Decentralized Identity Playbook

All you need to adopt decentralized identity & identity wallets.

This playbook provides you with everything you need to start your journey of adopting decentralized identity and identity wallets. The Playbook elaborates basic concepts and technologies, it explains market drivers, ID ecosystems as well as emerging regulations and helps you navigate technology selection and building pilots of applications, end-to-end use cases and beyond.

Let’s dive in.

Table of contents

Learn | Decentralized Identity 101

Digital identity

This is an eBook about digital identity and decentralized identity. What do these terms mean? You can think of your digital identity as the sum of all the (digital) information that exists about you. For example:

- core identity attributes (name, address or birthday),
- education and work history (diplomas, work records, certificates),
- health or insurance data (medical reports, prescriptions, vaccination passes),
- financial information (bank account information, transaction histories)..

As a result, your digital identity describes who you are in every aspect of your (digital) life. While decentralized identity will be explained later on, for now it is sufficient to know that decentralized identity is simply one (of many) approaches for making digital identity possible.

Brief history of digital identity

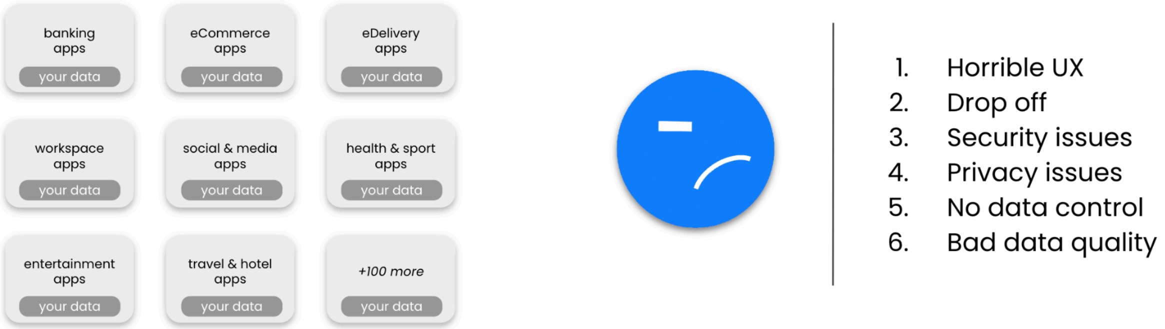
We can distinguish two different digital identity paradigms:

Era of silos (1990s-2020s)

It is no secret that the **internet was built without an identity layer**. However, as the world is growing more digital, we are confronted with seemingly insurmountable issues ranging from cumbersome user experiences to privacy issues, large scale data breaches and our growing dependence on big platforms.

Era of silos

dominated by centralized & federated ID

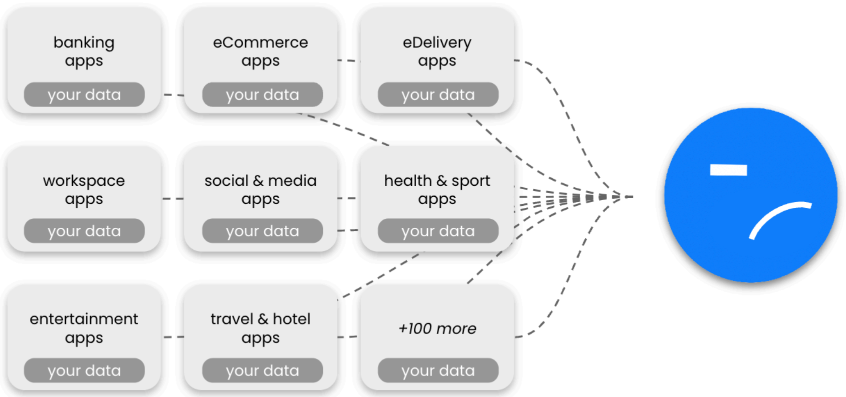


1. Horrible UX
2. Drop off
3. Security issues
4. Privacy issues
5. No data control
6. Bad data quality

Data is siloed, disconnected, fragmented, outdated ...

The underlying reason is that the digital world is built on the premise of data silos, which left us with only two ways to create something like digital identities:

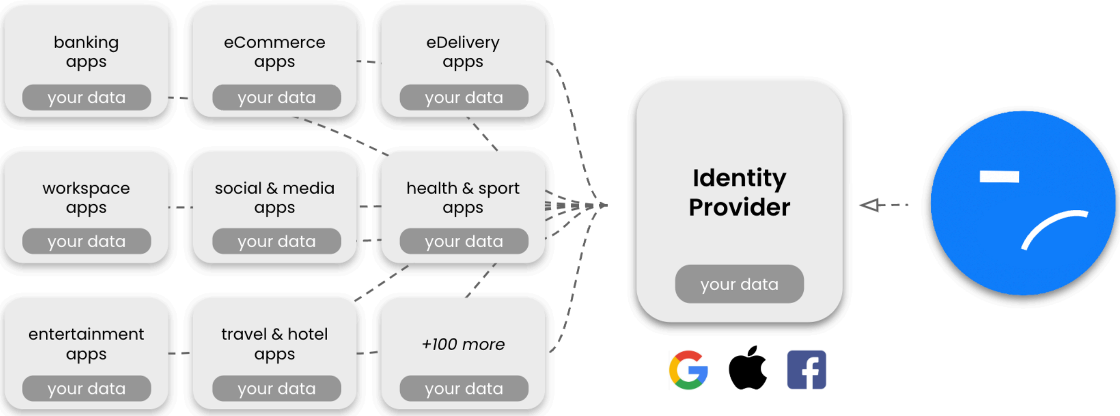
The first approach was to create "**one account per service**": Users pick a username (email), a password and provide information (forms, uploads) which is stored and managed by the service provider.



As a result, the user experience is horrible and accounts are hacked all the time (thanks to passwords). Moreover, users end up with different digital identities for each service they are using and their data is locked in with the service provider. In other words, users' digital identity is fragmented and only exists in disconnected silos.

Over time, a new paradigm emerged called "**Federated Identity**", which was enabled by the rise of platforms like Facebook or Google. While the idea is more or less the same as with the original approach (you create an account and fill it with information about ourselves), there is one big difference:

Instead of creating a new account with every service provider directly, users create one account with a big platform and use it to share data across different services. In short, users give so-called "Identity Providers" their data and ask them to manage and share it with other services.



While Federated Identity offers a better user experience (handle one account instead of many), it aggregates a lot of power in the hands of a few organizations creating lock-in effects, dependence, abuse of power, privacy and compliance issues. Also, this approach has built-in limitations, as it is not possible to build a centralized system that can accommodate every type of identity data for every use case in every industry.

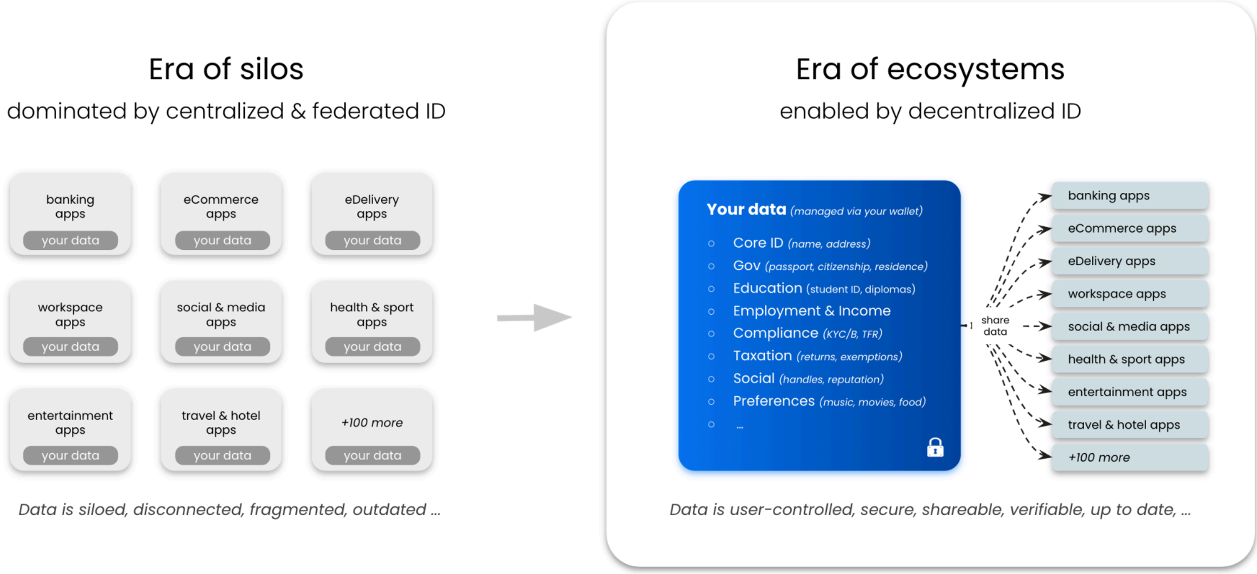
Rise of ecosystems (2020s onwards)

Data silos are the villains of this story. They are the root cause of some of the internet's biggest problems. What would happen if we could avoid data silos?

