eIDAS2 Implementers Guide

All you need to become eIDAS2 compliant.

This guide gives you the why and the how: a clear overview of eIDAS2, the ARF, and the LSPs, followed by role-based responsibilities and step-by-step guidance to achieve compliance—whether you build in-house or use proven solutions.

Let’s dive in.

Table of contents

Introduction

This eBook shows you how to make your organization eIDAS2-compliant, following a simple structure:

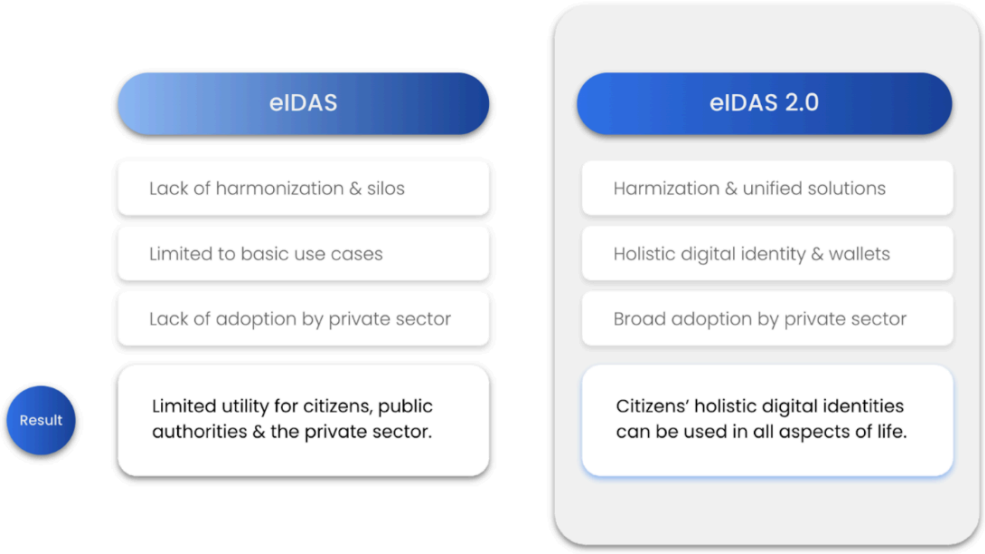
1. **Learn**: a high-level overview of eIDAS2 and the core terms—the Architecture and Reference Framework (ARF), Large-Scale Pilots (LSPs), the Implementing Acts, and the PID—plus a timeline so you know exactly when compliance is required.
2. **Plan**: the use cases eIDAS2 enables; the ecosystem actors (Issuers, Verifiers, and Wallet Providers) and the responsibilities, requirements, and go-to-market options for whichever role your organization falls into.
3. **Build**: a deep dive into each role (Issuer, Verifier, Wallet) and their sub-types—such as issuers of PID, PuB-EAA, QEAA, and EAA, and wallets (eIDAS2-certified and organizational/commercial)—with concrete technical requirements so you can start building.

Once you have read this eBook, you should be well equipped to start your eIDAS2 journey and will be able to ensure compliance before the upcoming regulatory deadlines.

Learn | eIDAS2

The problem eIDAS2 solves

In 2016 the eIDAS (electronic Identification, Authentication and Trust Services) regulation created a framework for cross-border electronic identification. It focused on a small set of trust services, notably electronic signatures, and left wide latitude to Member States. As a result, national implementations diverged, interoperability remained limited and citizens lacked a harmonised digital identity. During the pandemic, physical presence requirements made identity proofing difficult and fragmentation slowed adoption beyond the public sector.



The eIDAS2 regulation

eIDAS2 (Regulation (EU) 2024/1183) was created to address these shortcomings by introducing **European Digital Identity (EUDI) wallets** for every EU citizen. Its main goals are to provide user-controlled digital identities, reduce fraud and enable trustworthy digital interactions across borders.

Under eIDAS2:

- Governments must issue digital identity credentials and provide wallets.

- Citizens receive a **Person Identification Data (PID)** credential from their Member State as well as other types of identity credentials .
- Businesses are required to accept these credentials for onboarding and authentication.
- High levels of **security and privacy** are mandated and compliance is audited.
- Wallets support **selective disclosure** so users can share only what is necessary.

The regulation effectively **bootstraps the market** by forcing the issuance and acceptance of digital identity credentials in all EU member states. This accelerates adoption and lowers the "cold-start" barrier for decentralised identity solutions.

If you want to learn more about eIDAS2 and its impact on governments and business across industries, check out our "eIDAS2 is here" ebook.

The Architecture and Reference Framework (ARF)

The **Architecture and Reference Framework (ARF)** is the technical companion to eIDAS2 describing how the "law" could be implemented in practice. It defines:

- **High-level requirements** for each party (Issuer, Relying Parties aka. Verifiers and Wallet Providers).
- **How parties must interact** to ensure ecosystem security, user privacy and EU-wide interoperability.
- **Common schema catalogues and a shared trust infrastructure** (with issuer catalogues) to ensure the authenticity and reliability of digital interactions.

The ARF is published on the official EUDI Wallet Dev Hub (GitHub) here, with releases and updates announced on the European Commission's EUDI Wallet site here.

The Large-Scale Pilots (LSPs)

The **Large-Scale Pilots** (LSPs) are EU-funded, cross-border projects that **implement the ARF in real services**. They validate protocols (OID4VCI/OID4VP, ISO/IEC 18013-5/-7), data formats (SD-JWT VC, mDL, selected W3C VC profiles for EAAs), Wallet Unit components (WSCD, WUA/WIA/WTE) and end-to-end user journeys across Member States.

Four LSPs have been successfully concluded (POTENTIAL, EWC, NOBID, DC4EU) while two (APTITUDE, WE BUILD) started in 2025 and are currently active. More details on each LSPs focus below:

- **POTENTIAL** - Pilots the EUDI Wallet across six sectors: government services, banking, telecom, mobile driving licence, electronic signatures, and health; runs cross-border interoperability tests (e.g., mDL and e-prescription trials).
- **EWC** - Focused on Digital Travel Credentials (DTC) and end-to-end travel flows, building on the Commission's reference wallet.
- **NOBID** - Concentrates on the payments use case for domestic and cross border usage with the wallet, piloted by Nordic-Baltic countries plus Italy and Germany.
- **DC4EU** - Targets education, professional credentials/qualifications, and social security, providing feedback to the Commission on interoperability and scalability.
- **APTITUDE** - Tests the wallet across a broad range of use cases including travel and mobile vehicle registration certificates (mVRC); aims to demonstrate interoperability, usability and scalability.
- **WE BUILD** - Focuses on business and payment use cases that streamline B2B, B2G, and B2C processes.

The findings of LSPs (interoperability gaps, edge-case UX, policy clarifications) will feed back into the ARF.

The Implementing Acts

The implementing acts turn the high-level eIDAS2 regulation into **concrete rules and laws** building on top of the ARF and the LSP results. The rules come in dedicated regulations (list below & in Annex)–**covering core functionality, protocols, PID/EAA data handling, certification, notifications and registers**–everything needed so ID wallets (and their ecosystem) can become a reality across member states.

Below is an excerpt of the list of already adopted regulations. In the Annex you can find the full list.

- (EU) 2024/2979 — Integrity & core functionalities of EU Digital Identity Wallets.

- (EU) 2024/2982 — Protocols and interfaces to be supported by the EU Digital Identity Framework.
- (EU) 2024/2977 — Person Identification Data (PID) & Electronic Attestations of Attributes (EAAs) issued to wallets.

The PID

The **Person Identification Data (PID)** is a special type of digital credential defined under the eIDAS2 regulation. It's issued by appointed institutions ("PID Providers") in each member state to their citizens and will act as the core "digital ID" that is recognised across member states. A PID will be required to "activate" and use an eIDAS2 certified wallet.

Mandatory attributes of a PID:

- Family Name
- Given Name
- Birth Date
- Birth Place
- Nationality

Optional attributes of a PID include:

- Resident Address
- Resident Country
- Resident State
- Resident City
- Resident Postal Code
- Resident Street
- Resident House Number
- Personal Administrative Number
- Portrait
- Family Name Birth
- Given Name Birth

- Sex
- Email Address
- Mobile Phone Number

Note: The mandatory and optional attributes of a PID are defined in the (EU) 2024/2977 regulation.

The Timeline

While eIDAS2 entered into force in May 2024. Governments and businesses will have till the end of 2026 or 2027 to become fully compliant.

Governments (Member States)

- Must launch at least one EUDI wallet per member state by the end of 2026.
- Must ensure qualified trust service providers (QTSPs) have a way to verify required user attributes against authentic sources by the end of 2026
- Must ensure public-online services that already ask for eID/auth today, accept EUDI wallets once available.

