TrustScape

eIDAS2 is here.

The internet was built without an identity layer. As a result, people have no control over their data and we’ve seen the aggregation of power by large platforms as well as rising levels of identity theft and fraud which has been democratized by AI.

Decentralized identity promises to solve these problems and one of its main drivers are regulations, spearheaded by the European Union and its new eID law: “eIDAS2”. This regulation is a game changer as it forces the adoption of decentralized identity and identity wallets across one of the biggest economic zones in the world.

This document will explain everything you need to know about eIDAS2 and its impact on governments and businesses across industries.

Let’s dive in.

Table of contents

eIDAS2 is here

A brief history of eID law (eIDAS)

The eIDAS (electronic Identification, Authentication and Trust Services) regulation is a EU legal framework that aims to establish a standardized and secure system for electronic transactions and interactions across European member states.

Enforced since July 2016, eIDAS facilitates the recognition and acceptance of electronic identification (eID) and electronic signatures across borders, ensuring their legal validity and trustworthiness. The regulation promotes the use of secure digital identities and electronic signatures, fostering a seamless and trustworthy digital environment for businesses, citizens, and public administrations within the EU, ultimately enhancing cross-border digital services and e-commerce.

Why eIDAS2 was created (why eIDAS was not enough)

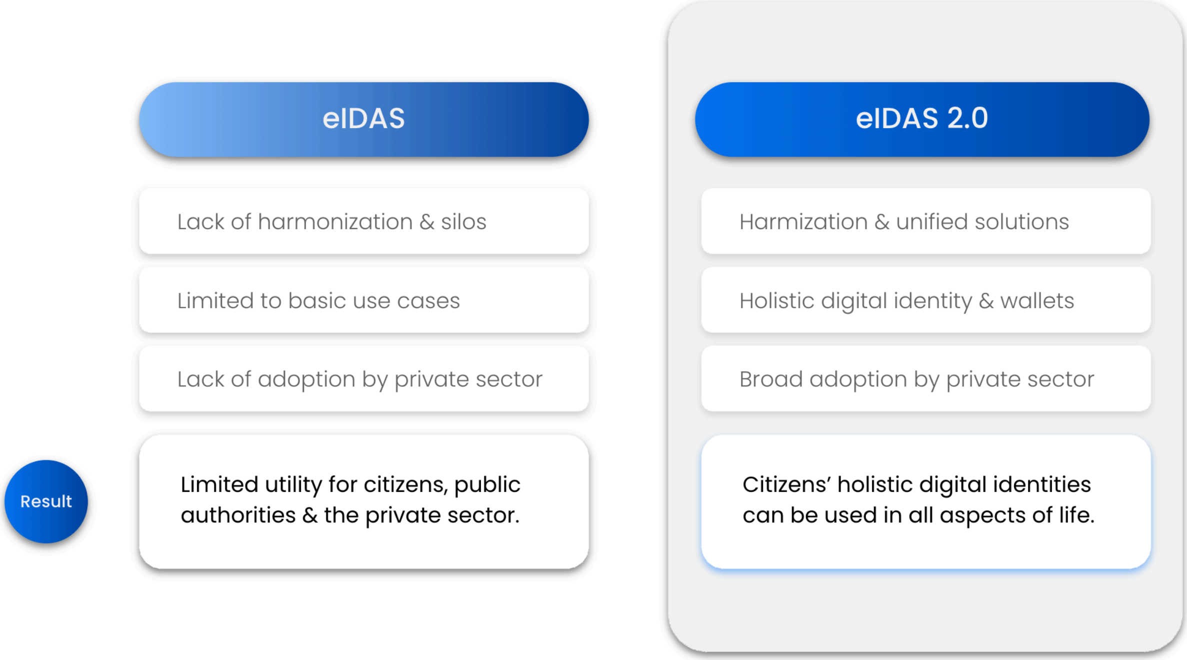
There are three shortcomings of eIDAS that are important to understand:

First, eIDAS gave rise to diverse national implementations of the regulation leading to variations in its application. As a result, the adoption of eIDAS for use cases across borders, industries or organizations has been complex and challenging as demonstrated by the EU eIDAS Revision Impact Study.

Second, eIDAS was inherently limited to a number of trust services, mainly focussing and building on electronic signatures. The regulation did not provide a framework for holistic digital identities, including, for example, education, work, financial, insurance or health related data. As a result, the value of eIDAS for individuals or organizations was mostly limited to facilitate citizen-to-government interactions (e.g. login for eGov portals) and electronically signing documents.