Digital interactions could become so effortless that it would almost feel like magic. Data could be user-controlled. There would be no worries about privacy violations, independence or about falling victim to data breaches or online fraud.

This is the promise of ID ecosystems and decentralized identity: A digital world in which interactions are effortless and worry-free.

Decentralized identity is simply the next evolutionary step, a new paradigm in which our data and our digital identities are no longer fragmented and locked into silos that are under someone else's control, but only at our own disposal to be securely and privately shared with others.



In short: Decentralized identity is freeing data from silos thanks to a wallet-centric architecture that puts users in control of their data.

You can read more about the evolution of digital identity in this Digital Identity eBook.

Decentralized identity

Decentralized identity (or Self-Sovereign Identity) enables people and organizations to "bring their own identity" and gives them full control over their data. Rather than relying on a central authority to manage their identity (as it is today), anyone can keep their own digital wallet that stores their identity data (e.g. passports, diplomas, work records, financial information). This provides people and organizations with the ability to choose when and with whom they share their data, improving their privacy and security, such as when they sign up for a new service or buy something. By using decentralized identity, anyone can maintain control over their identity data and reduce the risk of identity theft and other types of online fraud.

As a result, decentralized identity enables anyone to prove who they are and potentially anything about them in online and offline interactions.

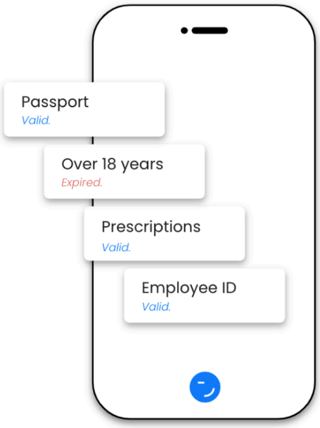
Value

Decentralized identity offers numerous advantages over traditional approaches to digital identity, both for people and organizations.

For people, digital interactions become more effortless which creates better experiences while minimizing the friction of traditional onboarding, such as by eliminating usernames, passwords, forms or traditional identification processes. Also, online fraud and identity theft can be prevented and security improved.

ID wallets

Bring your own identity.



Share any ID data with ease.

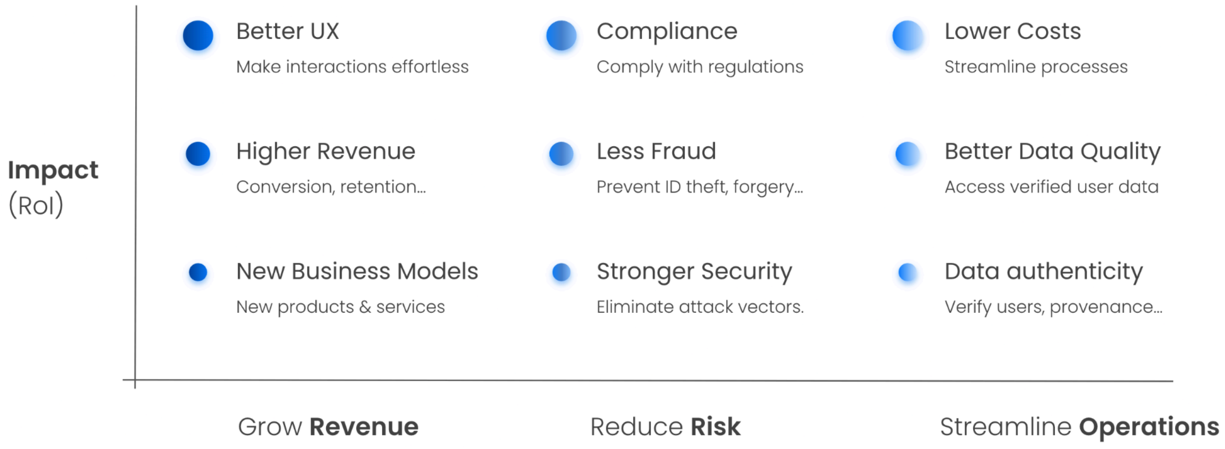
Users control data.
via ID wallets.

1-click data sharing.
for seamless digital interactions.

Compliance by design.
with eID, privacy, AML laws.

Fraud prevention.
via trusted, tamper-proof credentials.

For organizations, like governments and businesses, decentralized identity offers opportunities to grow revenue by improving UX for their customers (e.g. to reduce drop-off rates during user onboarding), strengthen their brand or introduce new products and services. Also, decentralized identity minimizes risk vectors related to compliance, fraud, security and privacy as well as enables organizations to streamline and automate processes to cut costs.



Impact (RoI)

● Better UX
Make interactions effortless

● Higher Revenue
Conversion, retention...

● New Business Models
New products & services

● Compliance
Comply with regulations

● Less Fraud
Prevent ID theft, forgery...

● Stronger Security
Eliminate attack vectors.

● Lower Costs
Streamline processes

● Better Data Quality
Access verified user data

● Data authenticity
Verify users, provenance...

Grow **Revenue** | Reduce **Risk** | Streamline **Operations**

At the end of the day, identity permeates every industry creating opportunities for countless use cases: From official documents required for user onboarding, KYC ("know your customer") or travel to diplomas or certifications required to offer services or apply for jobs to social information for creating unique experiences:

Public Sector	Seamless access to eGov services ...
Banking & Finance	Open bank account & get a loan <1 min ...
Platforms & eCommerce	Sign up & verify your age with 1 click ...
Education & HR	Digital diplomas & effortless job applications ...
Health & Insurance	ePrescriptions & insurance verification ...

Value

Onboard users **faster** | Verify users at **fraction of cost** | **Users love it**

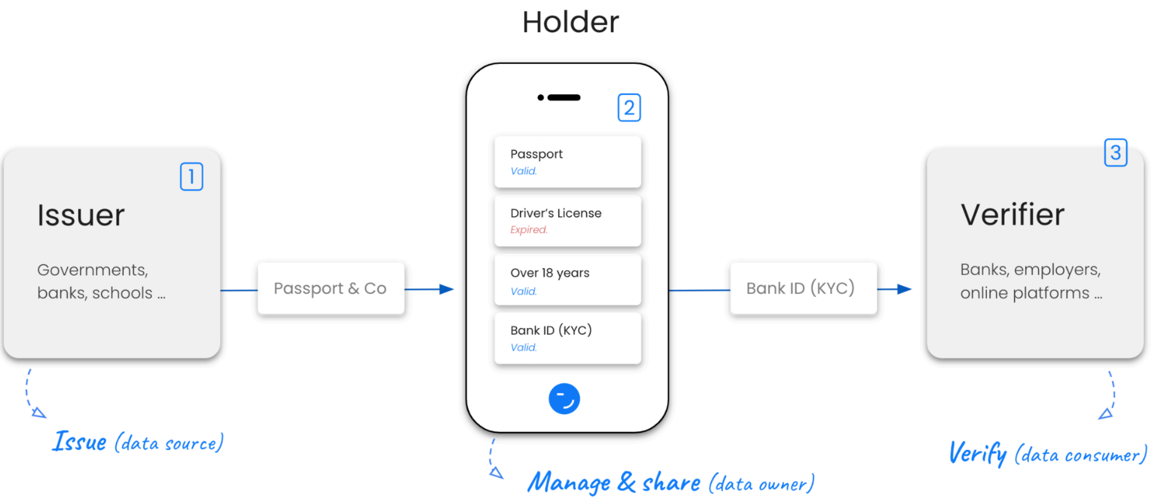
Compliant & secure by design | Trusted, **accurate data**

How it works

Decentralized identity enables governments and businesses to issue identity credentials to their citizens, users or other stakeholders. These credentials are stored in ID wallets and can be easily shared with others. It is like a 3-sided marketplace:

1. **Issuers** issue digital identity credentials (e.g. governments issue passports, universities issue diplomas).
2. **Holders** receive digital credentials (from Issuers) and store them in ID wallets. They control and share their digital credentials with third parties (Verifiers).
3. **Verifiers** rely on identity data to provide products and services, they verify and process credentials provided by Holders.

