML) requirements while enhancing data minimization:
    - ISO 17442 – for LEI integration.
    - ETSI TS 119 461 – identity proofing assurance.
    - DIF Presentation Exchange 2.0 – to support granular claims presentation

3.3.4 Employment & Payroll

- Diplomas/identity verification are required to sign employment contracts and obtain employer certificates or pay slips.
- Standards applied to provide certified education and ID records to streamline hiring and payroll issuance:
  - W3C VC Data Model – for diploma and ID reuse.
  - ETSI EN 319 401 – for employer-side trust services.
  - ISO/IEC 27001 – for payroll system security.

3.3.5 Essential Services & Proof of Address

- Many essential services provide utility bills (e.g., mobile phone, energy) and rent receipts, which can serve as proof of residence depending on legislation.
- Standards applied to facilitate reuse of service-based evidence in administrative and regulatory contexts:
  - W3C Verifiable Credentials – to issue verifiable bills or service attestations.
  - ISO 20488 – for trustworthy service data records.
  - ETSI TS 119 432 – to sign residence proofs.

3.3.6 Insurance & Healthcare

- Employment often includes health insurance with an annually updated card. Insurances also issue certificates (e.g., vehicle insurance attestations).
- Standards applied to ensure secure, structured, and recognized evidence for health and liability protection:
  - HL7 FHIR, ISO/IEC 27001 – for health data formats and privacy.
  - W3C VC – to manage reusable credentials for coverage.
  - EN 17269 – for cross-border patient summary.

3.3.7 Housing & Rental

- Identity verification is required to rent an apartment, with rent receipts serving as proof of residence (alongside mobile phone or energy bills, depending on regulations). These proofs are also essential for many administrative procedures.
- Standards applied to enable legal recognition of rental documents and tenant status in digital procedures:
    - W3C VC + JSON-LD – to encode rental contracts and receipts.
    - ETSI TS 119 432 – for notarization of tenant attestations.
    - ISO/IEC 27001 – for secure storage and communication.

The EUDIW will streamline these processes by providing a secure and interoperable digital identity that can replace manual document submissions. This will enhance efficiency, security, and accessibility in both public and commercial services.

3.4 Use Case #2: Pre-hospitalization File

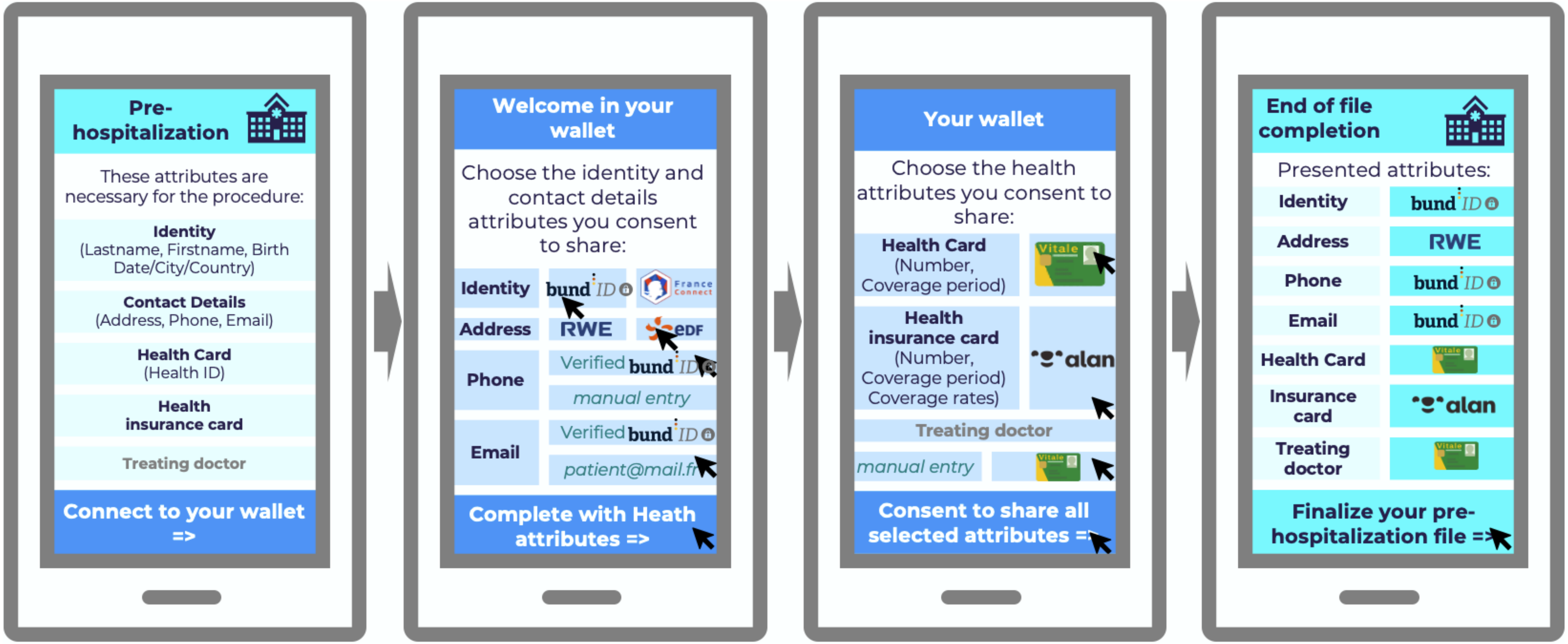
We choose to follow the digital journey of a Franco-German citizen, born in Germany, with a family residence in his country of origin, but residing and working in France (§ 3).