Businesses (Relying Parties - Verifiers)

- **Private-Sector businesses** that require e.g. strong user authentication (e.g. transport, energy, banking/financial services, …) and are not micro or small enterprises (< 50 employees & ≤ €10 million annually), must enable EUDI wallet usage for user authentication (sign-in, step-up auth, onboarding) by the end of 2027.
- **Very Large Online Platforms** (≥ 45 million average monthly users in the EU) must accept EUDI wallets for user authentication (sign-in, step-up auth, onboarding) as soon as the wallets are available (approx. end of 2026).

The timelines and use cases above mark when organisations and Member States must comply by law. But they're only the starting point. As millions of users gain access to a digital ID wallet, businesses can deploy many more use cases to cut costs, streamline processes, reduce fraud and deliver a better UX. The businesses that move quickly can gain a first-mover advantage in the space.

Plan | Steps to Get Started with eIDAS2

In the upcoming section, we look at the various use cases that digital IDs under eIDAS2 enable and help you decide which of these might be a good starting point for your organization.

As any digital ID ecosystem consists of actors (Issuers, Verifiers, and Wallet Providers), we will also explore who they are—their responsibilities and requirements.

Finally, we will look at the options for bringing a working solution to market.

Use Cases

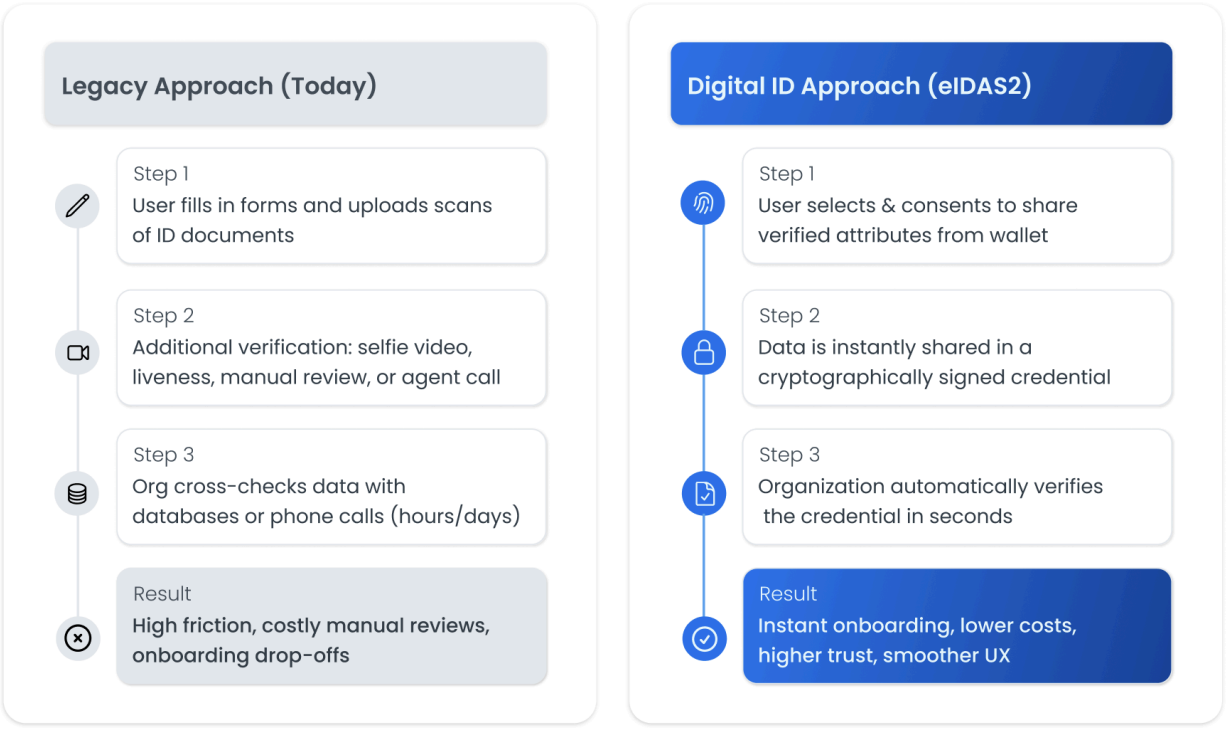
Digital identity will touch virtually every sector and industry across the EU. From governments to businesses, the opportunities are immense:

- cutting costs,
- streamlining operations,
- automating manual processes,
- reducing fraud and creating
- more seamless user experiences.

The most common ones—and those legally required under eIDAS2 (as discussed in "The Timeline" section)—center around user authentication. This includes:

- sign-in/sign-up,
- step-up authentication (extra-auth),
- user onboarding in general.

To understand the impact, let's take a closer look at the user onboarding journey and compare how it works today versus how it will work with digital IDs:



Beyond Authentication

While authentication and onboarding are the starting point, there are various other use-cases that digital IDs will unlock across industries. A few examples include:

	Industry	Use-Cases
	**Financial services**	• Streamlined KYC/AML checks • Faster account opening • secure digital signatures for contracts
	**Healthcare**	• Secure patient identification • Consent management • Cross-border health record access
	**Education**	• Issuance of diplomas and certificates as verifiable credentials • Student discounts with strong assurance • Micro credentials
	**Travel & Mobility**	• Seamless check-ins • e-ticketing • Digital travel credentials (DTCs)
	**Public services**	• Access to benefits • Tax filings • Permit applications
	**Employment**	• Verified professional credentials • Automated right-to-work checks • Smoother HR onboarding
	**eCommerce & Retail**	• One-click checkout with verified payment details • Secure proof-of-age for restricted goods • Loyalty programs tied to verified identities
	**Real estate & Housing**	• Verified tenant background checks • Digital lease agreements • Automated proof of income or employment
	**Telecommunications**	• Simplified SIM card registration • Contract signing
	**Legal & Notarial Services**	• Verified power of attorney • Notarized deeds • Company formation documents

How to Pick a Use Case

Generally speaking, if you are a government or technology provider for governments, use-cases with a legal deadline (as explained in “The Timeline" section) become the highest priority. The same goes for larger businesses that require strong user auth and don’t fall under the exemption rule of micro or small enterprises.

That being said, the highest priority use-cases are:

1. **Wallets** | Actor: Wallet Provider

Governments (each member state) must provide an eIDAS2 compliant wallet solution by the end of 2026.

2. **Online User Authentication** | Actor: Relying Party (Verifier)

Large businesses must enable user-auth with wallets by the end of 2027 while Very Large Online Platforms and public-services (e.g., government services) must enable it as soon as wallets are available (approx. end of 2026).

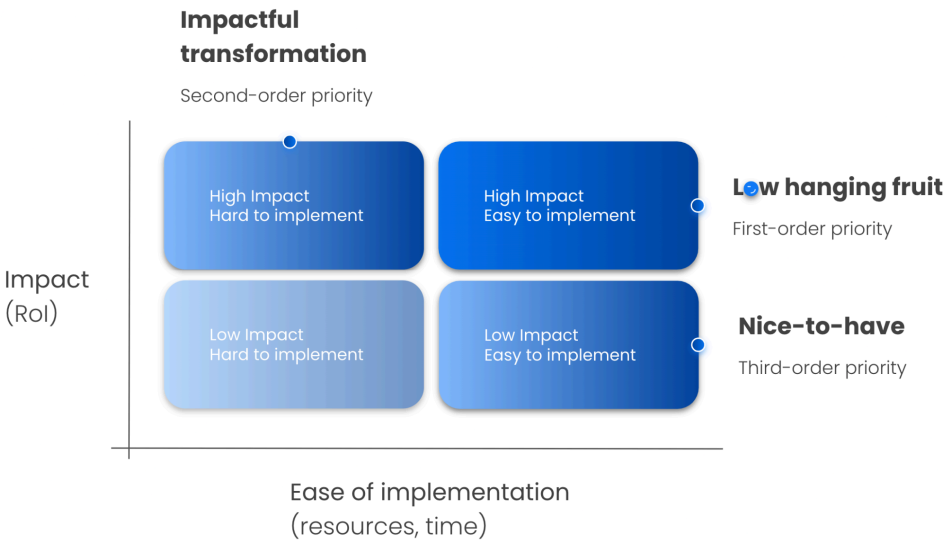
For detailed user flows, please see the Use-Case section above.

3. ***Use case without a regulatory deadline***

All other use-cases don’t have a legal deadline and can therefore be prioritized on a case-by-case basis. As a helper, you can use the following matrix.

First, take a sub-set of use cases listed above (e.g. use onboarding, authentication, ID wallet, check-out), which are relevant to your organization and prioritize them based on your strategy and product or service portfolio.

This matrix offers a simple way to prioritize use cases based on their impact on your organization (RoI) and ease of implementation (resources, time).



Here's a few tips on how to use the matrix:

Impact

- ☐ **Increase revenue**: Streamline onboarding or check-out, improve conversion & dropout rates.
- ☐ **Lower costs**: Enable digital interactions, automate processes to save costs & resources.
- ☐ **Prevent compliance issues**: Ensure regulatory compliance to avoid penalties & brand damage.
- ☐ **Prevent fraud**: Ensure reliable stakeholder verification to prevent ID theft or doc forgery.
- ☐ **Mitigate security risks**: Eliminate risk factors that cause data breaches (e.g. passwords).
- ☐ **Strengthen your brand**: Offer more seamless UX, strengthen compliance, security & enhance privacy.
- ☐ **Don't fall behind**: Decentralized ID changes everything & your competition is already on it.