The so-called "**Trust Triangle**" illustrates these roles:



Note that the same entity can act as Issuer, Holder and Verifier. For example, a university may issue diplomas (Issuer), manage its accreditations (Holder) and onboard students (Verifier).

Read more about decentralized identity in our case studies or eBooks:

- Introduction to Decentralized Identity,
- Me, myself and SSI (in collaboration with BCG),
- eIDAS2 is here (in collaboration with Trustscape).

Concepts & Market

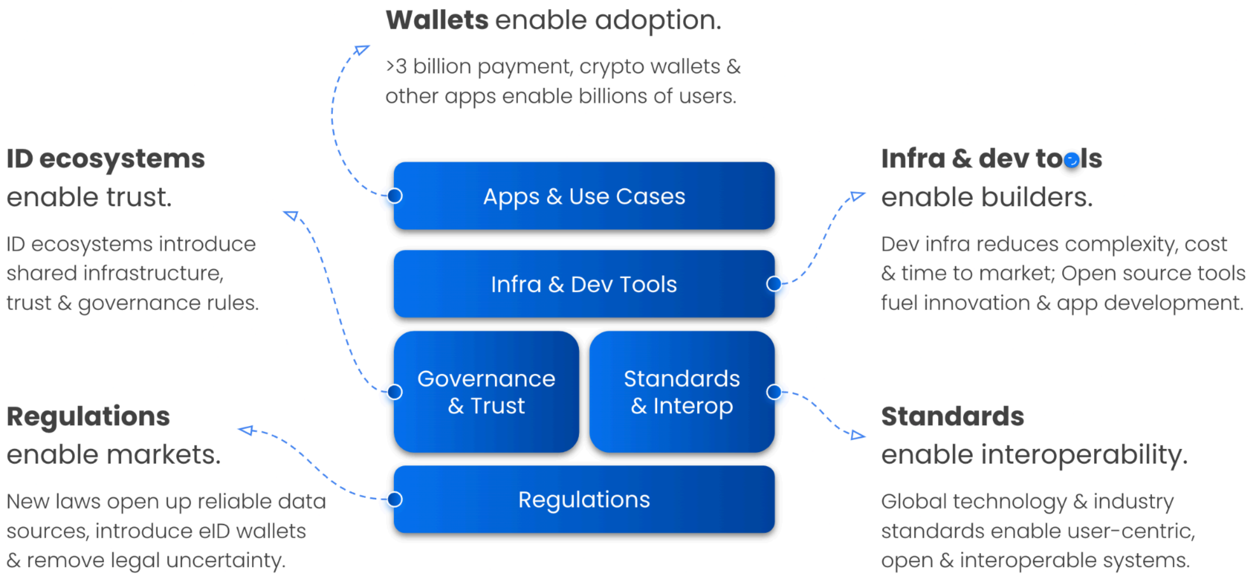
After years of R&D, the adoption of decentralized identity is accelerating fast:

- In 2018, there were only a handful of vendors, one ID ecosystem, no standards and hardly any awareness outside of the close-knit identity community.
- By 2023, three "trillion dollar companies" and leading incumbents of different identity markets announced decentralized identity products. A quickly growing number of startups as well as ID ecosystems emerged and regulators around the globe started to introduce legislation to drive the adoption of ID wallets.

Decentralized identity is on the rise and it is fundamentally changing our digital world. To help make sense of this complex and transformational shift, we created a framework for thinking about decentralized identity's adoption and analyzed the top trends and drivers behind this incredible evolution of a (new) technology category that is creating a multi-billion dollar market.

Framework & trends

Over the last years, five important trends have been coming together to enable the mainstream adoption of decentralized identity and identity wallets: Regulations enable markets. ID ecosystems enable trust. Standards enable interoperability. Developer tooling enables builders. Wallets enable adoption by end users.



Wallets enable adoption.

>3 billion payment, crypto wallets & other apps enable billions of users.

ID ecosystems enable trust.

ID ecosystems introduce shared infrastructure, trust & governance rules.

Infra & dev tools enable builders.

Dev infra reduces complexity, cost & time to market; Open source tools fuel innovation & app development.

Regulations enable markets.

New laws open up reliable data sources, introduce eID wallets & remove legal uncertainty.

Standards enable interoperability.

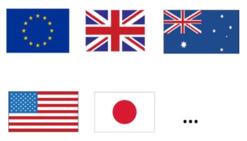
Global technology & industry standards enable user-centric, open & interoperable systems.

The following sections elaborate these five trends one by one:

Regulators enable the market.

Resolution of the industry's "cold start problem".

- Open up data sources. (Issuers/Supply)
- Establish wallet infrastructure. (Holders/Owners)
- Force acceptance. (Verifiers/Demand)



Regulators can make or break new markets. One of the main barriers to the widespread adoption of decentralized identity was the lack of data sources that can issue trustworthy digital identity credentials.

Digital identity regulations are emerging across the globe, spearheaded by the EU with its eIDAS2. These new regulations force data sources (like governments) to provide digital identity credentials and wallets to users and, at the same time, require the private sector (like banks, utility companies, large online platforms) to accept these credentials for onboarding, authentication and identity verification.

As a result, regulations support the solution of the identity industry's "cold start problem" by unlocking the supply side of the market (i.e. Issuers of identity credentials) and by creating a framework and legal certainty for the large-scale adoption of identity wallets and corresponding credential verification solutions.

ID ecosystems enable trust.

Introduce shared trust & governance framework.

- Single source of truth to anchor trust. (technology, PKI)
- Rules to establish trust. (onboarding, LoA)
- Framework to govern the ecosystem. (voting, payment)

Identity ecosystems are a core building block of decentralized identity. By combining technology (shared data registries) with governance frameworks (rules for establishing trust), they enable the shift away from today's centralized identity paradigm which created a world of data silos and with it some of the internet's biggest problems like privacy and compliance issues, lock-in effects, rising fraud and ID theft.

The number of ID ecosystems is growing quickly and led by international organizations (e.g. EU, GLEIF), governments (EU, MENA, APAC, Americas), businesses across industries and major blockchains. As a result, a rich variety of ID ecosystems is emerging to cater to enable use cases across applications, sectors and borders.

Standards enable interop.

Alignment to maximize utility & prevent lock-in:

- Global standards for crypto, DIDs & protocols.
- Ecosystem-specific flavours & extensions.
- Interop plugfests & LSPs.

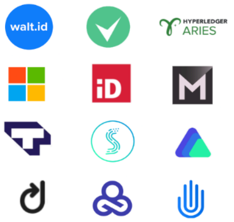
In the early days, vendors invented their own proprietary technology. As a result, solutions were factually centralized and could not live up to the promise of enabling decentralized identity ecosystems in which users can freely share data with anyone. Moreover, there was no backwards compatibility with existing IT infrastructure.

By now, major standardization bodies like the W3C, ISO, IETF, OpenID Foundation, OWF, DIF (etc) are driving standards to a point where interoperability is becoming a reality as demonstrated by the growing number of interop events and production systems.

Dev infra enables builders.

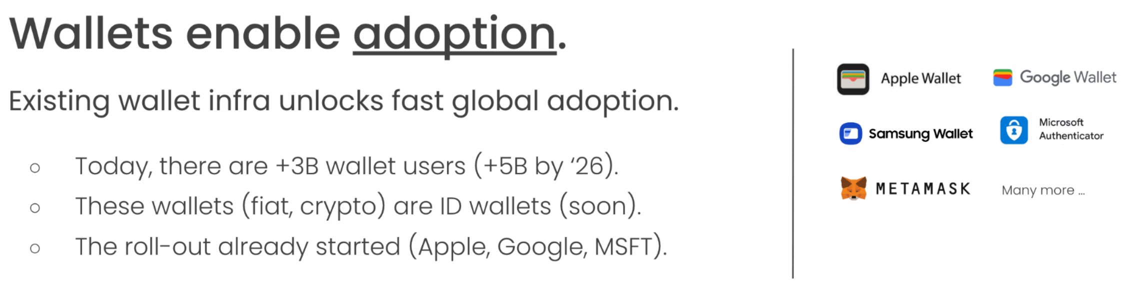
Reduced complexity, time-to-market & cost:

- Anyone can use decentralized ID.
- Healthy, growing vendor ecosystem.
- OSS for frictionless adoption & commoditization.



Developers are at the heart of every technological revolution. Creating infrastructure that makes it easier to build applications and use cases unlocks innovation and real world value by spawning new companies and enabling incumbents to leverage decentralized identity. In addition, we foresee identity becoming a commodity, not at least due to the emergence of open source tooling like The Community Stack we're building at walt.id.