3.4.1 EUDIW’s process

He already has an EDF energy bill in their wallet, a French Carte Vitale as a worker in France, and health insurance with ALAN. Unfortunately for him, he needs to be hospitalized because he broke his arm. The hospital could ask him to complete a pre-admission file in paper format, but there is also a process based on the European Wallet. Luckily, the patient has his phone and his wallet with the required attributes.

He scans a certified QR code provided by the reception. Once opened, it asks if he consents to open his wallet to share certain elements. Since these elements are standardized, the hospital's request can recognize attribute norms already available in the wallet. The patient consents and selects the sources of the attributes. For example, an internet bill and two energy bills (EDF for main address in France and RWE for family second home in Germany) are recognized as address certificates. He chooses his address in France because this on is used frequently used for administrative current procedures.

Some data can even be entered manually by the patient (such as an email different from the one linked to his digital identity. At the end, the wallet requests a grouped consent, and the data is shared with the hospital to complete the pre-admission file.



Pre-hospitalization

These attributes are necessary for the procedure:

Identity (Lastname, Firstname, Birth Date/City/Country)

Contact Details (Address, Phone, Email)

Health Card (Health ID)

Health insurance card

Treating doctor

Connect to your wallet =>

Welcome in your wallet

Choose the identity and contact details attributes you consent to share:

Identity	bund ID	France Connect
Address	RWE	EDF
Phone	Verified bund ID *manual entry*	
Email	Verified bund ID *patient@mail.fr*	

Complete with Heath attributes =>

Your wallet

Choose the health attributes you consent to share:

Health Card (Number, Coverage period)	Vitale
Health insurance card (Number, Coverage period) Coverage rates)	alan
Treating doctor	
manual entry	Vitale

Consent to share all selected attributes =>

End of file completion

Presented attributes:

Identity	bund ID
Address	RWE
Phone	bund ID
Email	bund ID
Health Card	Vitale
Insurance card	alan
Treating doctor	Vitale

Finalize your pre-hospitalization file =>

3.4.2 Standards

These standards enable trusted and interoperable exchange of sensitive health records while preserving patient control and consent:

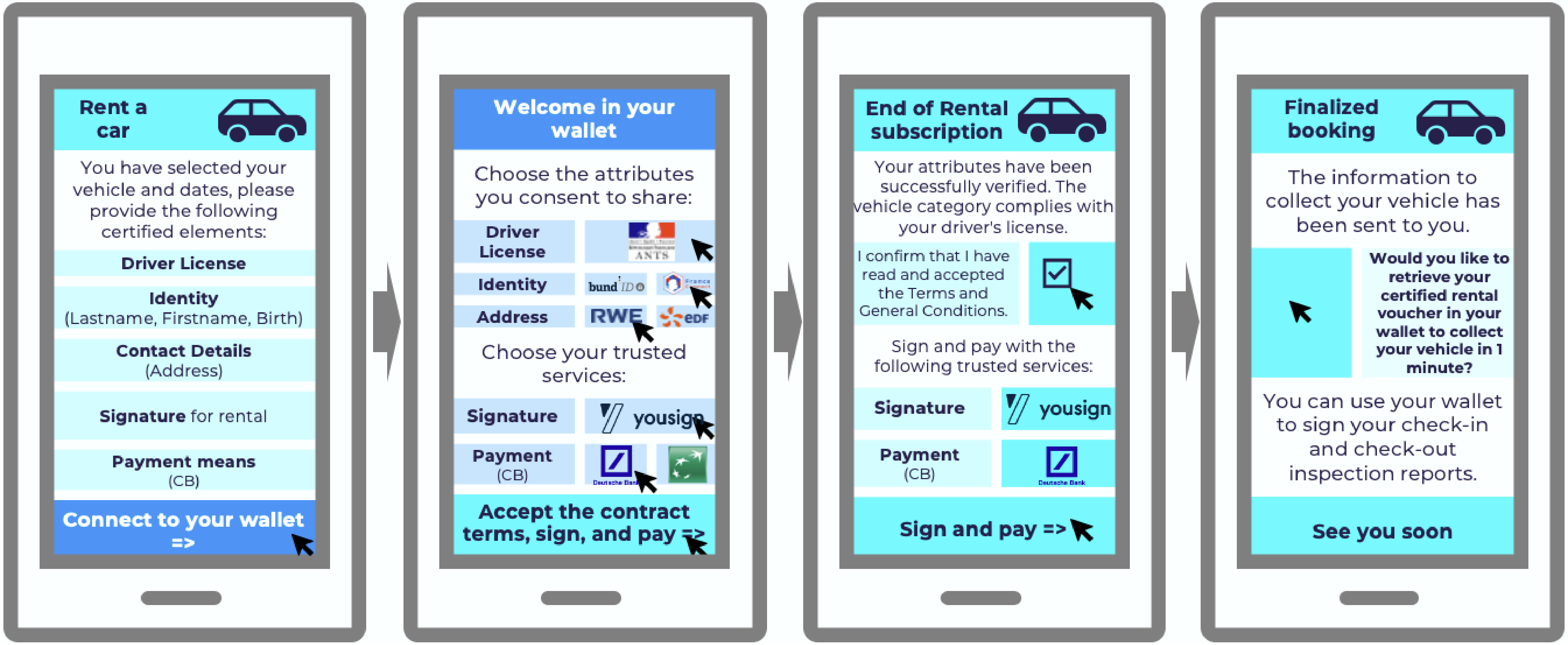
- HL7 FHIR & EN 17269 – for health data formatting and cross-border interoperability.
- W3C Verifiable Credentials – for structured and verifiable data sharing.
- ISO/IEC 27001, ISO/IEC 29100 – for security and privacy management.
- DIF Presentation Exchange – for selective sharing of sensitive health information.

3.5 Use Case #3: Vehicle rental with certified driver license

The same person as Use Case #1 want to rent a car after his flight arriving in Germany to go and see his family and spend some time in his family second home).

3.5.1 EUDIW's process

After selecting an offer based on a specific car type and defined dates, the car rental application suggests using his wallet to complete the reservation, informing him that he must have a certified driver's license, a digital identity, an address, an electronic signature, and a payment method.



Rent a car

You have selected your vehicle and dates, please provide the following certified elements:

Driver License

Identity (Lastname, Firstname, Birth)

Contact Details (Address)

Signature for rental

Payment means (CB)

Connect to your wallet =>

Welcome in your wallet

Choose the attributes you consent to share:

Driver License

Identity

Address

Choose your trusted services:

Signature

Payment (CB)

Accept the contract terms, sign, and pay =>

End of Rental subscription

Your attributes have been successfully verified. The vehicle category complies with your driver's license.

I confirm that I have read and accepted the Terms and General Conditions. ☑

Sign and pay with the following trusted services:

Signature

Payment (CB)

Sign and pay =>

Finalized booking

The information to collect your vehicle has been sent to you.

Would you like to retrieve your certified rental voucher in your wallet to collect your vehicle in 1 minute?

You can use your wallet to sign your check-in and check-out inspection reports.

See you soon

The user agrees and consents to present his French driver's license issued by the National Agency for Secure Documents (ANTS), his French identity document, and his German address, certified by his local energy provider. Being a user of an electronic signature solution, he agrees to use it directly within his wallet (which immediately certifies the signatory's identity). He then selects one of his two bank accounts (one in each country) and chooses to pay with his German bank account.

By finalizing his reservation with a signature and payment, he has the option to retrieve his certified rental voucher directly in his wallet, which he chooses to do. Additionally, he will be able to use his wallet to prove his identity and reservation when collecting the rented vehicle. He can also sign the check-in and check-out inspection reports directly from his wallet.