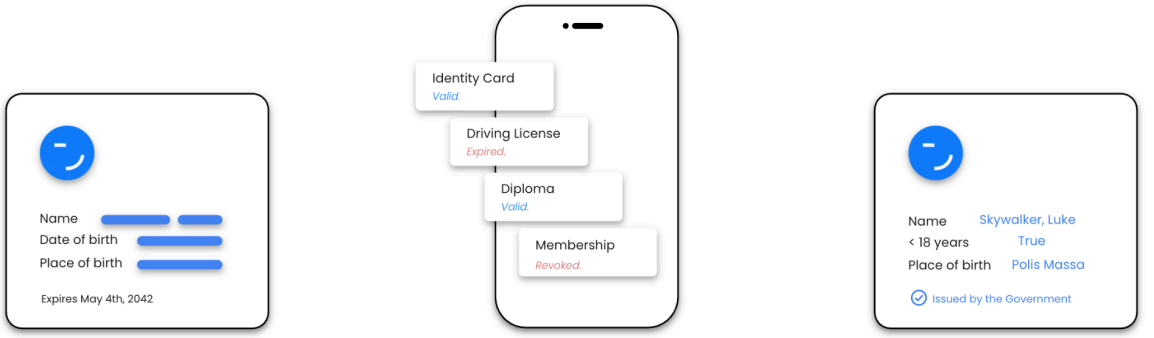
Ease of Implementation

- ☐ **UI/UX**: What will it take to offer users a seamless experience with new products or features?
- ☐ **Data**: What kind of data will we need, where and how is this data currently stored, processed?
- ☐ **Deployment**: How will solutions be tested and deployed, which environments will be used?
- ☐ **Integration**: How complex will be the integration with existing business processes and systems.
- ☐ **Ownership**: Which departments are involved in your use case(s) and how do they make decisions?
- ☐ **Buy vs Build**: Will you buy or build - potentially using open source solutions?

You can find a more detailed list for prioritizing use cases in the Annex.

Explained: Issuer, Verifier, Wallet Provider

Below, we define Issuer, Verifier and Wallet Providers–the required actors for any digital ID ecosystem–and their responsibilities and high-level requirements under eIDAS2. The more detailed technical requirements, we will discuss in the upcoming "Build" section.



Issuer

Issues digital credentials

Wallet Provider

Offers digital ID wallet

Relying Party

Verifies digital credentials.

The Issuer

Issuers are governments and/or businesses that **attest claims about a user or legal entity (e.g. name, VAT ID) in the form of a digital credential**, also called Electronic Attestations of Attributes (EAAs) in eIDAS2 terms. These credentials are a piece of data that is cryptographically signed by a key only the issuer controls and verified using the public counterpart of the key. Trust is established through official lists and registries each actor (Issuer, Verifier and Wallet Provider) must be listed on in order to be trusted by other actors in the ecosystem. The credential data format will follow technical standards such as mdoc/mDL, SD-JWT VC IETF and/or W3C VC v2.0 and are delivered over the internet to end-users using protocols like OID4VCI/ISO-18013-7.

Under eIDAS2 the credentials (attestations) issuers can issue are divided into five categories:

1. **Person Identification Data (PIDs)** - PIDs are the core “digital ID” attribute set (e.g. name, address, nationality, …) every wallet user gets issued by the PID Providers in each member state.
2. **Legal Person Identification Data (LPIDs)** - LPID is the counterpart for natural persons PID for legal persons (e.g. companies, organisations, institutions) also issued by the PID Providers in each member state.
3. **Public Body Authentic Source Electronic Attestation of Attributes (PuB-EAAs)** - PuB-EAAs are official documents (e.g. birth certificate, residence permits, tax IDs) in their digital form and they hold the same legal value as their paper counterpart. They are issued by registered PuB-EAA providers.
4. **Qualified Electronic Attestation of Attributes (QEAA)** - QEAAs are attestations whose attributes are verified against authentic sources (e.g. company formation documents sourced from a Companies Register). They also hold the same legal value as paper documents. They are issued by registered qualified trust service providers.
5. **Non-Qualified Electronic Attestation of Attributes (EAAs)** - are all other types of attestations (e.g. boarding passes, online learning badges, membership cards, gym passes). They are issued by non-qualified trust service providers.

The concrete attributes (e.g. name, address, …) of each credential type (e.g. PID, QEAA, EAA) and sub-type (e.g. birth certificate, boarding pass) will be defined via so-called rulebooks. The rulebook, next to the schema of the credential, might also define sector specific rules (e.g. for banking) and information on if a credential must be revocable or not.

In the table below you will find the high-level requirements overview for each issuer of the different attestation types.

Requirement	PID/LPID	PuB-EAA	QEAA	EAA
Register as Issuer (become trusted actor in the ecosystem)	✅	✅	✅	✅
User Identity Proofing with Level of Assurance High before issuance	✅	✅ (can use PID for LoA)	✅ (can use PID for LoA)	- (depends on the rulebook)
Authentication of the wallet before issuance	✅	✅	✅	✅
Support credential standards ISO/IEC 18013-5 & SD-JWT VC (IETF)	✅	✅	✅	✅
Support credential standards W3C VC VCDM v2.0	-	-	-	✅
Support for the OID4VCI/ISO-18013-7 issuance protocols	✅	✅	✅	✅
Issued credential must contain a status (e.g. revocation if validity > 24h)	✅	✅	✅	- (depends on the rulebook)
Ensure alignment with attestation rulebook	✅	✅	✅	✅
Provide embedded disclosure policies which specify who (relying party) may receive the credential	-	Optional	Optional	Optional

The Verifier (Relying Party)

Verifiers are **governments and/or businesses that want to request and verify a set of claims about a user (e.g. is over 18).** Verifiers, like Issuers, will need to be registered in order to be trusted by the wallet. They will need to support the required credential exchange protocols like OID4VP/ISO-18013-7 for online verifications and ISO-18013-5 for offline verification depending on their use-case. As well as, be able to interpret the different credential formats and types (e.g. mdoc/mDL, SD-JWT VC IEFT, W3C VCDM v2.0).

In the table below we will see the high-level requirements overview for relying parties depending on if they operate online or offline.

Requirement	Online	Offline
Register as Verifier (become a trusted actor in the ecosystem) and state which attributes you want to request.	✅	✅
Support credential standards SD-JWT VC (IETF) & W3C VC VCDM v2.0	✅	-
Support credential standards ISO/IEC 18013-5	✅	✅
Support for the OID4VP/ISO-18013-7 verification protocols	✅	-
Support ISO-18013-5 verification protocol (offline)	-	✅
Ensure to request only attributes listed during registration	✅	✅
Validate presented credential (signature check, user binding check, rulebook specific checks, ...)	✅	✅
Keep logs relating to an identity matching process and its outcome	✅	-

(max 12 months)		
Support pseudonym authentication (if user identity not required by service)	✅	-
Allow remote presentation via the W3C Digital Credentials API once the API is fully standardised & supported	✅	-

The Wallet Provider

Wallet providers under eIDAS2 are either

- **member states** or
- **certified organisations that offer wallets to users**.

They must only deliver the software (the Wallet Instance) *and* ensure it fulfills all security requirements to reach Level of Assurance "High". They are responsible for issuing Wallet Unit Attestations which are digital credentials stating the technical capabilities of the wallet during the wallet activation process. The attestation will be used in exchanges with other ecosystem participants such as Issuers to establish trust. Also, wallet providers must ensure the wallet supports all required exchange protocols (e.g. OID4VCI) and credential formats (e.g. mdoc/mDL). They must manage the whole lifecycle of wallets from installation, activation, management and uninstallation, while ensuring the user retains sole control over their digital IDs.

Next to the certified wallet providers, there will also be a market for **non-certified wallets for consumers or businesses** use cases where certification is not required. Organisations that already have a strong, trusted user base could enhance their apps with wallet capabilities and thereby become an even stronger focus in the everyday life of their users. Every time users need to access their credentials, they'll open their ID wallet app, deepening engagement and opening moments for value capture. Early movers in industries like **banking and finance, tech and telecommunications, social media and large platforms, travel, education and health care** providers therefore greatly benefit from increased app usage by becoming an everyday identity hub for their users and their digital lives.

In the table below we will see the high-level requirements overview for wallet providers (certified or non-certified).