Five years ago, building decentralized identity solutions took organizations months if not years. Today, developers can build production-grade applications and use cases in less than a week.



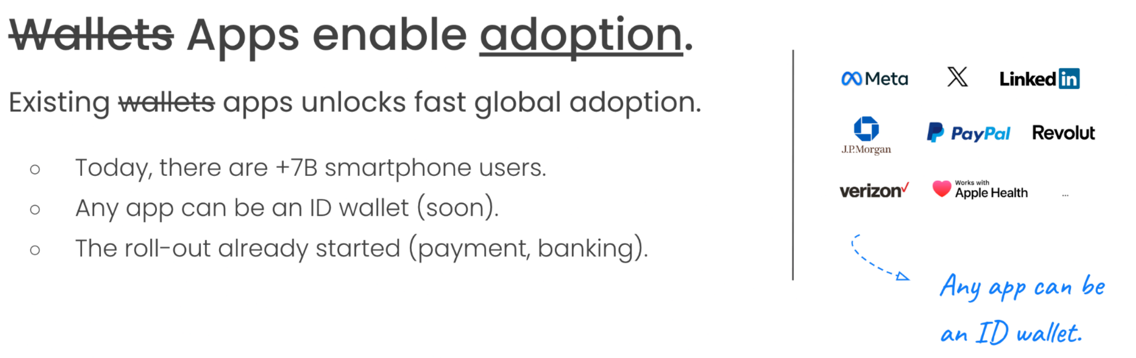
Wallets enable adoption.

Existing wallet infra unlocks fast global adoption.

- Today, there are +3B wallet users (+5B by '26).
- These wallets (fiat, crypto) are ID wallets (soon).
- The roll-out already started (Apple, Google, MSFT).

Apple Wallet
Google Wallet
Samsung Wallet
Microsoft Authenticator
METAMASK
Many more ...

There are roughly three billion payment wallets, a number that is expected to pass five billion by 2026. Digital wallets are becoming ubiquitous and will soon be available to most people on the planet. This means there is a wallet infrastructure that is already in place (for payments and crypto) and can quickly be extended to include digital identity.



~~Wallets~~ Apps enable adoption.

Existing ~~wallets~~ apps unlocks fast global adoption.

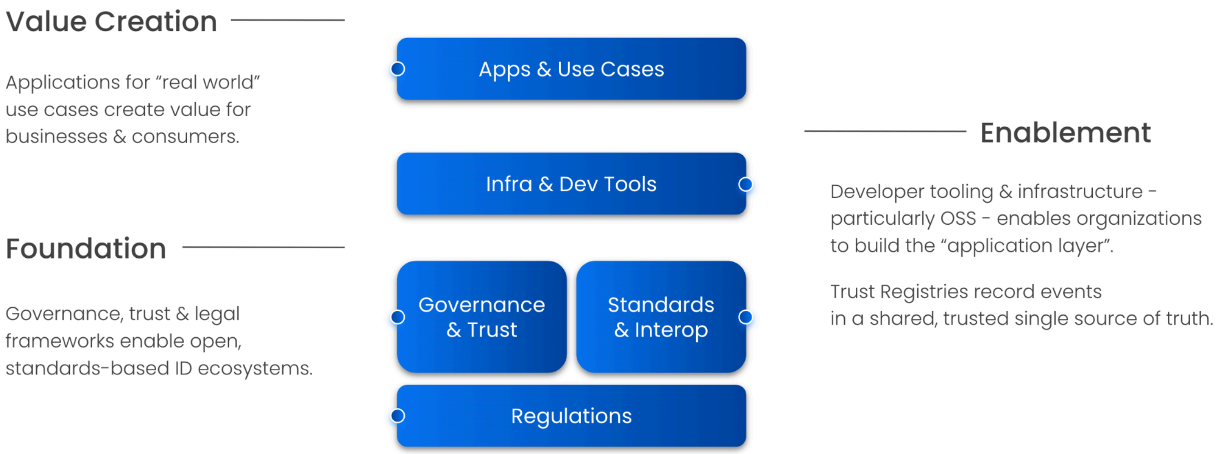
- Today, there are +7B smartphone users.
- Any app can be an ID wallet (soon).
- The roll-out already started (payment, banking).

Meta
X
LinkedIn
J.P.Morgan
PayPal
Revolut
verizon
Works with Apple Health
...
Any app can be an ID wallet.

In fact, not only the leading wallet providers (like Google, Apple) already started to roll-out identity capabilities. Other players like banks, telcos, payment or tech companies - whose applications are already being used by billions - are also working on ID wallets.

These five trends are coming together and form **3 layers**:

- ID ecosystems, regulations and standards create the **foundation**,
- Dev tooling and infrastructure **enable** development of apps and use cases.
- Apps and use cases ensure **value creation** in the economy.



Applications for "real world" use cases create value for businesses & consumers.

Developer tooling & infrastructure - particularly OSS - enables organizations to build the "application layer".

Trust Registries record events in a shared, trusted single source of truth.

Governance, trust & legal frameworks enable open, standards-based ID ecosystems.

The following sections will dive deeper into the most important concepts that underpin the framework and trends that have been outlined above.

ID regulations

Regulators are working on new laws to enable better digital identity systems around the globe often forcing the adoption of ID wallets. For example:

- Europe: The EU passed a new eID law - eIDAS2 - in early 2024, creating a European ID ecosystem based on ID wallets until 2026. In addition, the EU supports market adoption via publicly-funded large-scale projects spanning across various industries, use cases and countries.
- Asia / Pacific: Governments in large Asian countries (e.g. Thailand, Philippines, India) are already working on ID wallets. Japan announced a collaboration with the EU to introduce ID wallets and Australia passed new ID legislation and announced digital identity funding programs.
- MENA: Similar as in Asia, governments in the Middle East are already working on ID wallets with ambitious plans for mainstream adoption.

- **Americas**: The US is rolling out ID wallets in a state-driven approach and recently announced plans for a national ID ecosystem and Canada has been among the first governments to work decentralized identity.

Regulators are pushing for ID wallets and user-centric identity systems for various reasons. For example, to improve government-citizen interactions, streamline or automate processes, cut costs, prevent fraud as well as to enable ecosystems in which citizens can control and use their data in a secure and privacy-preserving way for more seamless and worry-free digital experiences.

Considering that Europe is spearheading global regulatory developments, the following section will analyze and explain EU's eIDAS2 regulation to provide a concrete example for regulatory action:

Example: eIDAS2 - Europe's new eID law

The eIDAS2 regulation is the first global framework introducing digital identity wallets for individuals and organizations, giving them full control over personal data across all aspects of life. This regulation is transforming the digital landscape, influencing global practices, and impacting organizations even outside Europe.

eIDAS2 aims to provide citizens and organizations with secure, private, and user-controlled digital identities to reduce fraud and enable seamless digital interactions across borders. It achieves this by:

- providing citizens with ID wallets to manage and share data with third parties.
- requiring governments to provide ID wallets and issue digital credentials (e.g. passport, driver's license).
- forcing businesses to accept digital credentials for user auth and verification.
- ensuring high security and privacy through standards and certifications.

Note that, eIDAS2 and decentralized identity are related because both use the concept of ID wallets and leverage the same set of technologies. Economically, eIDAS2 creates a market for decentralized identity by mandating digital credentials and ID wallets, solving the industry's "cold start problem." Technically, eIDAS2 aligns with global decentralized identity standards (W3C, ISO, OIDC, IETF).

eIDAS2 has a big **impact on people** as it requires all EU member states to provide ID wallets to their citizens. Thanks to the roll-out of ID wallets, citizens will benefit from more convenient digital interactions with both governments and the private sector, better security and privacy-enhancing mechanisms like selective disclosure. Also, the wallets will enable users to electronically sign documents with legal validity.

Similarly, eIDAS2 has a big **impact on businesses** as they are required to adopt decentralized identity and ID wallets across industries like banking, insurance, eCommerce, healthcare, large online platforms and more. Beyond regulatory compliance, businesses benefit from:

- Better user experience through seamless onboarding.
- Higher revenue from increased user conversion and satisfaction.
- New business models for issuing and verifying credentials.
- Lower costs by streamlining processes.
- Fraud prevention by eliminating ID theft and forgery.
- Improved data quality through verified digital credentials.
- Stronger security by mitigating data breaches and eliminating passwords.

Finally, eIDAS2 **impacts governments** by mandating them to provide ID wallets and digital credentials to citizens. Governments must also enable electronic signatures equivalent to handwritten signatures and accept digital identity credentials for authentication. Beyond compliance, governments benefit from:

- Improved citizen experience in interactions.
- Higher citizen satisfaction through easy data management.
- Interoperability by reusing known citizen information
- Lower costs by streamlining services.
- Reduced fraud and better data quality across organizations.