Third, eIDAS strongly relied on physical presence for identity proofing, which was not possible during the COVID crisis and the global lockdown. This resulted in EU member states to interpret the applicable requirements differently which conflicted with the harmonization of the identity and trust foundation which is fundamental for eIDAS.

To sum up, given the lack of harmonization and the inherent limitations of eIDAS, it never achieved broad adoption within the EU (although COVID accelerated its adoption in most countries), particularly not within the private sector. The eIDAS2 regulation was created to resolve these issues.



	eIDAS	eIDAS 2.0
	Lack of harmonization & silos	Harmization & unified solutions
	Limited to basic use cases	Holistic digital identity & wallets
	Lack of adoption by private sector	Broad adoption by private sector
Result	Limited utility for citizens, public authorities & the private sector.	Citizens' holistic digital identities can be used in all aspects of life.

Why eIDAS2 is important

The eIDAS2 regulation is important because it is the **first regulatory framework** on a global level **that introduces digital identity wallets for individuals and organizations** giving them full control over personal data across all aspects of their life. As a result, the eIDAS2 regulation is transforming the digital landscape and is already being copied around the world, endowing it a global impact and even relevance for organizations operating outside of Europe.

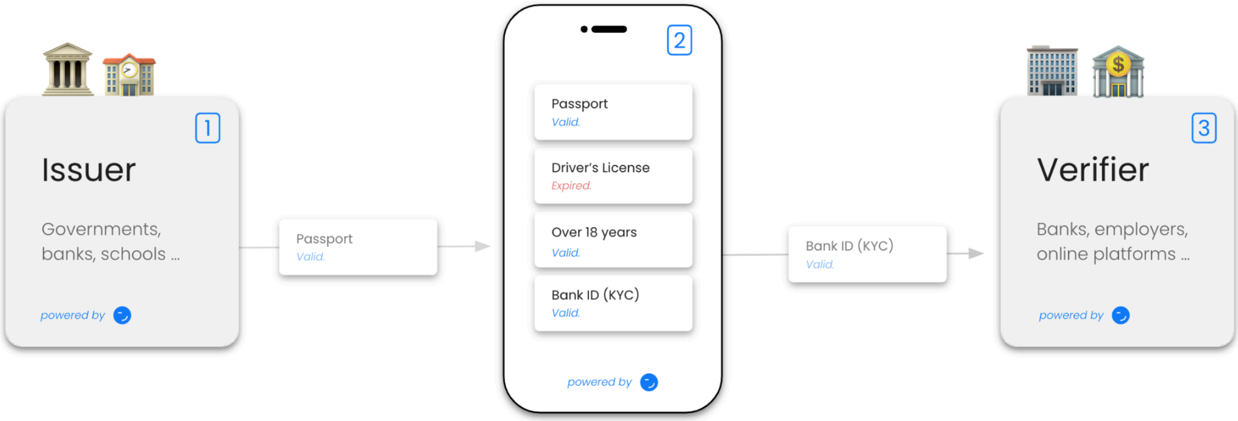
The **main goals of eIDAS2** are to provide citizens and organizations with holistic and user-controlled digital identities that are secure, private and can be trusted to reduce fraud and enable digital interactions across borders, organizations and applications. It will do so by

- **providing citizens with digital identity wallets** to collect, store, manage and share their data with third parties (e.g. governments, businesses)
- **forcing governments to provide digital identity wallets** (with a so-called "PID" based on ISO 18013 and W3C VC) and issue digital identity credentials to citizens (e.g. passport, driver's license, proof of residence, …)
- **forcing businesses to accept digital identity credentials** for authenticating and verifying users (e.g. onboarding, check-out).
- requiring a high level of security and privacy to ensure that citizen information is processed securely, confirmed by a mandatory external audit.

eIDAS2 was successfully **adopted by the European Parliament on the 29th of February 2024**. As a result, governments and many businesses have already started with preparation and implementation to comply with the regulation.

eIDAS2 & Decentralized identity

The main connection between eIDAS2 and decentralized identity is that both approaches leverage identity wallets, which enable users to collect, manage and share their data, putting them into the center of their digital interactions.