3.5.2 Standards

These standards support verification of credentials in an offline or online flow, ensuring legal conformity and user privacy:

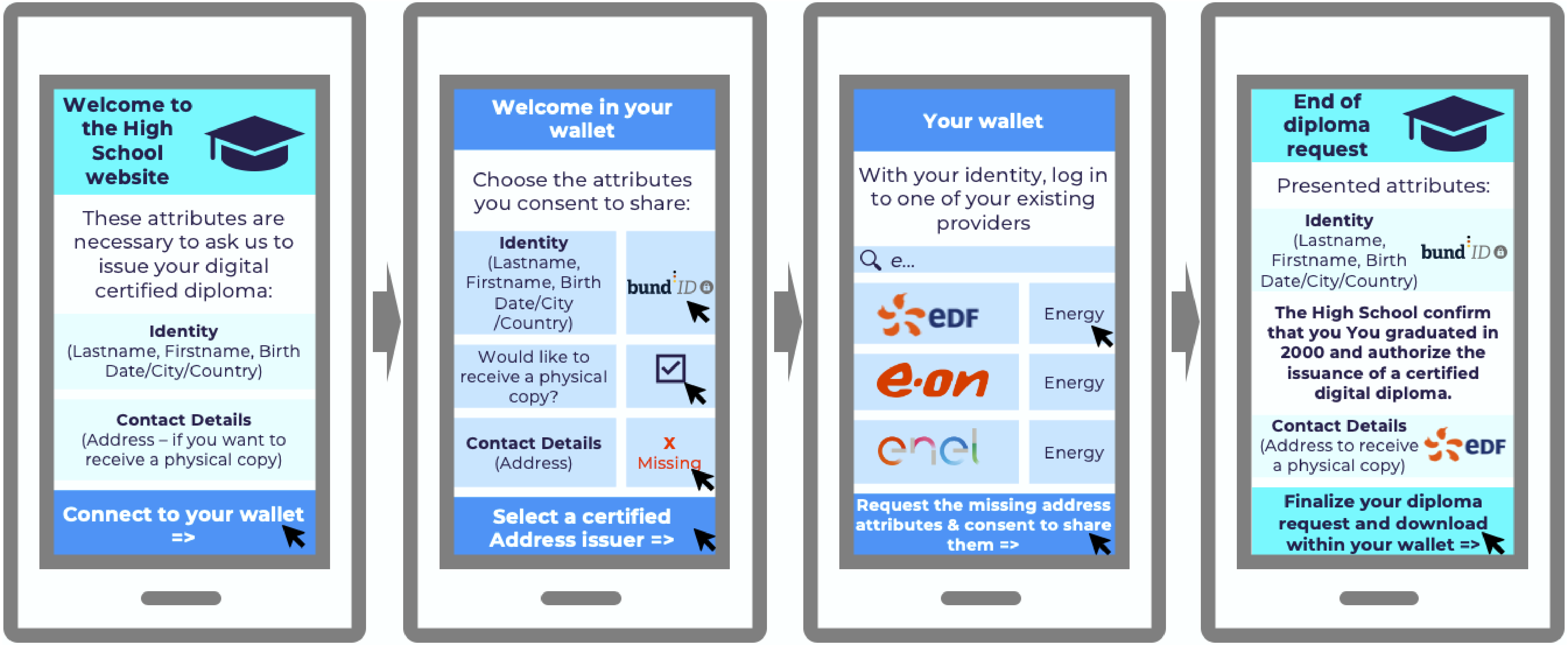
- ISO/IEC 18013-5 – defines technical specifications for mDL.
- ETSI TS 119 432 – for digital signature integrity.
- W3C Verifiable Credentials + DIDComm – for secure delivery of license data.
- OIDF OpenID for Verifiable Presentations – for dynamic verification workflows.

3.6 Use Case #4: Request a Digital Diploma from a Higher School

This procedure outlines how a user can request a certified digital diploma through a wallet-based identity verification system.

3.6.1 EUDIW's process

The user accesses the High School website, where they are informed that certain identity attributes are required to request a certified digital diploma.