You can read more about regulations in our eIDAS2 eBook (written with Trustscape).

ID ecosystems

ID ecosystems are important, because the internet lacks a native identity layer. As elaborated, this led websites to create their own local ID systems which led to the emergence of the "walled data gardens" that characterize the “Era of Silos”.

ID ecosystems resolve this problem by enabling users to control and share their data with others. They are open, user-centric systems that enable direct interactions and the free exchange of identity information. While ID ecosystems can be more or less decentralized, the key is that users can control their data without relying on intermediaries like large tech platforms.

In short: ID ecosystems form the foundation for new user-centric identity solutions that free data from silos and make data user-controlled, easily shareable and reliably verifiable.

How do ID ecosystems work?

Identity ecosystems create trust between people and organizations that typically don’t know each other. They have two major components: "Trust Registries" and "Governance and Trust Frameworks".

Trust Registries enable the verification of identity data, serving as the single source of truth and can be implemented with different technologies and levels of decentralization (e.g. Domain Name Service, traditional PKIs, permissioned blockchains, public blockchains/L1/L2s).

There are different types of Trust Registries for different purposes. For example:

- Organization Registries: Verify information about organizations acting as Issuers or Verifiers.
- Schema Registries: Establish standards for data semantics and models.
- Revocation Registries: Manage and verify credential lifecycle.

Governance and Trust Frameworks are like the constitution of an ID ecosystem, ensuring trust in identity data from Issuers and other ecosystem participants. They regulate governing bodies and processes, onboarding and accreditation, liability and enforceability, trust and assurance levels, privacy and data protection, security and interoperability standards. Also, these frameworks align with regulations that impact the identity industry, such as GDPR or eIDAS2 in Europe.

You can read more about this topic in our ID ecosystem ebook.

Finally, it's important to mention **incentives**. Since ID ecosystems work like 3-sided marketplaces (Issuers, Holders, Verifiers), the success of ID ecosystems depends on incentive structures, which is where payments come in. Payments are a way to incentivize participants of ID ecosystems particularly the Issuers who act as the supply side of the market. We can differentiate three approaches to payment:

- Direct monetization based on peer-to-peer transactions;
- Indirect monetization via a settlement layer which can be implemented via a wallet-based or a registry-based model;
- Hybrid models that combine peer-to-peer payments with a settlement layer.

While direct monetization models come with strong privacy features, are highly scalable and independent from third parties or external technical infrastructure, this approach comes with downsides such as that they are suboptimal for incentivizing credential life cycle management by Issuers and require consumers to pay for their data which creates barriers for adoption. On the other hand, indirect monetization approaches come with strong incentive structures but introduce privacy, security and dependency challenges.

Outlook

Identity ecosystems are foundational for the future of digital identity. Different use cases and jurisdictions have unique requirements shaped by regulations, customer needs, and business models. As a result, multiple ID ecosystems are emerging, each with distinct Trust Registries, Governance and Trust Frameworks.

You can read more about incentives in our data monetization eBook.

Technologies & standards

Decentralized identity is based on a set of complex technologies and protocols which can be thought of as building blocks that are available in different variations and can be put together in different ways. As a result, there are different “flavors” or ways to implement decentralized identity depending on the business requirements.

The following list outlines some of the most important ones:

- **Cryptographic keys** convey control over digital identities and enable core functionality such as encryption and authentication.
- **Decentralized Identifiers** (DIDs, W3C) establish a public key infrastructure by linking keys to identifiers allowing parties to find and interact with each other.
- **Verifiable Credentials** (VCs, W3C) and **mobile driver’s license/mdoc** (ISO/IEC 18013-5/-7) are the most common “types” of digital credentials. They can be easily and securely shared with and verified by others. (Note that they are never stored on a blockchain due to privacy and compliance reasons.)
- **Selective Disclosure** (SD) and **Zero Knowledge Proofs** (ZKPs) are ways to minimize data exposure. Selective disclosure using SD-JWTs (IETF) is a solid and reliable way to improve users’ privacy that is gaining traction. While ZKPs are a promising technology with a bright future, they not yet broadly adopted due to concerns or lacking certifications of the underlying cryptography,
- **Non-fungible** tokens (NFTs) and **soulbound tokens** (SBTs) are used to tokenize proofs or assets on blockchains. They enable “ownership-based access” such as for holders of tickets or memberships. Also, they enable on-chain proofs that can be processed by smart contracts (without the use of oracles).
- **Data Exchange Protocols** enable the transfer of identity credentials between parties (like Issuer to Holder or Holder to Verifier). Currently, OpenID Connect, the standard that already enables federated identity, is evolving into the most used standard for the exchange of digital credentials. Protocols can enable data exchange online and in-person scenarios (even offline).
- **ID Wallets** store our keys (control) and credentials (identity data). They enable the management and sharing of our identity data via easy-to-use apps.

Finally, note that **different ID ecosystems will require ecosystem-specific “flavors”** of these technologies based on the respective governance and trust frameworks.

The role of blockchain

A blockchain is a decentralized, immutable ledger that records transactions using cryptography, creating a chain of blocks that are linked together.

Here’s a more easy way to think about it:

Imagine a group of people who want to keep track of things they own and things they've done, like a shared record book. Instead of one person keeping the book and being responsible for it, everyone in the group keeps their own copy of the book and every time someone wants to add or change something, everyone else gets a copy of the new book. This way, everyone always has the same information, no one can cheat or change things without everyone else noticing, and there's no need to trust just one person to keep the book safe. That's basically how a blockchain works - it's a shared digital record book that's kept by lots of people, and when someone adds or changes something, everyone else gets a copy of the updated book. This makes it really secure and transparent because everyone has the same information and no one can change things without everyone else noticing.

Why are blockchains important for decentralized identity?

Decentralized identity relies on ID ecosystems, which create trust between people and organizations by ensuring reliable identity data. A key component of these ecosystems are "Trust Registries” which act as shared databases for verifying identity data's provenance, authenticity, integrity, and validity.

Blockchains are a useful technology to create Trust Registries (e.g. Organization Registries) due to their decentralization, immutability, transparency, security and efficiency. They provide a permanent, auditable record without intermediaries. Also, they can be used to enable NFTs or SBTs for diverse use cases like tokenizing proofs or assets in a way that can be processed by smart contracts. However, they are not necessary (ID ecosystems can also be built on e.g. traditional PKI or DNS).

What are the challenges of using blockchains for decentralized identity?

The main challenges of using blockchains in identity systems fall into four categories:

1. **Costs**: Blockchains' strengths like security and decentralization come with transaction fees, which are generally higher than off-chain operations despite becoming cheaper.

2. **Scalability**: Blockchains can introduce scalability issues due to the time required for settling and executing transactions.
3. **Privacy**: Public blockchains' transparency can lead to privacy concerns, as transaction details can be used to infer information through data correlation. It’s crucial to decide what information to handle on-chain vs. off-chain.
4. **Compliance**: Privacy and data protection laws, like the GDPR’s “right to be forgotten,” can conflict with blockchains' immutable nature.

Note that these challenges can be mitigated by using permissioned blockchains.

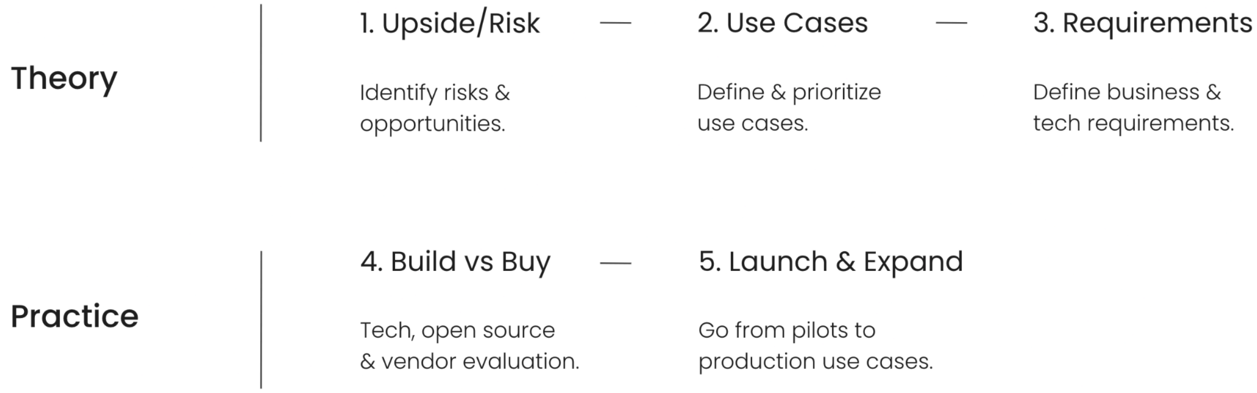
Outlook

Different blockchains have unique advantages suitable for various use cases. With the growing number of ID ecosystems relying on blockchains for Trust Registries, we are heading towards a multi-blockchain future, complemented by traditional PKIs.