From an economic perspective, **eIDAS2 is creating the market for decentralized identity solutions** by forcing member states to provide digital identity credentials and wallets to citizens and, at the same time, requiring the private sector to accept these credentials for user onboarding, authentication and identity verification /

proofing. In other words, eIDAS2 solves the industry’s “cold start problem” by unlocking the supply side of the market (Issuers of ID credentials) and by creating a framework and legal certainty for the large-scale adoption of identity wallets and corresponding credential verification solutions.

From a technical perspective, **eIDAS2 uses the same new concepts** (identity wallets, trust registries…), **technologies and standards** (W3C Verifiable Credentials, IETF SD-JWTs, ISO mobile driver’s license, OpenID Connect…) **that are being used by the decentralized identity industry**. In other words, eIDAS2 is forcing the adoption of mobile digital identity aligned with global and industry standards.

What eIDAS2 means for individuals

TL;DR

The eIDAS2 regulation forces all EU member states to provide identity wallets to their citizens. As a result, **every EU citizen will have an identity wallet with digital identity credentials issued by governments and the private sector by 2026**. This will transform citizens' lives by making digital interactions (online and offline) more seamless, secure and trusted.

In addition to a mobile digital identity, the wallet will allow citizens to securely store credentials such as a driving license, passport or proof of residence which in turn can be used while traveling or applying for a government subsidy.

Given the wallet will store users' digital identity and optionally other identity related documents, security and privacy are of utmost importance. To support stringent security and privacy requirements, digital wallets are required to adhere to privacy by design, zero knowledge proof and selective disclosure principles which will be confirmed with mandatory formal audits and certifications.

Complementary to digital identity capabilities, the digital wallet will enable users to electronically sign documents using a qualified electronic signature. This will allow individuals and organizations to electronically sign documents, which have the same legal value as a handwritten/wet signature using their mobile phones.

Use Cases

Selected use cases below illustrate the impact of eIDAS2 on individuals:

1. eGovernment

Many governments are already providing eServices to their citizens, for example, for tax filings or to request official government attested documents such as proof of residence or a criminal records extract. These services are often dispersed so that a citizen needs to contact the local municipality for one service but use the national eGovernment services for others (like tax filings). Such cumbersome processes and user experiences create confusion and frustration for citizens .

The digital wallet will be able to solve these challenges by offering citizens a seamless and worry-free experience to access government applications, using their digital wallets. Additionally, citizens can request, store and manage their government-issued documents or renew their driving license using their digital wallet in both online and offline interactions.

The capabilities of the digital wallet can also be combined to provide a seamless user experience. For example, when citizens are subject to a police vehicle and identification request, citizens can use the wallet to provide their identity information, driving license, vehicle registration and insurance information electronically to the police officer. To ensure that citizens' information remains secure and protected, the wallet will only disclose the minimum information required after consent provision. Additionally the police officer is identified before any information will be disclosed.

2. Education & Employment

Another great example of how digital identity wallets benefit every individual, is the education and employment journey. For example, students can collect education credentials like diplomas, micro-credentials and certifications from schools, universities or other education providers with their wallets. Also, they can collect and use digital student IDs to access learning portals, claim special services or discounts provided by third parties like museums or banks. Students can also use these credentials to facilitate student mobility, such as when they apply for new study programs or semesters abroad.

Once ready to enter the employment market, following all the steps of the employment process - like job applications, interviews or signing employment contracts - typically requires individuals to disclose (parts of) who they are.

During each step of the job application process, users can selectively disclose their identity using the digital wallet, only providing the information that is required for that specific milestone in the journey. For example, users can disclose their name and place of residence using the digital wallet and augment that with their license plate information when invited for an interview.

When the employer is preparing an employment agreement, additional information can be shared like the exact address, social security number or driving license.

Finally, users can use the wallet to sign the employment agreement in a seamless, low friction experience without having to disclose all identity information immediately or having to fill out multiple documents or forms.

3. **Digital services across industries**

Apart from government interactions or in the context of education and employment, digital identity wallets can be used to facilitate access to potentially any digital product or services: Individuals can use their wallets to seamlessly create accounts and share their information with online platforms, open bank accounts and apply for loans or even travel across the globe providing digital travel credentials, visas or booking confirmations.

Value & Benefits

As illustrated by the use cases, citizens will be able to

- **seamlessly access public and private services** without passwords, forms or cumbersome traditional identity verification processes.
- **control their data across different areas of their lives** (e.g. education, employment, finance, insurance, health care, …).
- **easily share data on their own terms** and in a way that is privacy-preserving without having to handle paper-based documents or identity cards.
- **rely on more secure and trusted digital interactions as** the risk of ID theft, document forgery and other forms of **fraud**, which already create billions in damages every year, **is significantly reduced**.