Requirement	Certified	Non-Certified
Distribute the wallet solution via the official OS app stores or side-loading.	✅	✅
Enforce OS-level user auth	✅	Optional
Prompt user for provider account setup + link account to wallet unit instance	✅	Optional
Use device WSCA or deploy remote HSM for key management	✅	✅
Activate wallet unit only if at least one WSCA/WSCD is certified for LoA.	✅	Optional
Issue Wallet Unit Attestation (WUA)	✅	Optional
Support credential standards ISO/IEC 18013-5 & SD-JWT VC (IETF) & W3C VC VCDM v2.0	✅	No requirement for all types
Support for the OID4VP/ISO-18013-7 verification protocols	✅	No requirement for all standards
Support for the OID4VCI/ISO-18013-7 issuance protocols	✅	No requirement for all standards
Provide Trust Mark View (user can verify certification status)	✅	-
Ingest & user trusted lists	✅	Optional

Publish trust anchor & enable trust processing by other parties (e.g. Issuers)	✅	Optional
Present requested attributes & party details when user interacts with relying parties	✅	Optional
Maintain a transaction log of actions (presentation, issuance) available for users	✅	Optional
Provide backup, recovery, migration options	✅	Optional
Support pseudonyms and passkeys	✅	Optional
Enable Users to create qualified electronic signatures/seals	✅	Optional
Enable issuance & remote presentation via the W3C Digital Credentials API once the API is fully standardised & supported	✅	Optional
Revocation and suspension management (e.g. user or PID provider request revocation)	✅	Optional
Undergo conformity assessment by an accredited body and obtain a certification	✅	-

Should my Organization be an Issuer, Verifier or Wallet Provider?

To understand into which role (Issuer, Verifier or Wallet Provider) your organization falls, let's look at the following:

Issuer

Guiding Question	Do we manage or control data that could be issued as a digital credential?
You're in this role if…	The data your org holds has legal, commercial, or operational value for you, partners, or the market.
Typical Examples	Government authority issuing PIDs, university issuing diplomas, health provider issuing insurance cards.

Note: For more details on the type of issuer your organization might be (PID/LPID, QEAA, EAA) refer to the "Build" section.

Verifier (Relying Party)

Guiding Question	Do we need to authenticate users or validate claims about them?
You're in this role if…	You must check identity attributes or entitlements to deliver a service or meet compliance needs.
Typical Examples	Bank verifying income statements, healthcare provider checking patient data, online platform requiring strong auth.

Wallet Provider

Guiding Question	Do we want to provide end-users with a digital wallet to store and present credentials?
You're in this role if…	You plan to ship and maintain a wallet app/service for users.
Typical Examples	eIDAS2 certified citizen wallets, non-certified enterprise/ consumer wallets bundled with a product or service.

Note: An organization may hold multiple roles at the same time (e.g. acting both as an Issuer and a Verifier).

Build vs. Buy

Now that you have a good understanding of the roles, high-level requirements and use cases, it is time to ask the question of whether you should build your own solution (in-house) or buy an existing one.

There are three options to choose from:

1. **Build apps, buy infra** (only build UI and apps, outsource infrastructure)
2. **Build apps, own infra** (use open source to own the infrastructure)
3. **Build everything** (build and maintain the whole stack in-house)

Each option comes with advantages and disadvantages:

What "build everything" really entails

Implementing an eIDAS2-aligned solution in-house means tackling multiple domains. Teams must implement and stay up-to-date with:

- **Credential standards:** ISO/IEC 18013-5, SD-JWT VC (IETF), W3C VCDM 2.0
- **Exchange protocols:** ISO/IEC 18013-7, OID4VCI, OID4VP
- **Key management:** integrate a KMS or build your own
- **Revocation:** sign/manage/publish Attestation Status/Revocation Lists
- **Data sourcing:** connect authentic sources/DBs for issuance data
- **Disclosure policies:** embed EDPs at issuance; interpret at verification
- **Privacy measures:** e.g. avoid correlating issuance batches
- **Certification management:** access certificates for issuers/verifiers and audits
- … all of this is in addition to a product's own applications and business logic.

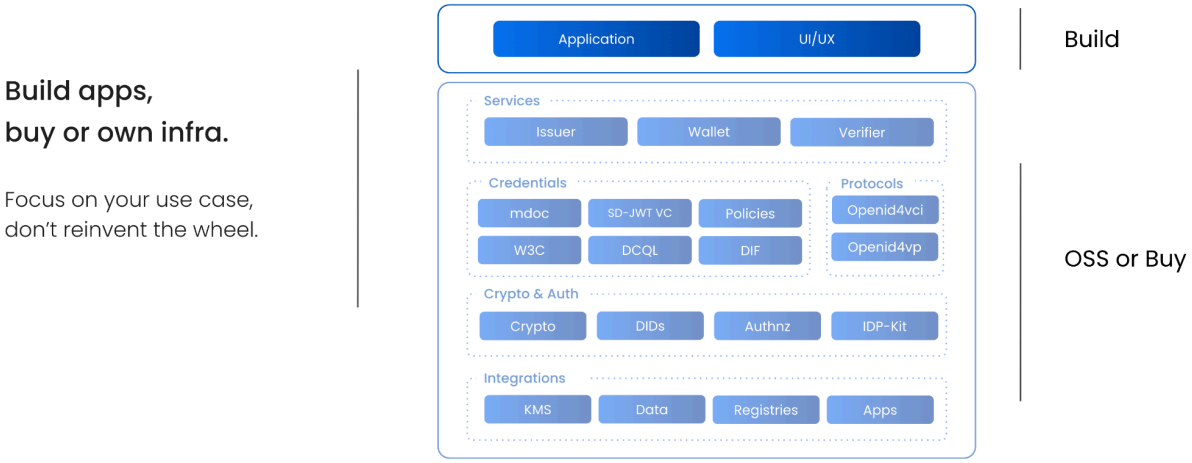
The model most teams adopt: Build Apps, Buy/Own Infrastructure

Governments and businesses must adopt digital ID wallets, but struggle with:

- **Urgency** from regulatory deadlines and competitive/customer pressure
- **Limited talent pool** (protocols & standards) for building in-house
- **Technical complexity** (PKI, KMS, sigs, credentials, protocols) raising failure risk
- **Fast-moving standards** (W3C, OIDF, ISO, IETF, ...) inflating maintenance cost
- **Compliance risks** (e.g. from eIDAS2) increasing audit scope and liability

Most organizations want to **launch applications and solutions quickly without owning technical and regulatory complexity and risks.**

As a result, most organizations use existing infrastructure (open or closed-source) and build custom apps on top (inhouse or with partners). They prefer (open source) infrastructure that can be operated by themselves ("self-managed") to maximize control, while offloading the most significant implementation work and complexity to existing solutions in order to reduce costs, risk and speed up time to market.



A starting point when it comes to open source solutions are e.g. the EUDI Wallet Reference Implementation (B2C wallet app) or the walt.id Community Stack (Issuer, Wallet, Verifier). When it comes to closed-source options you can take a look at the walt.id Enterprise Stack.

Since technology and vendor selection can be complex, we also created a checklist based on how other organizations across industries evaluate their options:

Checklist for your tech evaluation.

Focus on your use case, don't reinvent the wheel.

- ☐ Solution can enable my **use case(s)**.
- ☐ Solution complies with **eIDAS2 required tech standards**.
- ☐ Solution is **open source** / permissive license.
- ☐ Solution allows to mix/match **3rd party infra** (KMS, data, QTSP).
- ☐ Solutions supports required **deployment options**.
- ☐ Solution **integrates with existing systems** & apps.
- ☐ Solution supports various **data sources** (DBs, business systems)
- ☐ Services **onboarding & support** are available.

You can find a detailed checklist for technology and vendor evaluation in the Annex.

Build | Issuer, Verifier, Wallet & Technical Requirements

In this section, we take a closer look at the roles (Issuer, Verifier, Wallet Provider) introduced earlier. We'll explore each role in more detail and outline the specific technical requirements they must meet. This will give you the knowledge for building your chosen use case.

Issuers

PID/LPID Providers (natural/legal person identifiers)

PID providers are organizations appointed by member states to issue PIDs/LPIDs. PIDs act as the core identity data credential which each eIDAS2 wallet must hold in order to be valid. "LPIDs" are the core identity data for legal persons.

The data set in the PID/LPID is officially defined, trusted and acts as the user's "digital ID" across all member states.

The PID:

For a detailed overview of the attributes of a PID, please refer to the section "The PID" at the beginning of this document

The LPID:

Mandatory attributes of an LPID:

- Current Legal Name
- Unique Identifier constructed by the issuing Member State (compliant with cross-border specifications)

Optional attributes of an LPID include:

- Current Address
- VAT Registration Number

- Tax Reference Number
- European Unique Identifier (Directive (EU) 2017/1132)
- Legal Entity Identifier (LEI)
- Economic Operators Registration And Identification (EORI) Number
- Excise Number

Note: The mandatory and optional attributes of a PID/LPID are defined in the annex of the (EU) 2024/2977 regulation.