You can read more about the role of blockchains for identity in our respective eBook.

Plan | 5 steps to get started

This section outlines a 5-step-approach to help you get started and leverage decentralized identity: From identifying opportunities and use cases to defining requirements and planning the implementation to rolling-out your solutions:



Theory

1. Upside/Risk — Identify risks & opportunities.

2. Use Cases — Define & prioritize use cases.

3. Requirements — Define business & tech requirements.

Practice

4. Build vs Buy — Tech, open source & vendor evaluation.

5. Launch & Expand — Go from pilots to production use cases.

Step 1: Identify opportunities & risks

Start by defining your business opportunities and risks.

One way to segment opportunities is based on whether they make or save money. For example: A better user experience during onboarding or check out can drive brand image and revenue. Also, having machine-readable, verifiable and trusted identity data allows the automation of processes or consolidation of IT infrastructure.

Make money	Revenue Faster, cheaper user onboarding.	Brand Effortless, worry-free user experiences.	Data Get more accurate & trusted data.
Save money	Cost ID becomes cheap (commoditization).	Compliance More secure, private & compliant.	Automation Digitize, streamline business processes.

One way to segment risks is based on whether they are internal or external. For example: You may lose customers to competitors who adopt decentralized identity faster, experience disintermediation or even the disruption of your existing business model. Similarly, adopting too slowly will negatively affect brand and revenue (e.g. considering cumbersome traditional auth and IDV processes) and may introduce compliance issues (e.g. eIDAS2).

Internal	Revenue High drop-off, churn, frustration.	Brand & UX Slow, cumbersome, multi-step flows.	Compliance Security, privacy & compliance risks.
External	Competition Lose customers to faster adopters.	Disintermediation Lose customers by being cut out of the picture.	Disruption Business model no longer makes sense.

To get started, it is helpful to focus on specific categories or areas of your operations.

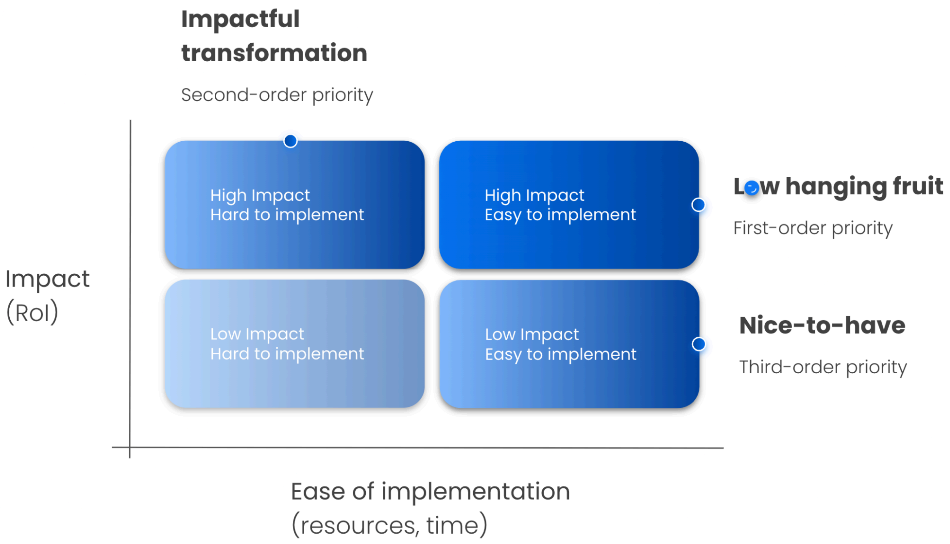
For example:

1. **User experience**: Analyze your customer or stakeholder interactions like onboarding or check out processes.
2. **Data quality**: Do you face data quality or data consistency issues? Are customers providing wrong information, intentionally or due to human error?
3. **Security & Privacy**: Analyze your current security practices in the context of user authentication, identification and the handling of user data. Which user data do you request and store?
4. **Compliance**: Analyze your current practice for complying with regulations in areas like data protection (GDPR, CCPA), anti-money laundering (AML) or Transfer of Funds (TFR)? Will your organization be required to accept ID credentials from ID wallets under eIDAS2 or similar regulations?
5. **Process automation**: Analyze your current strategy for process automation against opportunities created by machine-readable digital ID data.
6. **Start with multi-party processes**: Analyze your business processes with a focus on multi-party interactions, such as those between your organization and groups like customers, employees, suppliers, investors, etc.

Step 2: Select & prioritize use cases

Based on your opportunities and risks, list all use cases 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).



Impactful transformation

Second-order priority

Low hanging fruit

First-order priority

Nice-to-have

Third-order priority

High Impact
Hard to implement

High Impact
Easy to implement

Low Impact
Hard to implement

Low Impact
Easy to implement

Impact (RoI)

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.

Step 3: Define requirements

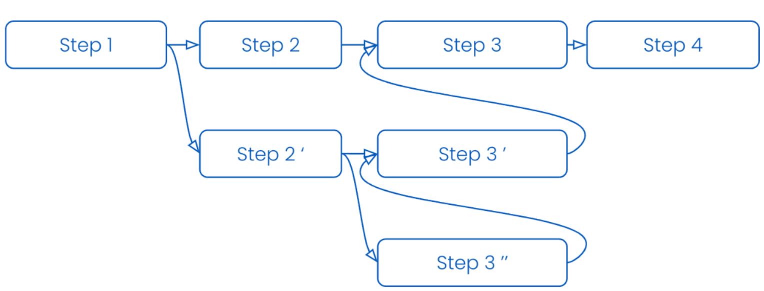
Once you have selected your use cases, it is time to define requirements. The following list guides you through important areas of consideration:

Use cases

Your requirements will differ depending on your use cases. Also, use cases will differ in terms of complexity ranging from simple, reusable to highly customized patterns. The definition of user journeys down to user stories are a helpful way to formalize your use cases and define your business requirements.

1. **Use Cases.**

Formalize your business requirements & processes.

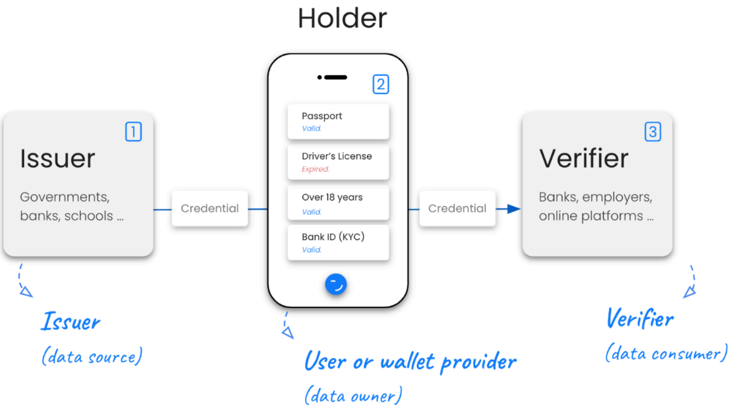


Roles

Your requirements will differ depending on whether your organization is acting as Issuer, Verifier, Holder (or Wallet Provider) or a mix of those.

2. **Roles.**

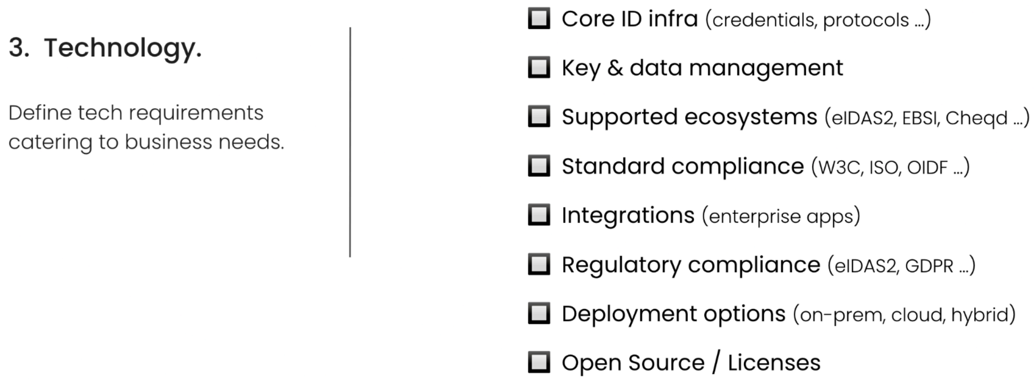
Identify your organization's roles in different use cases.