What eIDAS2 means for businesses

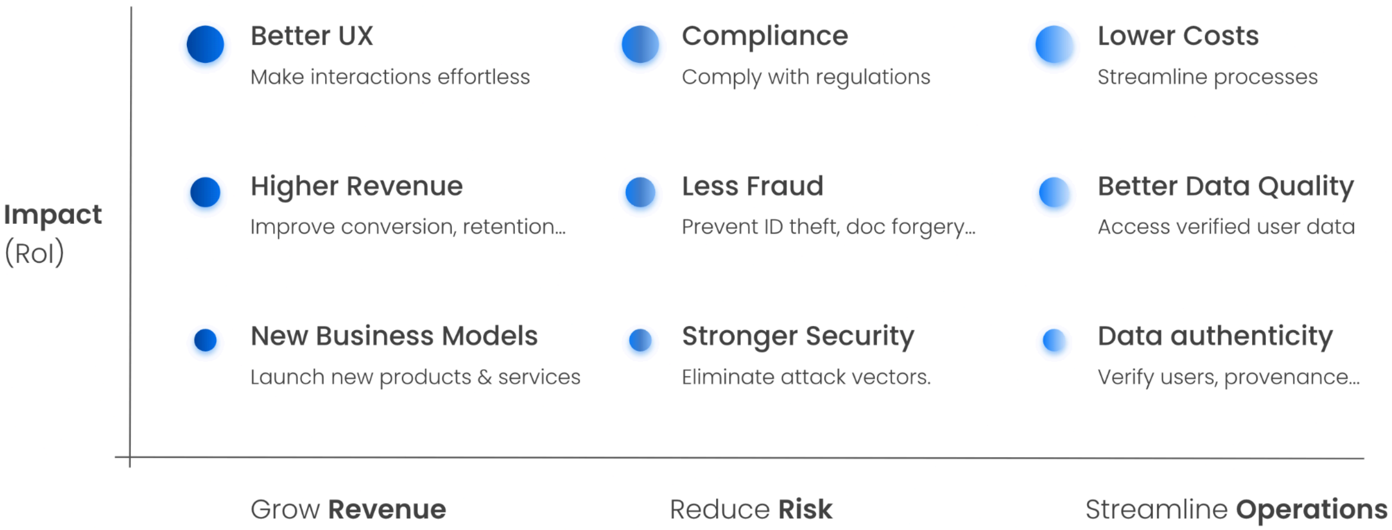
TL;DR

The **eIDAS2** regulation **forces the adoption of decentralized identity and identity wallets for businesses operating in Europe by 2026**. Every organization in every industry will be affected including, banking and financial services, insurance, eCommerce, health care, telcos, tech and cloud services, logistics and supply chain, education, employment, hospitality and aviation among others.

That being said, **regulatory compliance** (eIDAS2, AMLR, TFR) is only one of many reasons why businesses adopt decentralized identity:

- **Better user experience**: Offer more seamless user onboarding and access to products or services.
- **Higher revenue**: Increase user conversion, retention and satisfaction by enabling users to share data with ease and piece of mind.
- **New business models**: Launch new products or services (ID wallets, credential issuance/verification) to unlock new revenue opportunities.
- **Lower costs**: Streamline processes (with employees, customers, suppliers…), reduce help desk requests & costs for ID services (as decentralized identity is consolidating identity solutions).
- **Prevent fraud**: Prevent SPAM and fraud like ID theft or document forgery.
- **Verify authenticity**: Verify users or prove the authenticity and provenance of content to identify AI-generated content & prevent IP issues .
- **Better data quality**: Improve data quality by offering stakeholders to provide digital credentials that are verified and signed by trusted third parties.
- **Stronger security**: Mitigate the risk of data breaches and other security issues by eliminating the risk factors like passwords or aggregated data storage.

The value proposition of decentralized identity and identity wallets based on eIDAS2:



Impact (RoI)

Better UX
Make interactions effortless

Compliance
Comply with regulations

Lower Costs
Streamline processes

Higher Revenue
Improve conversion, retention...

Less Fraud
Prevent ID theft, doc forgery...

Better Data Quality
Access verified user data

New Business Models
Launch new products & services

Stronger Security
Eliminate attack vectors.