Organizations that want to become a PID provider need to fulfill the following requirements:

Requirement
Identity proofing and LoA ☐ PID providers must verify the identity of the wallet user at Level of Assurance (LoA) High. ☐ Typical methods include: ☐ In-person or remote document verification ☐ Biometric checks ☐ Liveness tests
Wallet unit attestation verification ☐ Before issuing a PID, the provider must authenticate the wallet unit. ☐ Required checks: ☐ Verify the Wallet Unit Attestation (WUA) signature ☐ Confirm that the WUA has not been revoked ☐ Check that the wallet possesses the private key corresponding to the WUA's public key

- ☐ Validate the properties of the Wallet Secure Cryptographic Device (WSCD) to ensure LoA High.

Issuance protocol and formats

- ☐ Implement the OpenID for Verifiable Credential Issuance (OID4VCI) protocol with the HAIP profile.
- ☐ Support credential formats:
  - ☐ ISO/IEC 18013-5
  - ☐ SD-JWT VC (IETF)
- ☐ Support ISO/IEC 18013-7 for mdoc remote flows.
- ☐ Ensure the credential is cryptographically bound to the wallet's WSCD.
- ☐ Embed the wallet's public key into the credential and sign it (provider action).

Status management & revocation

- ☐ Maintain a revocation mechanism.
- ☐ Publish status information (without access control) so relying parties can check validity:
  - ☐ Attestation Status Lists or an Attestation Revocation List mechanism
- ☐ Align PID validity with WUA status:
  - ☐ Because Article 5 of the implementing regulation requires revoking a PID if the wallet unit is revoked, the PID's validity period must not exceed that of the WUA.
- ☐ Support:
  - ☐ Short-lived credentials (validity < 24 hours)
  - ☐ Continuous status monitoring (WUA gets revoked, PID should also be revoked)
  - ☐ Revocation on user request

Registration and trust lists

- ☐ Register as a PID provider with a national Registrar.
    - ☐ Obtain an access certificate and have the provider's trust anchor published on the relevant trusted list.
- ☐ Enable verification by relying parties:
    - ☐ Publishing the trust anchor allows relying parties to verify signatures over PIDs
- ☐ Include the access certificate in the OID4VCI issuer metadata.
- ☐ Sign the issuer metadata with the private key corresponding to the access certificate.
- ☐ Wallet usage:
    - ☐ The wallet uses this information to verify the authenticity of the provider.

PID Content and Data Integrity

- ☐ Ensure alignment with PID Rulebook which specifies structure, type, identifiers, logical organization, encoding, and metadata for mandatory and optional PID attributes.
- ☐ Ensure that all unique elements within a PID have values that are unique across all PIDs issued by that provider.
- ☐ Ensure that the attributes attested in the PID are valid for the identified PID subject at any point in time during the PID's validity period.

Privacy Enhancing Measures for Presentation

- ☐ When issuing in batch, providers must ensure timestamps do not reveal that PIDs come from the same batch, e.g., by making timestamps sufficiently imprecise to support herd privacy.
- ☐ Implement a policy specifying which method to limit PID presentations (e.g., Once-only, Limited-time, Rotating-batch, or Per-Relying Party attestations).

PuB-EAA and QEAA providers

PuB-EAA providers are public-sector bodies (public authorities) that want to issue their official documents as digital credentials. These digital credentials will hold the same legal status as their paper originals.

Examples include:

- **Government authorities** - Ministries, Registries, Municipalities
- **Civil registries** - Birth certificates, marriage certificates, death certificates
- **Immigration & residence authorities** - Passports, visas, residence permits
- **Tax authorities** - Tax IDs, income/tax reports
- **Social security agencies** - Social insurance numbers, health cards
- **Driver licensing authorities** - Driving licenses, vehicle registrations
- **Public universities (for diplomas with legal effect)** - Degrees recognized in law

QEAA providers are certified private businesses or organizations that want to issue digital credentials containing official and verified data sets from public authorities (authentic sources). QEAA providers need to be Qualified Trust Service Providers, otherwise their issued digital credentials are EAAs from an eIDAS2 point of view.

Examples include:

- **Identity Verification Companies (IDVs)** - Postal identity services or remote-ID providers authorized to attest identity/residence as digital credentials (e.g., Post-ID/Video-ID operators).
- **Accredited testing & inspection bodies (TIC)** - Roadworthiness/vehicle inspection centers, metrology & conformity-assessment labs issuing statutory certificates.
- **Corporate service providers acting on official data** - Company registrars' agents or trust/corporate service providers attesting director/representative roles and UBO status against the business register.
- **Accredited private universities / schools (state-recognized)** - Degrees/diplomas with legal effect.

- **Notaries / civil-law notaries** - Notarial deeds, certified copies, company formation documents, or powers of attorney.

Organizations that want to become a PuB-EAA or QEAA provider need to fulfill the following requirements:

Requirement
Identity proofing and LoA ☐ QEAA and PuB-EAA providers often need to verify the user's identity before issuing a QEAAs. ☐ They may use the user's PID to perform this verification at LoA High. ☐ PuB-EAA providers, which are not QTSPs, nevertheless rely on their qualified certificate to sign attestations. *PuB-EAA providers, which are public sector bodies (such as government agencies) responsible for issuing electronic attestations of attributes, are not themselves Qualified Trust Service Providers (QTSPs). However, to ensure the trustworthiness and legal effect of the attestations they issue, a PuB-EAA provider obtains a qualified certificate from a QTSP. This qualified certificate then allows the PuB-EAA provider to legally and securely sign their attestations. When a third party (Relying Party) verifies such an attestation, they check the signature of the PuB-EAA provider (which is based on the certificate issued by the QTSP) and also verify the QTSP's certificate*
Wallet unit attestation verification ☐ Before issuing a QEAA and PuB-EAA attestation, the provider must authenticate the wallet unit. ☐ Required checks: ☐ Verify the Wallet Unit Attestation (WUA) signature. ☐ Confirm that the WUA has not been revoked. ☐ Check that the wallet possesses the private key corresponding to the WUA's public key.

- ☐ Validate the properties of the Wallet Secure Cryptographic Device (WSCD) to ensure LoA High.

Issuance protocol and formats

- ☐ Implement the OpenID for Verifiable Credential Issuance (OID4VCI) protocol with the HAIP profile.
- ☐ Support credential formats:
  - ☐ ISO/IEC 18013-5
  - ☐ SD-JWT VC (IETF)
- ☐ Support ISO/IEC 18013-7 for mdoc remote flows.
- ☐ Ensure the credential is cryptographically bound to the wallet's WSCD.
- ☐ Embed the wallet's public key into the credential and sign it (provider action).

Status management & revocation

- ☐ Maintain a revocation mechanism.
- ☐ Publish status information (without access control) so relying parties can check validity:
  - ☐ Attestation Status Lists or an Attestation Revocation List mechanism.
- ☐ Support:
  - ☐ Short-lived credentials (validity < 24 hours).
  - ☐ QEAA and PuB-EAA revocation on user request.
- ☐ Optional:
  - ☐ If revocation chaining (revoking attestations when the WUA is revoked, like PIDs) is used, the attestation's expiration must not exceed the WUA's expiration used during issuance and continuous status monitoring (WUA gets revoked - Attestation should also be revoked) must be performed.

Registration and trust lists

- ☐ Register as a QEAA and PuB-EAA provider with a national Registrar.
    - ☐ Obtain an access certificate and have the provider's trust anchor published on the relevant trusted list.
- ☐ Enable verification by relying parties:
    - ☐ Publishing the trust anchor allows relying parties to verify signatures over QEAA and PuB-EAAs.
- ☐ Include the access certificate in the OID4VCI issuer metadata.
- ☐ Sign the issuer metadata with the private key corresponding to the access certificate.
- ☐ Wallet usage:
    - ☐ The wallet uses this information to verify the authenticity of the provider.

QEAA and PuB-EAA Content and Data Integrity

- ☐ Ensure alignment with Attestation Rulebooks which specifies structure, type, identifiers, logical organization, encoding, and metadata for mandatory and optional attributes in the attestation. Each attestation will have their own rulebook.
- ☐ Ensure that all unique elements within a QEAA and PuB-EAA have values that are unique across all QEAA and PuB-EAAs issued by that provider.

Embedded disclosure policies

- ☐ Optionally embed disclosure policies specifying which relying parties may receive the QEAA and PuB-EAAs.
- ☐ When present, the wallet will enforce these policies during presentation.
- ☐ Ensure that relying parties are listed appropriately and that policies comply with data-protection law.
- ☐ Types of policies:
    - ☐ No policy
    - ☐ Authorised relying parties only policy

☐ Specific root of trust
Privacy Enhancing Measures for Presentation ☐ When issuing in batch, providers must ensure timestamps do not reveal that QEAA and PuB-EAAs come from the same batch, e.g., by making timestamps sufficiently imprecise to support herd privacy. ☐ Implement a policy specifying which method to limit QEAA and PuB-EAAs presentations (e.g., Once-only, Limited-time, Rotating-batch, or Per-Relying Party attestations).
Attribute sourcing ☐ Maintain interfaces to authentic sources (e.g., tax authorities, registries) to verify attributes. ☐ When a wallet requests a QEAA or PuB-EAA: ☐ Fetch the attributes from the authentic source. ☐ Ensure the accuracy of the fetched attributes. ☐ Include the verified attributes in the attestation.