While most organizations will be adopting two or all three roles described above, some organizations will be more focused on issuance (governments, universities), others on ID wallets (governments, banks, tech) or verification (banks, eCommerce).

Technology

Once you have determined your business requirements, it’s time to define the technical requirements for making your use cases or applications a reality.



3. Technology.

Define tech requirements catering to business needs.

- □ Core ID infra (credentials, protocols ...)
- □ Key & data management
- □ Supported ecosystems (eIDAS2, EBSI, Cheqd ...)
- □ Standard compliance (W3C, ISO, OIDF ...)
- □ Integrations (enterprise apps)
- □ Regulatory compliance (eIDAS2, GDPR ...)
- □ Deployment options (on-prem, cloud, hybrid)
- □ Open Source / Licenses

You can find a detailed checklist for technical requirements in the Annex.

Step 4: Build vs. Buy

Once you understand your requirements, it's time to answer 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:

1. **Build apps, buy infra.**	2. **Build apps, own infra.**	3. **Build everything.**
Build apps, but outsource ID & wallet infrastructure.	Leverage open source & own your infrastructure.	Build and maintain the whole stack in-house.
Fastest, least overhead, comes at cost of dependence.	*Easy to adopt, promise of resilience, control, flexibility.*	*Big investment, high risk of failure, long time-to-market.*

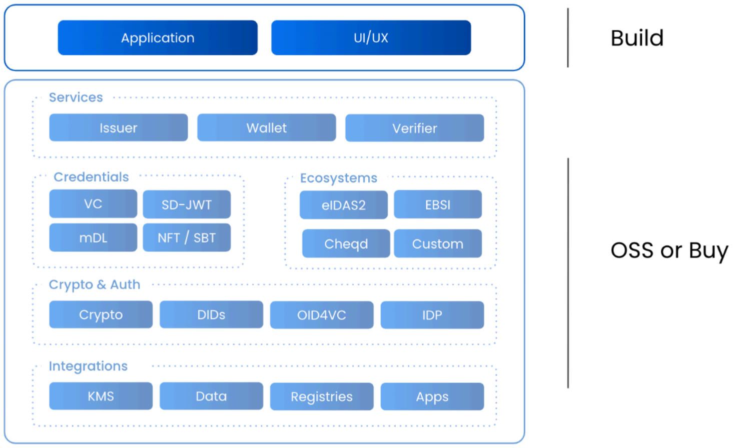
Ultimately, it all comes down to your resources and timeline. Building decentralized identity solutions in-house requires extensive knowledge about a range of emerging regulations, complex technologies and evolving standards as well as a strong technical team capable of implementing, maintaining and continuously extending it. Moreover, building your own solution will significantly slow down time to market.

As a result, we suggest screening the market for solutions that fit your requirements, optionally with the help of experts. Open source solutions are a great way to learn and experiment quickly and without much overhead. Also, they allow you to build your own solution cheaper and faster if you want to be able to control the system - compared to starting from scratch. (You can find instructions on how to build your first apps and use cases with decentralized identity in the next chapter: "Build | Applications and use cases".)

As a result, many organizations follow the approach of buying - open or closed source - infrastructure (libs, SDKs, APIs) and building custom applications on top (inhouse or with partners):

Build apps, buy or own infra.

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



Since technology and vendor selection can be complex, we 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.

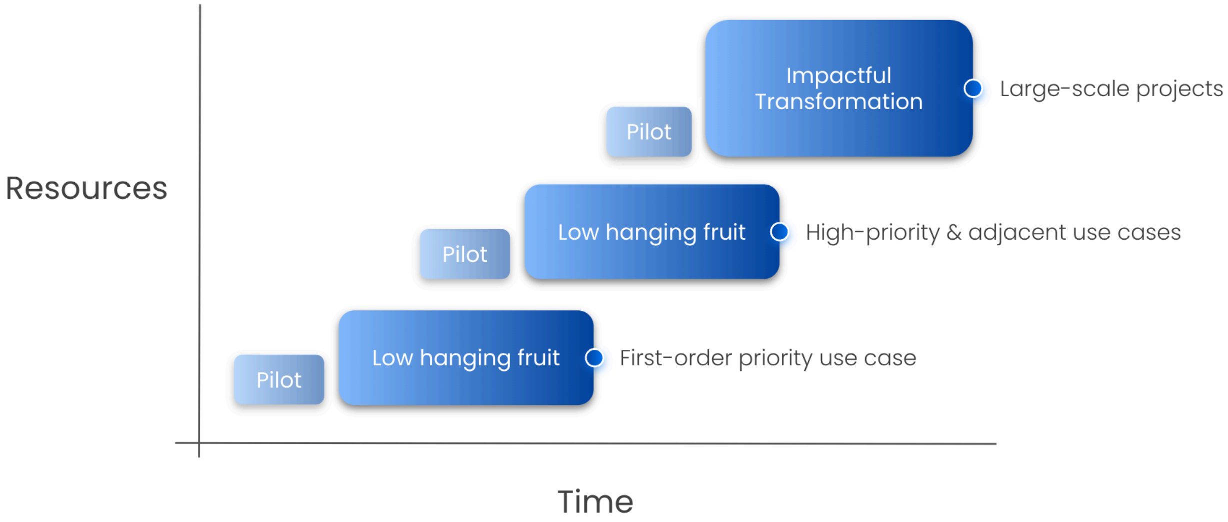
- □ Solution can enable my **use case(s).**
- □ Solution complies with **open standards.**
- □ Solution complies with **new regulations (eIDAS2).**
- □ Solution supports all required **ID ecosystems.**
- □ Solution is **open source** / permissive license.
- □ Solution allows to mix/match **3rd party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

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

Step 5: Launch & Expand

Once you have decided whether you build or buy, it's time to implement use cases.

Start with low-hanging fruits based on your prioritization (Step 3). We recommend an iterative approach by which you start with a pilot and move to production by introducing one product, feature or use case at a time depending on your business priorities and the way you want to communicate with customers.

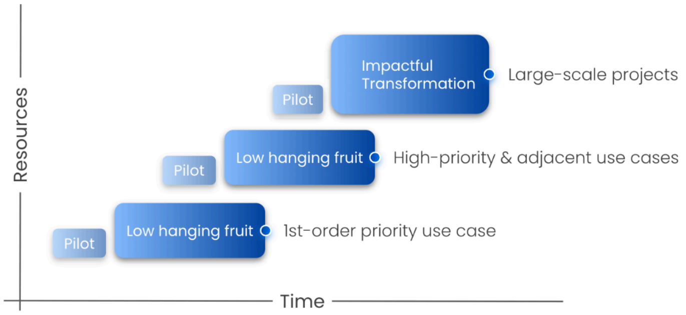


Importantly, we recommend to start with use cases that have high impact but are relatively easy to implement ("low hanging fruits") either because of simpler technical requirements, lower risks (privacy, compliance, brand damage), administrative reasons (existing management buy-in, less departments involved) or others. Often you will find that one use case enables adjacent ones or at least facilitates the implementation of other use cases, such as if they have similar patterns and share technological requirements.

Once you have built up knowledge, successfully delivered first use cases and secured the buy-in of your organization's leadership, you can start tackling high impact projects which are hard to implement ("Impactful transformation").

Low-hanging fruit before **impactful transformation.**

Start with low-risk use cases, expand as you grow capacities & secure organizational buy-in.



In short: Launch low-risks, high-reward use cases. Move from pilot to production and expand use cases as you acquire operational capacities & organizational buy-in.

Build | Applications & use cases

This section will help you to get started by building your first applications and use cases with decentralized identity. This will help you to better understand the technologies and build demos to communicate the benefits within your organization.

Use Case

A use case that impacts every organization is user onboarding. Therefore, we start with a simple end-to-end use case:

1. Imagine a scenario where a person - Lea - visits her government's website.
2. She logs into her account and is offered an ID wallet as well as digital versions of her passport, driver’s license, proof of residence and social security card.
3. She opens (or downloads) an ID wallet and requests the credentials.
4. The government issues the credentials to Lea.
5. Lea visits a bank to open an account.
6. Lea is asked for her information, so shares her government-issued credentials.
7. The bank verifies the credentials and opens an account for Lea.

To build this use case, you will implement solutions for Issuers, Verifiers and a Wallet.