Welcome to the High School website

These attributes are necessary to ask us to issue your digital certified diploma:

Identity
(Lastname, Firstname, Birth Date/City/Country)

Contact Details
(Address – if you want to receive a physical copy)

Connect to your wallet =>

Welcome in your wallet

Choose the attributes you consent to share:

Identity (Lastname, Firstname, Birth Date/City /Country)	bund ID
Would like to receive a physical copy?	☑
Contact Details (Address)	X Missing

Select a certified Address issuer =>

Your wallet

With your identity, log in to one of your existing providers

e...

eDF	Energy
e·on	Energy
enel	Energy

Request the missing address attributes & consent to share them =>

End of diploma request

Presented attributes:

Identity (Lastname, Firstname, Birth Date/City/Country)	bund ID

The High School confirm that you You graduated in 2000 and authorize the issuance of a certified digital diploma.

Contact Details (Address to receive a physical copy)	eDF

Finalize your diploma request and download within your wallet =>

The requested attributes include:

- Identity (Last name, First name, Birth Date/City/Country).
- Contact Details (Address – required if they want to receive a physical copy).

The user is prompted to connect to their wallet to proceed. Inside the wallet, the user chooses the attributes they consent to share with the school. The identity details are already available and can be shared. The address information is missing (marked with an "X"), meaning the user must select a certified address issuer to retrieve it.

The wallet provides a list of certified providers, listed on the trusted lists stored on the EBSI, and starting with “e” that can verify and certify the user’s address. The user logs in to one of these energy providers with their identity. Once authenticated, the missing address attributes are retrieved and consented for sharing with the school.

The school verifies the shared attributes. It confirms that the user graduated in 2000 and authorizes the issuance of a certified digital diploma. If a physical copy is needed, the selected address is shared with the high school. The user finalizes the diploma request and downloads the certified digital diploma into their wallet.

3.6.2 Standards

The following references standardize digital diploma issuance, enhances trust and streamlines future verifications:

- EDCI & Europass JSON Schema – for academic credential structure.
- W3C VC Data Model – to deliver portable and verifiable claims.
- ETSI EN 319 401 – to anchor trust in the issuing institution.

3.7 Use Case #5: Application of candidate with his Digital Diploma and Certification

The citizen is specialized within Cybersecurity, he passed the CISSP certification last year, then his certification is still valid (3 years).

3.7.1 EUDIW’s process

He want to apply to a job offer from UNESCO, based in Paris. This process demonstrates how a candidate can seamlessly apply for a job offer on LinkedIn by using a wallet-based digital identity verification system.

The user accesses a LinkedIn job offer and is informed that certain verified attributes are required to apply. The required attributes include:

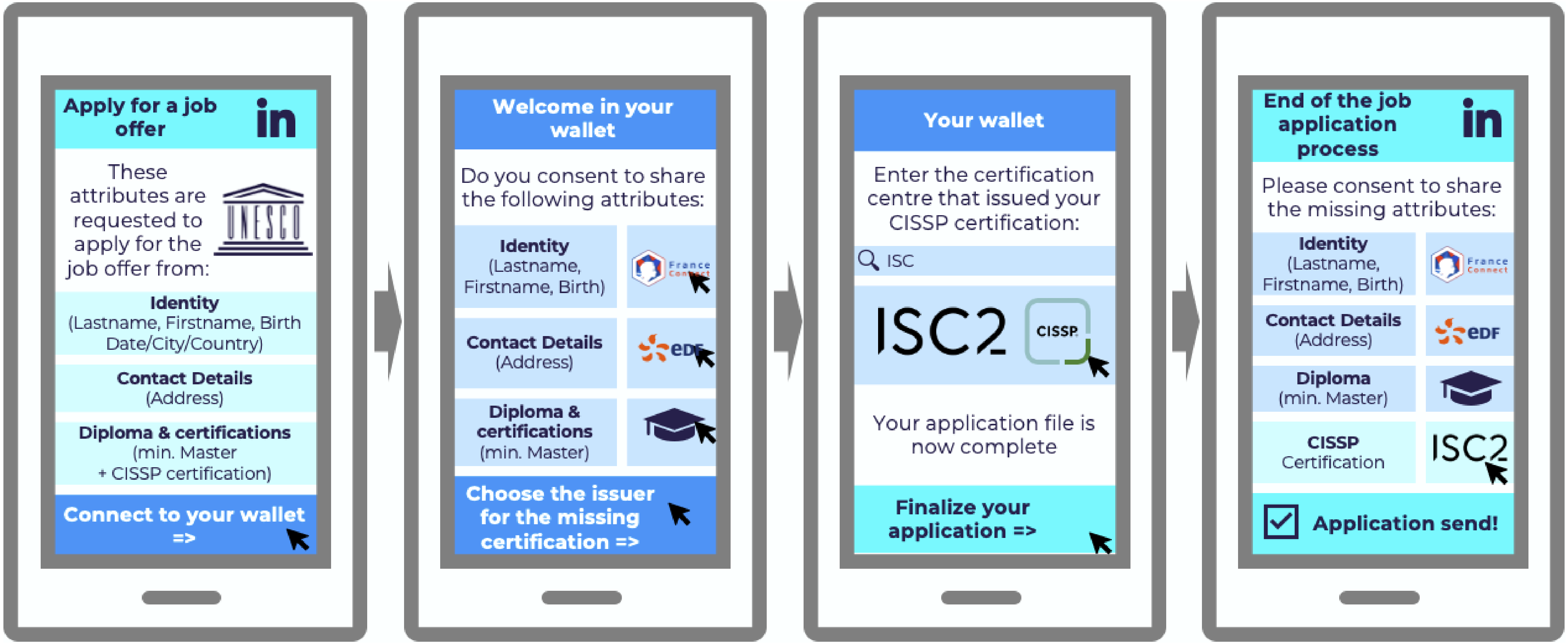
- Identity details (Last name, First name, Birth Date/City/Country).
- Contact details (Address).
- Diplomas & certifications (e.g., Master’s degree, CISSP certification).