Non-Qualified EAA Provider

Non-Qualified EAA Providers are all types of private-sector businesses and organizations that want to issue digital credentials to streamline operations, reduce costs, and improve the user experience.

Examples include:

- **Commerce & Retail** → loyalty cards, memberships, discount programs
- **Banking & Finance** → customer onboarding, KYC-light checks, account access
- **Travel & Hospitality** → hotel check-in, boarding passes, car rentals
- **Events & Entertainment** → concert tickets, festival wristbands, sports passes
- **Education & Training** → course completion certificates, student IDs, online learning badges

- **Workforce & HR** → employee badges, professional training credentials, workplace access
- **Telecommunications & Utilities** → SIM registration, service contracts, customer identification
- **Insurance** → policyholder cards, claims process credentials
- **Mobility & Transport** → public transport passes, bike/scooter rentals, parking permits
- **Clubs & Associations** → membership cards, gym passes, NGO or community access

Organizations that want to become a Non-Qualified EAA provider need to fulfill the following requirements:

Requirement
Identity proofing and LoA ☐ Identity proofing is not fixed by the ARF; it's set by the applicable Attestation Rulebook / sectoral framework for that EAA. ☐ When identity proofing is required, providers can leverage the user's PID to identify/authenticate at LoA High by verifying PID attributes (described in the ARF for QEAA; Rulebooks may allow a similar approach for non-qualified EAAs). ☐ Not all EAAs are person-bound (e.g., vouchers); in such cases, personal identity proofing may not apply.
Wallet unit attestation verification ☐ Before issuing an EAA attestation, the provider must authenticate the wallet unit. ☐ Required checks: ☐ Verify the Wallet Unit Attestation (WUA) signature. ☐ Confirm that the WUA has not been revoked.

- ☐ Check that the wallet possesses the private key corresponding to the WUA's public key.
- ☐ Validate the properties of the Wallet Secure Cryptographic Device (WSCD) to ensure LoA High or Substantial depending on the attestation type issued and the providers own issuance policies.

Issuance protocol and formats

- ☐ Implement the OpenID for Verifiable Credential Issuance (OID4VCI) protocol with the HAIP profile.
- ☐ Support credential formats:
  - ☐ ISO/IEC 18013-5
  - ☐ SD-JWT VC (IETF)
  - ☐ W3C Verifiable Credentials Data Model v2.0
- ☐ Support ISO/IEC 18013-7 for mdoc remote flows.
- ☐ Ensure the credential is cryptographically bound to the wallet's WSCD.
- ☐ Embed the wallet's public key into the credential and sign it (provider action).

Status management & revocation

- ☐ The applicable Attestation Rulebook decides revocability. For non-qualified EAAs, the relevant Rulebook must state whether the EAA is revocable and, if yes, which method to use.
- ☐ If revocability is required, maintain a revocation mechanism.
- ☐ Publish status information (without access control) so relying parties can check validity.
- ☐ Use the revocation method specified in the rulebook. Methods can include:
  - ☐ Attestation Status Lists, an Attestation Revocation List or short-lived credentials (validity < 24 hours).
- ☐ Have a revocation policy and revoke on compromise; also revoke when attribute values change and the EAA remains valid for ≥24h.

- ☐ Support revocation of EAA on user request.
- ☐ Optional:
    - ☐ Revocation of EAA if the Wallet Unit is revoked (revocation chaining).

Registration and trust lists

- ☐ Register as a Non-Qualified EAA provider with a national Registrar.
    - ☐ Obtain an access certificate.
    - ☐ For Non-Qualified EAAs the provider's trust anchor is not automatically published on the relevant trusted list compared to other issuer types. The applicable Rulebook must define how Relying Parties obtain and trust your EAA signing trust anchor (e.g., via a domain-specific list).
- ☐ Include the access certificate in the OID4VCI issuer metadata.
- ☐ Sign the issuer metadata with the private key corresponding to the access certificate.

EAA Content and Data Integrity

- ☐ Ensure alignment with Attestation Rulebooks which specifies structure, type, identifiers, logical organization, encoding, and metadata for mandatory and optional attributes in the attestation. Each attestation will have their own rulebook.
- ☐ Ensure that all unique elements within an EAA have values that are unique across all EAAs issued by that provider.

Embedded disclosure policies

- ☐ Optionally embed disclosure policies specifying which relying parties may receive the EAA.
- ☐ When present, the wallet will enforce these policies during presentation.
- ☐ Ensure that relying parties are listed appropriately and that policies comply with data-protection law.
- ☐ Types of policies:

☐ No policy ☐ Authorised relying parties only policy ☐ Specific root of trust
Privacy Enhancing Measures for Presentation ☐ When issuing in batch, providers must ensure timestamps do not reveal that EAAs come from the same batch, e.g., by making timestamps sufficiently imprecise to support herd privacy. ☐ Implement a policy specifying which method to limit EAAs presentations (e.g., Once-only, Limited-time, Rotating-batch, or Per-Relying Party attestations).

Wallet Providers (Certified)

Wallet Provider: A Member State or an organisation mandated/recognised by a Member State that provides the EUDI Wallet solution—operating the wallet for users and issuing wallet attestations/trust evidence for its management and authentication.

Wallet Unit: A specific, user-controlled configuration of a wallet solution—comprising the wallet app (wallet instance), secure cryptographic application and device—provided by a Wallet Provider to an individual user as the vehicle for storing and presenting PID and (Q)EAAs.

Organizations that want to become a Wallet Provider need to fulfill the following requirements:

Requirements
Wallet unit installation ☐ Distribute the certified Wallet Solution via the official OS app stores for installation; if side-loading (made available via somewhere other than the platform's official app stores), provide a way for the user to verify authenticity and clear install instructions.

User accounts and authentication

- ☐ Enforce activation of OS-level user authentication during installation; allow a wallet-specific PIN alternative. WSCA/WSCD must perform user auth before cryptographic operations.
- ☐ Ask the user to set up a provider account (may be pseudonymous) and register authentication methods independent of the device/wallet; link the account to the Wallet Unit (used e.g., for revocation requests).

Wallet unit activation

- ☐ When the wallet unit is opened the first time, the wallet provider requests device capabilities and available WSCA/WSCD characteristics which are needed for the issuance of the Wallet Unit Attestation (WUA).
- ☐ Deploy a WSCA if needed; use a remote HSM if no suitable local WSCD is available.
- ☐ Activation finalises only if the Wallet Unit includes at least one WSCA/WSCD certified for LoA High (per ARF's reference to 2015/1502) and the WUA key is protected by that WSCA/WSCD; ensure key separation when a WSCA/WSCD serves multiple wallet units.

WUA issuance

- ☐ During activation, create, sign, and issue at least one WUA to the Wallet Unit. The WUA (i) describes wallet & WSCD capabilities previously requested, (ii) contains a WUA public key for Proof of Possession (PoP) checks, and (iii) enables revocation checks.
- ☐ The Wallet Unit must present WUAs only to PID/Attestation Providers during issuance (not to relying parties - RPs).
- ☐ Consider "once-only" WUAs to reduce tracking risk.

Protocols for issuance and presentation

- ☐ Implement the OpenID for Verifiable Credential Issuance (OID4VCI v1) and OpenID for Verifiable Credential Presentation (OID4VP v1) protocols with the HAIP profile.
- ☐ Support credential formats:
  - ☐ ISO/IEC 18013-5
  - ☐ SD-JWT VC (IETF)
  - ☐ W3C Verifiable Credentials Data Model v2.0 (optional for wallets)
- ☐ Support ISO/IEC 18013-7 for mdoc remote flows.

Trust mark and certification

- ☐ Provide a Trust Mark view so users can verify certification status of the Wallet Solution.

Trust management

Wallet Unit — ingest & use trusted lists:

- ☐ Download from relevant Trusted List Provider(s):
  - ☐ PID Provider Access CA Trusted List(s)
  - ☐ Attestation Provider Access CA Trusted List(s)
  - ☐ Relying Party Instance (RPI) Access CA Trusted List(s)
- ☐ Issuance: authenticate PID/Attestation Providers by validating their access certificate and chain against the appropriate Access CA TLs; after issuance, verify the credential signature using trust anchors from the relevant Provider TLs.
- ☐ Presentation: authenticate Relying Party Instances by validating their access certificate and chain against RPI Access CA TLs.

Wallet Provider — publish trust anchor & enable trust processing:

- ☐ Ensure the Wallet Provider trust anchors are notified and listed on the Wallet Provider Trusted List so other actors can authenticate your Wallet Units.

- ☐ Ensure the Wallet Solution (incl. Wallet Units) accepts and keeps up to date all required trusted lists (Access CA TLs for PID/Attestation Providers and RPI Access CA TLs).