Data authenticity
Verify users, provenance...

Grow **Revenue**

Reduce **Risk**

Streamline **Operations**

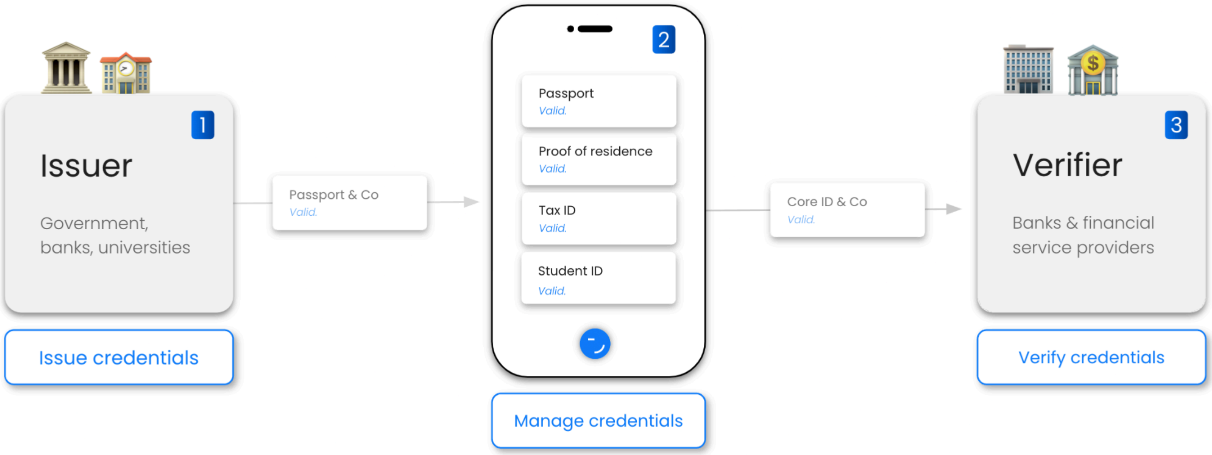
To illustrate the importance and the impact of eIDAS2 and decentralized identity, the following sections provide short analyses of various industries including brief elaborations of different use cases and their value proposition for businesses and their stakeholders.

Banking & Financial Services

Banks and other financial service providers are one of the most heavily impacted actors and need to comply with eIDAS2 for digital transactions, online banking, and remote customer identification.

As a result, we're seeing banks, payment providers, asset managers, fintechs etc. getting started with decentralized identity to build new applications and use cases.

1. **User onboarding**: Businesses offer their customers more seamless experiences in the context of user onboarding or other digital interactions.
2. **KYC/B (AML)**: Businesses offer their customers faster, simpler, cheaper and more reliable identity verification.
3. **ID wallets**: Businesses offer ID wallets to their customers (via their existing apps) to remain "top-of-mind", prevent disintermediation by competition and own (what will soon be) users' most important app.
4. **Lending**: Businesses offer customers faster and easier access to financial products like loans by enabling their customers to share all required information within seconds based on reusable identity credentials



Decentralized identity & eIDAS2 enable the flow of data like name, date of birth, address, proof of residence, tax or student IDs. Data is issued from trusted sources (e.g. governments, banks) to individuals or organizations who can share their data (via wallets) with banks and financial service providers for use cases like user onboarding, ID verification (KYC/KYB), provision of financial products like lending or compliance with new laws (eIDAS2, TFR for CASPs).

As a result, there are huge opportunities for businesses in this industry:

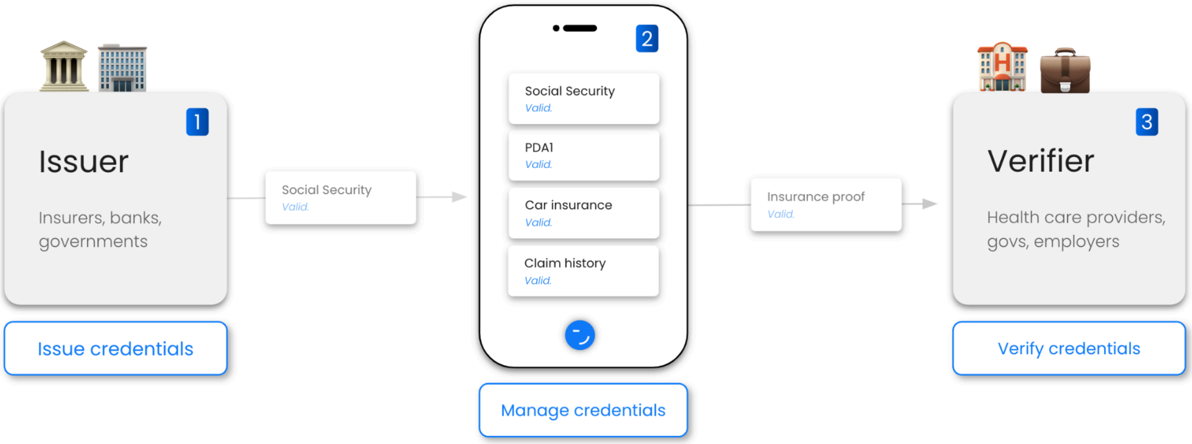
- **Better UX**: Offer more seamless onboarding, access to products or services.
- **Higher revenue**: Increase user conversion, retention and satisfaction by enabling users to share data with ease and piece of mind.
- **New business models**: Launch new products or services (ID wallets, credential issuance/verification) to unlock new revenue opportunities.
- **Lower costs**: Streamline processes (with employees, customers, investors) & reduce costs for identity-related services like auth or ID verification.
- **Prevent fraud**: Prevent SPAM and fraud like ID theft or document forgery.
- **Better data quality**: Improve data quality with pre-verified digital credentials.
- **Stronger security**: Mitigate the risk of data breaches by eliminating the risk factors like passwords or aggregated data storage.

Insurance

Insurers are among the most heavily impacted actors and need to comply with eIDAS2 for digital transactions, online banking and remote customer identification.

As a result, we're seeing insurance companies and startups getting started with decentralized identity to build new applications and use cases.

1. **User onboarding**: Businesses offer their customers more seamless experiences in the context of user onboarding or other digital interactions.
2. **ID wallets**: Businesses offer ID wallets to their customers (via their existing apps) to remain "top-of-mind", prevent disintermediation by competition and own (what will soon be) users' most important insurance app.
3. **Insurance products**: Businesses offer customers faster and easier access to insurance products by enabling their customers to share all required information within seconds based on reusable identity credentials.
4. **Insurance cards**: Issue digital insurance cards or proofs to your customers so they can easily prove their insurance status towards third parties.



As a result, there are huge opportunities for businesses in this industry:

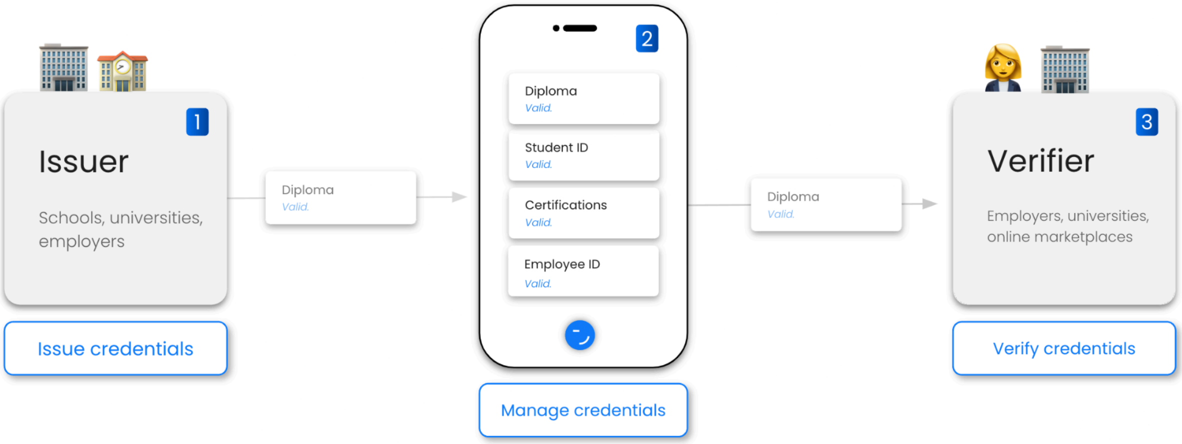
1. **Better UX**: Offer more seamless onboarding, access to products or services.
2. **Higher revenue**: Increase user conversion, retention and satisfaction by enabling users to share data with ease and piece of mind.
3. **New business models**: Launch new products or services (ID wallets, credential issuance/verification) to unlock new revenue opportunities.
4. **Lower costs**: Streamline processes (with patients, doctors…) & reduce costs for identity or data verification services.
5. **Prevent fraud**: Prevent fraud like ID theft or document forgery.
6. **Better data quality**: Improve data quality with pre-verified digital credentials.
7. **Stronger security**: Mitigate the risk of data breaches by eliminating the risk factors like passwords or aggregated data storage.