The user is prompted to connect to their digital wallet to retrieve and share these attributes. Inside the wallet, the user is asked to consent to share the requested attributes. While the identity, contact details, master’s degree are available, the CISSP certification is missing.

The user must select an certified issuer to retrieve the missing certification. The wallet searches for the appropriate certification issuer (in this case, ISC2, which issues CISSP certifications). The wallet connect to the CISSP Issuer list of certified people, find the valid certification. Once added, the application file is now complete. The user finalizes the application by confirming all shared attributes.

The system revalidates the attributes and asks for final user consent before submitting the application. The user confirms the shared details (identity, address, diploma, and CISSP certification). The job application is successfully sent on LinkedIn.

This wallet-based application process makes job applications faster, safer, and more reliable by allowing users to directly share verified credentials, without any manual data enter, but with several automated verification, enhancing efficiency and security.



Apply for a job offer in

These attributes are requested to apply for the job offer from: UNESCO

Identity (Lastname, Firstname, Birth Date/City/Country)

Contact Details (Address)

Diploma & certifications (min. Master + CISSP certification)

Connect to your wallet =>

Welcome in your wallet

Do you consent to share the following attributes:

Identity (Lastname, Firstname, Birth) — France Connect

Contact Details (Address) — eDF

Diploma & certifications (min. Master)

Choose the issuer for the missing certification =>

Your wallet

Enter the certification centre that issued your CISSP certification:

ISC

ISC2 CISSP

Your application file is now complete

Finalize your application =>

End of the job application process in

Please consent to share the missing attributes:

Identity (Lastname, Firstname, Birth) — France Connect

Contact Details (Address) — eDF

Diploma (min. Master)

CISSP Certification — ISC2

☑ **Application send!**

3.7.2 Standards

These standards allow trusted validation of a candidate’s education and competencies while respecting data minimization principles.

- W3C BBS+ Signatures – to enable selective disclosure of attributes.
- W3C Verifiable Presentation – to bundle multiple credentials securely.
- ISO/IEC 27001 – to manage secure processing and verification by employer systems.

These standards enable secure, privacy-respecting authentication aligned with eIDAS 2.0 and interoperable across EU member states:

- W3C Verifiable Credentials – for presenting verified identity claims.
- OIDF OpenID for Verifiable Presentations – for federated login with selective disclosure.
- ETSI EN 319 401 – to ensure trust service policy compliance.

4 Conclusion

The future of digital identity is rapidly evolving, driven by the necessity for secure, verifiable, and interoperable identity solutions. This document highlights the transformative potential of digital wallets and verifiable credentials in streamlining identity verification, enhancing security, and fostering seamless interactions across public and private services.

As digital identity frameworks continue to mature, stakeholders must prioritize interoperability, compliance, and user trust to ensure widespread adoption. By leveraging standards such as eIDAS, W3C Verifiable Credentials, and blockchain-based identity solutions, the digital identity ecosystem can become more resilient and efficient.

Ultimately, the successful implementation of digital identity solutions will depend on collaboration between governments, private enterprises, and technology providers to create a universally accepted, user-centric system that enhances privacy, security, and convenience.