User privacy & selective disclosure

- ☐ Present the relying party's identity and the exact attributes being requested, and allow the user to approve or deny each attribute group.
- ☐ Implement selective disclosure so the user can share only necessary claims.
- ☐ Respect embedded disclosure policies from attestation providers.

Transaction log

- ☐ Maintain a transaction log accessible via the wallet's dashboard and ensure the user can view, delete or report transactions.

Revocation, backup, recovery and migration

- ☐ Provide mechanisms to revoke the wallet unit or WUA if its security is compromised.
- ☐ Support backup and restore of credentials or migration to another wallet solution.
- ☐ Ensure that key material is securely deleted upon uninstallation, even when using external WSCDs.

Pseudonym and passkey support

- ☐ Enable users to generate unique pseudonyms for relying parties when identification is unnecessary.
- ☐ Support passkeys via W3C WebAuthn; pseudonym attestation ensures each pseudonym is unique per relying party, enhancing privacy.

Note: The detailed specification is forthcoming, but wallet providers should prepare to implement pseudonym attestation and authentication flows.

Qualified electronic signatures/seals

- ☐ Enable Users to create qualified electronic signatures/seals (QES/QSeal) via a QSCD (local, external, or remote).
- ☐ Signature formats:
  - ☐ PAdES (mandatory) per ETSI EN 319 142-1 V1.1.1.
  - ☐ Should also support XAdES, JAdES, CAdES, ASiC.

Digital Credentials API

- ☐ Enable issuance and remote presentations via the W3C Digital Credentials API. However, only once the API is fully standardized and is broadly supported by the relevant browsers and operating systems.

Accessibility and user experience

- ☐ Ensure the wallet application meets accessibility standards (Directive (EU) 2019/882).

Revocation and suspension management

- ☐ Monitor WIA validity and provide functions to suspend, revoke or unsuspend wallet instances.
- ☐ Allow users to request wallet revocation via a channel independent of the device (e.g., web portal).
- ☐ Revoke the wallet if instructed by a PID provider (e.g., when the user dies) after verifying the requestor's status.
- ☐ Inform users promptly of any suspension or revocation and the reasons.

Conformity assessment and obtain certification

- ☐ Follow the Commission's technical specifications for wallet units, undergo a conformity assessment by an accredited body and obtain a certification.

Wallet Providers (Non-Certified)

Non-certified wallet providers are private-sector businesses that want to add to their existing apps or platforms digital-wallet capabilities without the formal eIDAS2

certification. This is ideal for many day-to-day use-cases where high-level compliance is not required.

Examples include:

- **Banking & Finance** → account access, KYC-light, card controls
- **Telecommunications** → SIM/eSIM registration, contract signing
- **Social Media Apps** → age/attribute proofs, creator verification
- **Travel & Hospitality** → boarding passes, hotel check-in, car rentals
- **Healthcare** → patient IDs, e-prescription pickup
- **Education & Training** → student IDs, course badges, exam eligibility
- **Commerce & Retail** → loyalty, memberships, age-gated purchases
- **Events & Entertainment** → tickets, passes, backstage credentials
- **Mobility & Transport** → transit passes, bike/scooter rentals, parking
- **Workforce & HR** → employee badges, building/IT access

Organizations that want to offer non-certified wallets need to fulfill the following requirements:

Requirements
User accounts and authentication (optional) ☐ Enforce activation of OS-level user authentication during installation; allow a wallet-specific PIN alternative. WSCA/WSCD must perform user auth before cryptographic operations. ☐ Ask the user to set up a provider account (may be pseudonymous) and register authentication methods independent of the device/wallet; link the account to the Wallet Unit (used e.g., for revocation requests).
Wallet unit activation (optional) ☐ When the wallet unit is opened the first time, the wallet provider requests device capabilities and available WSCA/WSCD characteristics which are needed for the issuance of the Wallet Unit Attestation (WUA). ☐ Deploy a WSCA if needed; use a remote HSM if no suitable local WSCD is available.

- ☐ Activation finalises only if the Wallet Unit includes at least one WSCA/WSCD certified for LoA High (per ARF's reference to 2015/1502) and the WUA key is protected by that WSCA/WSCD; ensure key separation when a WSCA/WSCD serves multiple wallet units.

WUA issuance (optional)

- ☐ During activation, create, sign, and issue at least one WUA to the Wallet Unit. The WUA (i) describes wallet & WSCD capabilities previously requested, (ii) contains a WUA public key for Proof of Possession (PoP) checks, and (iii) enables revocation checks.
- ☐ Consider "once-only" WUAs to reduce tracking risk.

Protocols for issuance and presentation

- ☐ Implement the OpenID for Verifiable Credential Issuance (OID4VCI v1) and OpenID for Verifiable Credential Presentation (OID4VP v1) protocols with the HAIP profile.
- ☐ Support credential formats (one or all depending on the use-case):
  - ☐ ISO/IEC 18013-5
  - ☐ SD-JWT VC (IETF)
  - ☐ W3C Verifiable Credentials Data Model v2.0
- ☐ Support ISO/IEC 18013-7 for mdoc remote flows if the wallet supports the mdoc credential format.

Trust management (optional)

Wallet Unit — ingest & use trusted lists:

- ☐ Download from relevant Trusted List Provider(s):
  - ☐ Attestation Provider Access CA Trusted List(s)
  - ☐ Relying Party Instance (RPI) Access CA Trusted List(s)
- ☐ Issuance: authenticate Attestation Providers by validating their access certificate and chain against the appropriate Access CA TLs; after issuance,

verify the credential signature using trust anchors from the relevant Provider TLs.

- ☐ Presentation: authenticate Relying Party Instances by validating their access certificate and chain against RPI Access CA TLs.

User privacy & selective disclosure

- ☐ Present the relying party's identity and the exact attributes being requested, and allow the user to approve or deny each attribute group.
- ☐ Implement selective disclosure so the user can share only necessary claims.
- ☐ Respect embedded disclosure policies from attestation providers.

Transaction log (optional)

- ☐ Maintain a transaction log accessible via the wallet's dashboard and ensure the user can view, delete or report transactions.

Revocation, backup, recovery and migration (optional)

- ☐ Provide mechanisms to revoke the wallet unit or WUA if its security is compromised.
- ☐ Support backup and restore of credentials or migration to another wallet solution.
- ☐ Ensure that key material is securely deleted upon uninstallation, even when using external WSCDs.

Pseudonym and passkey support (optional)

- ☐ Enable users to generate unique pseudonyms for relying parties when identification is unnecessary.
- ☐ Support passkeys via W3C WebAuthn; pseudonym attestation ensures each pseudonym is unique per relying party, enhancing privacy.

Note: The detailed specification is forthcoming.

Qualified electronic signatures/seals (optional)

- ☐ Enable Users to create qualified electronic signatures/seals (QES/QSeal) via a QSCD (local, external, or remote).
- ☐ Signature formats:
  - ☐ PAdES (mandatory) per ETSI EN 319 142-1 V1.1.1.
  - ☐ Should also support XAdES, JAdES, CAdES, ASiC.

Digital Credentials API (optional)

- ☐ Enable issuance and remote presentations via the W3C Digital Credentials API. However, only once the API is fully standardized and is broadly supported by the relevant browsers and operating systems.

Accessibility and user experience (optional)

- ☐ Ensure the wallet application meets accessibility standards (Directive (EU) 2019/882).

Revocation and suspension management (optional)

- ☐ Monitor WIA validity and provide functions to suspend, revoke or unsuspend wallet instances.
- ☐ Allow users to request wallet revocation via a channel independent of the device (e.g., web portal).
- ☐ Inform users promptly of any suspension or revocation and the reasons.

Verifiers (Relying Parties)

A relying party — also called a verifier — is a public or private service provider that, with the user's approval, requests and verifies PID or EAA (QEAA/PuB-EAA/non-qualified EAA) attributes from an EUDI Wallet to deliver a service - for example opening a bank account, enrolling at a university, applying for a job, authorising a payment, or identifying yourself for a hotel booking.

Organizations that want to become a Verifier need to fulfill the following requirements:

Requirements
Registration and certificates ☐ Register with the national Registrar to interact with EUDI Wallets. ☐ Register each service (“intended use”) and the exact attributes/attestations you’ll request from wallets. ☐ You may register multiple intended uses; each has its own attribute set. ☐ Obtain an Access Certificate for each Relying Party Instance: ☐ Get the RP Instance access certificate from the Registrar’s Access Certificate Authority (ACA). ☐ Use it to authenticate the RP Instance to Wallet Units when requesting attributes.
Protocols for verification ☐ Implement OpenID for Verifiable Credential Presentation (OID4VP v1) protocol with the HAIP profile. ☐ Support credential formats: ☐ ISO/IEC 18013-5 ☐ SD-JWT VC (IETF) ☐ W3C Verifiable Credentials Data Model v2.0 ☐ Support ISO/IEC 18013-7 for mdoc remote flows. ☐ Each request must include the relying party instance’s access certificate and intermediate certificates up to (but excluding) the trust anchor. ☐ Sign the request with the private key corresponding to the access certificate.
Request only registered attributes

- ☐ The wallet verifies that the requested attributes match those registered. If you request more attributes, the wallet warns the user and may refuse the request.