Technology

One way to start building quickly and without much overhead, is to use open source solutions. The following sections will guide you through the required components and steps to set up an end-to-end solution.

Components

Issuer

In our case, the government issues various credentials to Lea. However, this could be any government or business entity that wants to issue verifiable credentials to its users.

When building an issuer, there are few things to consider:

- **ID Ecosystems**: Trust and governments frameworks differ across ecosystems, creating ecosystem-specific requirements e.g. for being accepted as a "Trusted Issuer".
- **Key & DID management**: Issuers should be able to create and manage keys based on different algorithms (e.g. ed25519, secp256k1, secp256r1, RSA) and DIDs from various ecosystems (e.g. did:jwk, did:web, did:ebsi, did:cheqd). Key material should be secured in either a local or external KMS environment like Hashicorp Vault or KMS solutions from Oracle, Google, Azure and AWS.
- **Issuance**: Issuers should be able to sign and issue various credential and signature types (e.g. VCs, mdoc, SD-JWT) and support different data models and use case requirements.
- **Exchange**: Issuers should be able to transfer credentials to users via data exchange protocols like OpenID Connect (OID4VCI) and support different exchange flows and user journeys.

For our example use-case, we will be setting up the issuer using walt.id's open-source APIs. We will issue an eID based on the W3C credential standard using a JWT signature. For the issuer DID, we will be using a did:key.

Please visit our guide here to learn more about setting up the issuer and issuing an eID credential.

Wallet

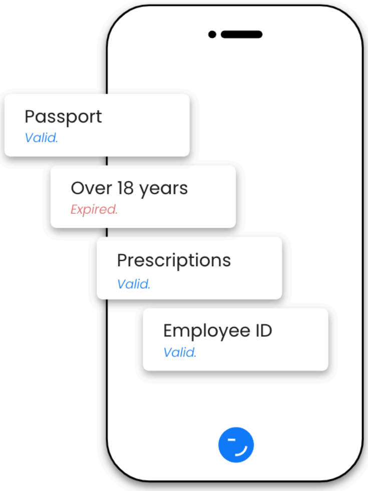
The application with which Lea can store and receive credentials that she can later present to verifiers, e.g. the Bank.

When building a wallet, there are few things to consider:

- **Types**: ID wallets can be standalone apps or embedded within existing apps.
- **Architecture**: Wallets can be custodial, non-custodial or use a hybrid architecture depending on where keys and data are stored (e.g. on-device, server).
- **UX vs. control**: Custodial wallets enable a better, more seamless user experience incl. backup and recovery options. Non-custodial wallets provide users with more control and independence. In hybrid approaches, the app user can decide about their experience.
- **Utility & interoperability**: Wallets should support a diverse set of ID ecosystems and corresponding trust registries, credential types, protocols following open standards.
- **Privacy & trust**: Wallets should support selective disclosure, consent management and prevent fraudulent requests (e.g. by verifying the Verifier).

ID wallets

Bring your own identity.



For our example use-case, we will be setting up the wallet using walt.id's open-source wallet API and white-label web app. With that, we can launch an end-user custodial wallet solution quickly with our own branding. By default the walt.id wallet will be available via the browser but can also be installed as PWA (Progressive Web APP) on IOS and Android. When Lea visits the government website she can pull up her wallet, and create an account if she doesn't have one already and receive the credentials. By default, Lea will get a set of keys and DIDs to which the credentials will be bound. Which type of key or DID is created by default can be configured.

Please visit our guide here to learn more about setting up the wallet and creating the first user account.

Verifier

The Bank which requests credentials from Lea to open a bank account. However, this could be any government or business entity that wants to verify verifiable credentials from their users to provide services or access.

When building a verifier, there are a few things to consider:

- **ID Ecosystems**: As in the case of the Issuer, solutions should support ecosystem-specific requirements e.g. for being accepted as a relying party.
- **Verification**: Verifiers should be able to request and verify various credential types (e.g. VCs, mdoc, SD-JWT), signature types (JWT, SD-JWT) as well as perform checks against Trust Registries to verify provenance, integrity, data models, revocation status among others.
- **Exchange**: As in the case of the Issuer, Verifiers should be able to receive credentials via data exchange protocols like OpenID Connect (OID4VP, SIOP) and support different exchange flows and user journeys.
- **Policies**: Customizable verification policies are useful for automating processes and support different user flows. For our example use-case, we will be setting up the verifier using walt.id's open-source APIs. We will verify the eID issued previously, which is based on the W3C credential standard using a JWT signature.

Please visit our guide here to learn more about setting up the verifier and verifying the eID credential.

Deep Dive | Annex

Guide: Prioritize 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: Definition of technical requirements

Category	Description
Key Management	Keys are the heart of decentralized identity and eIDAS2, because control over keys means control over digital identities. As a result, key management is one of the most important areas to get right: ○ Which solutions and vendors are you using today (if any)? ○ What architecture requirements do you have (mobile, cloud)? ○ What are your security and key management requirements? ○ Which regulatory requirements do you have (e.g. eIDAS2)? ○ Which deployment options do you prefer (on-prem, cloud)? ○ Do you prefer to self-manage the solution or SaaS? ○ Do you require the flexibility to use, mix-and-match or switch between different key management solutions?
Data Management	The handling and management of (personal) data is crucial. Data management is an area where the roles (Issuers, Wallet Provider, Verifier) an organization plans to adopt has outsized impact: Example - Issuer: ○ How do you store and manage data today? ○ Which credential formats and data models do you need? ○ Which auth/data exchange protocols do you need? ○ What are potential security, privacy or compliance issues? Example - Wallet Provider: ○ Where should user data be stored? ○ Do you want to offer different storage options (device, cloud)? ○ Which auth/data exchange protocols do you want to support? ○ How do you handle compliance or consent management? ○ Which UX do you want to offer (e.g. data recovery, backups) Example - Verifier: ○ Which user data do you need for your use case(s)? ○ What is the minimum amount of user data required?

	○ How do you handle compliance or consent management? ○ Do you need to store user data? If so, where and how? ○ Which auth/data exchange protocols do you want to support? ○ What is the impact of your decisions on the user experience?
Standards	Which technical standards do you want to support to ensure interoperability? For example, credentials (W3C VCs, ISO mDL…), selective disclosure (SD-JWTs, ZKPs…) auth protocols (OID4VC…), DID methods (did:key…) among others.
Ecosystems	Which ID ecosystems do you want to support (beyond eIDAS2)? For example, government- or industry-driven ones (EBSI, GLEIF…) or do you want to build your own ecosystem? Which requirements result from the respective governance and trust frameworks? Which Trust Registries or standards do you need to support?
Integration	What are the requirements for integration with your existing identity infrastructure and applications? Which integration options are available? Are there (open source) solutions that already offer integrations with the tools you need?
Deployment	Do you have relevant regulatory or procurement requirements? Do you prefer to self-manage (on-prem, cloud, hybrid) or a managed service (SaaS)?
Licenses & Open Source	Do you have regulatory or procurement requirements with regards to licenses? Are there viable open source solutions? Which open source or business licenses are acceptable?

Checklist: Technology and vendor evaluation

Criteria	Description
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…) .
Ecosystems	Ensure that your solution supports all ID ecosystems you need. Solutions that support multiple ecosystems can ensure that your organization is future-proof considering the emergence of new public and private ID ecosystems across countries and industries.
Standards	Ensure that your solution supports all relevant open standards. For example, credential standards like Verifiable Credentials (W3C), SD-JWTs (IETF), mDL/mdoc (ISO) or protocols like OID4VC (OIDF). Solutions that support different versions or "flavors" of these standards give you more flexibility to address your business requirements and ensure interoperability.
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 (eIDAS2) 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 thousands of developers, governments and businesses globally and across industries.

- Website: https://walt.id
- Developer hub: https://docs.walt.id
- Contact: https://walt.id/contact
- GitHub repo: walt.id identity
- Community: Discord — X/Twitter — LinkedIn — Youtube — GitHub

Further Readings

- Introduction to Digital Identity (eBook)
- Introduction to Decentralized Identity / Self-Sovereign Identity (eBook)
- Introduction to non-fungible (NFTs) and soulbound tokens (SBTs) for identity (eBook)
- NFTs/SBTs vs Self-Sovereign Identity (eBook)
- Monetizing decentralized identity (eBook)
- The rise of identity ecosystems (eBook)
- The role of blockchain for decentralized identity (eBook)
- eIDAS2 is here (eBook in collaboration with Trustscape)
- Me, myself and SSI (eBook in collaboration with BCG)
- A digital twin for everything (eBook in collaboration with BCG)