Validating presented credentials

- ☐ Upon receiving a verifiable presentation, validate the presentation's signature and full certificate chain to the correct trust anchor.
- ☐ Ensure the wallet instance uses the correct private key and that the credential is bound to the wallet unit (user binding).
- ☐ Respect any disclosure policy embedded in the attestation and abide by advice presented by the wallet to the user.
- ☐ For credentials governed by rulebooks (e.g., diplomas, health attestations), implement additional validation rules prescribed by the rulebook.
- ☐ Keep logs relating to an identity matching process and its outcome (incl. user-provided values, the date and time of the process, any relevant supporting documentation, and applicable identifier). Retain for min 6 months, max 12 months.
- ☐ Optional:
    - ☐ Check the credential's status via the provider's status endpoint.

User approval and selective disclosure

- ☐ The wallet must always obtain explicit user approval before presenting data.
- ☐ Do not assume that user approval alone creates a lawful basis for processing; you must have your own legal basis under GDPR.
- ☐ Support selective disclosure so users can decline optional attributes.

Data minimisation and retention

- ☐ Only retain data necessary for the service.
- ☐ Refrain from storing credential contents or transaction logs beyond what is legally required (see section Validating presented credentials above).

- ☐ Intermediaries acting on behalf of relying parties must not store data about the transaction content.

Handling intermediaries

- ☐ If you engage an intermediary, it must register separately as a relying party and obtain its own access certificate.
- ☐ The intermediary registers each of its relying party clients and the attributes they request.
- ☐ Intermediaries must perform all relying-party tasks—requesting, verifying and respecting user consent—on behalf of their clients.

Pseudonym and strong user authentication

- ☐ Support pseudonym authentication when the service does not require the user's identity.
- ☐ Each pseudonym is unique per relying party.

Digital Credentials API

- ☐ Optionally allow remote presentation via the W3C Digital Credentials API once the API is fully standardised and supported by relevant browsers and operating systems.

Annex

List of Adopted Implementing Acts (eIDAS2)

Below is an overview of already adopted regulations grouped into four packages. The first and second packages are important for organisations and businesses that want to act as wallet providers, issuers and/or relying parties. The third package is mostly targeted towards issuers that want issue Q(E)AAs and/or run trust services. The fourth package focuses on qualified electronic signature, seal, time-stamping, registered delivery, validation and preservation services.

Note: The provided list is not yet complete as the Commission is still consulting on additional Implementing Acts right now.

Regulations Package 1:

- (EU) 2024/2979 — Integrity & core functionalities of EU Digital Identity Wallets.
- (EU) 2024/2982 — Protocols and interfaces to be supported by the EU Digital Identity Framework.
- (EU) 2024/2977 — Person Identification Data (PID) & Electronic Attestations of Attributes (EAAs) issued to wallets.
- (EU) 2024/2981 — Certification framework for EU Digital Identity Wallets.
- (EU) 2024/2980 — Notifications to the Commission.

Regulations Package 2:

- (EU) 2025/846 — Cross-border identity matching for natural persons.
- (EU) 2025/847 — Reactions to security breaches of EU Digital Identity Wallets.
- (EU) 2025/848 — Registration of wallet-relying parties.
- (EU) 2025/849 — Submission of information for the EU list of certified wallets.

Regulations Package 3:

- (EU) 2025/1566 — reference standards for verifying the identity/attributes when issuing qualified certificates or qualified EAAs.
- (EU) 2025/1567 — management of remote QSCDs and QSealCDs as qualified trust services.

- (EU) 2025/1568 — peer-review procedures for eID schemes.
- (EU) 2025/1569 — (Q)EAAs and EAAs provided by/for a public-sector body responsible for an authentic source.
- (EU) 2025/1570 — notification of information on certified QSCDs/QSealCDs.
- (EU) 2025/1571 — formats and procedures for annual reports by supervisory bodies.
- (EU) 2025/1572 — format/procedures for notification of intention & verification to start qualified trust services.

Regulations Package 4:

- (EU) 2025/1929 — Lays down rules on binding date and time to data and on accuracy requirements for time sources used for qualified electronic time stamps.
- (EU) 2025/1942 — Defines requirements for qualified validation services for qualified electronic signatures and qualified electronic seals.
- (EU) 2025/1943 — Establishes reference standards for qualified certificates for electronic signatures and electronic seals.
- (EU) 2025/1944 — Sets reference standards and interoperability rules for processes of sending and receiving data in qualified electronic registered delivery services (QERDS).
- (EU) 2025/1945 — Specifies rules for validation of qualified electronic signatures and seals, and of advanced signatures and seals based on qualified certificates.
- (EU) 2025/1946 — Lays down requirements for qualified preservation services for qualified electronic signatures and qualified electronic seals.

Guide for prioritizing use cases

Impact (ROI)	
Category	Description
Increase revenue	Streamline user flows such as by eliminating passwords, forms or multi-step identification processes during onboarding or check-out to increase conversion or lower dropout rates.
Lower costs	Enable online interactions that traditionally required in-person meetings or automate business processes to save costs and resources (e.g. for manual data processing) or even replace third-party services you are currently using to solve related issues with a single, unified solution.
Prevent compliance issues	Facilitate regulatory compliance especially with regards to data protection, eID, AML and other relevant regulations (e.g. GDPR, eIDAS2, AML) to avoid penalty payments and brand damage.
Prevent fraud	Ensure reliable stakeholder verification and introduce tamper proof digital documents to prevent identity theft or document forgery.
Mitigate security risks	Eliminate main risk factors that cause data breaches such as passwords or aggregated data storage.
Strengthen your brand	Offer more seamless user experiences, strengthen security and enhance privacy by giving stakeholders control over their data.
Don’t fall behind	Finally, consider the impact on your business if competitors adopt decentralized identity before you do.

Ease of implementation	
Category	Description
UI/UX	Evaluate how different actors in a use case interact and what it would take to offer users a seamless experience with new products or features.
Data	Identify what kind of data you will use, where and how this data is currently stored, processed and whether it needs to be anonymized.
Deployment	Evaluate how solutions should be deployed, which environments are used and the system requirements for staging, testing and production.
Integration	Evaluate the complexity of the business processes and existing IT infrastructure or applications involved in the use cases.
Ownership	Identify which departments are involved in your use cases and how they make decisions, especially if you require buy-in for implementations.
Buy vs Build	Evaluate whether you will buy or build, potentially using open source solutions, and how worklead will be distributed among internal or external teams.

Checklist: Technology and vendor evaluation

Criteria	Description
Ecosystem Role	Ensure that your solution enables your business to take on the required role (PID, LPID, QEAA, PuB-EAA, EAA Provider, Relying Party or Wallet Provider).
Use Cases	Ensure that your solution fulfills your business requirements and can be used to implement your use cases.
Compliance	Ensure that your solution complies with all regulations required by your business operations (eIDA2, GDPR, AML, TFR…) .
Standards	Ensure that your solution supports all relevant open standards required by eIDAS2. For example, credential standards like Verifiable Credentials (W3C), SD-JWTs (IETF), mDL/mdoc (ISO) or protocols like OID4VCI/VP.
Open Source	Evaluate open and closed source solutions. Many organizations prefer open source solutions in order to maximize control, protect from vendor-related risks, ensure transparency with regards to quality and security and enable faster adoption at lower costs.
Flexibility	Solutions that allow you to mix-and-match or switch between different key management solutions, cloud or trust services (QTSPs) etc. prevent vendor- and technology lock-in and may even be required to comply with regulatory or business requirements (certified KMS, local data storage…).

Deployment	Make sure to pick a solution that is flexible enough to support your operational strategy. Think about how you want to run your ID infrastructure for the next few years. Do you prefer or are you required to self-manage solutions on-premise or in your cloud environment vs. using a managed cloud service?
Integration	Ensure that your solution can integrate with your existing infrastructure and applications. Prevent rip-and-replace where possible as well as vendor- or technology-related lock-in effects.
Services	Ensure to verify whether vendors offer professional services (consulting, development, integration or technical support) either directly or via their partner network.

About walt.id

walt.id offers **holistic open source digital identity and wallet infrastructure** already used by 25K+ developers, governments and businesses globally.

- Website: https://walt.id
- GitHub (Open Source): walt.id identity
- Developer hub: https://docs.walt.id
- Contact: https://walt.id/contact
- Community: LinkedIn — Youtube

Further Readings

- eIDAS2 is here (with Trustscape)
- Decentralized Identity Playbook
- Digital Identity Standards & Ecosystems
- Introduction to Digital Identity
- Monetizing digital identity
- The rise of identity ecosystems
- The role of blockchain for decentralized identity