Education & Employment

Educators like universities and employers need to comply with eIDAS2 if they want to leverage the advantages and legal guarantees of this regulation for authentication and identification.

As a result, we're seeing educators like universities or schools, edtechs, HR-software vendors and background verification providers getting started with decentralized identity to build new applications and use cases.

1. **Digital IDs**: Organizations issue digital IDs to students, employees and others for more seamless onboarding experiences or access to digital services.
2. **Onboarding**: Organizations facilitate student mobility and employee onboarding by making it easy to share or collect all required documents.
3. **ID Wallets**: Organizations launch ID wallets for students and professionals to own (what will soon be) users' most important education/employment app.
4. **Diplomas**: Educators issue digital education credentials like diplomas to their students and graduates.
5. **Job application**: Employers offer applicants a 1-click application process and can verify the provided information reliably and within seconds.



As a result, there are huge opportunities for businesses in this industry:

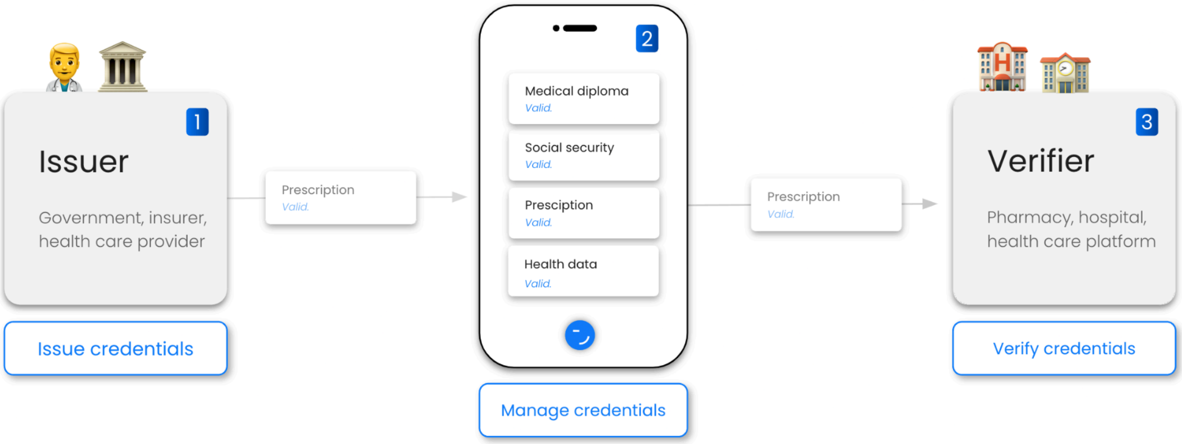
- **Better UX**: Effortless onboarding, access to digital services or job applications.
- **Lower costs**: Streamline processes (with employees, customers, investors) & reduce costs for identity-related services like auth or ID verification.
- **Better data quality**: Improve data quality with pre-verified digital credentials.
- **Prevent fraud**: Prevent SPAM and fraud like ID theft or document forgery.
- **User satisfaction**: Increase user conversion, retention and satisfaction.
- **New business models**: Launch new products or services (ID wallets, credential issuance/verification) to unlock new revenue opportunities.
- **Stronger security**: Mitigate the risk of data breaches by eliminating the risk factors like passwords or aggregated data storage.

Health Care

Healthcare Providers, including online healthcare services like telemedicine, require eIDAS2 compliance for patient data protection and secure digital communication.

As a result, we're seeing health care and telemedicine providers getting started with decentralized identity to build new applications and use cases.

1. **User onboarding**: Organizations offer more seamless onboarding for patients, doctors or others by making it easy to share or collect required documents.
2. **ID wallets**: Organizations launch ID wallets for patients and healthcare professionals to own (what will soon be) users' most important eHealth app.
3. **ePrescriptions**: Organizations issue and verify digital prescriptions.
4. **Patient data**: Organizations issue health data to patients and enable patients to easily share their data with doctors and health service providers.
5. **Insurance Cards**: Organizations issue or verify the insurance status of patients.



As a result, there are huge opportunities for businesses in this industry:

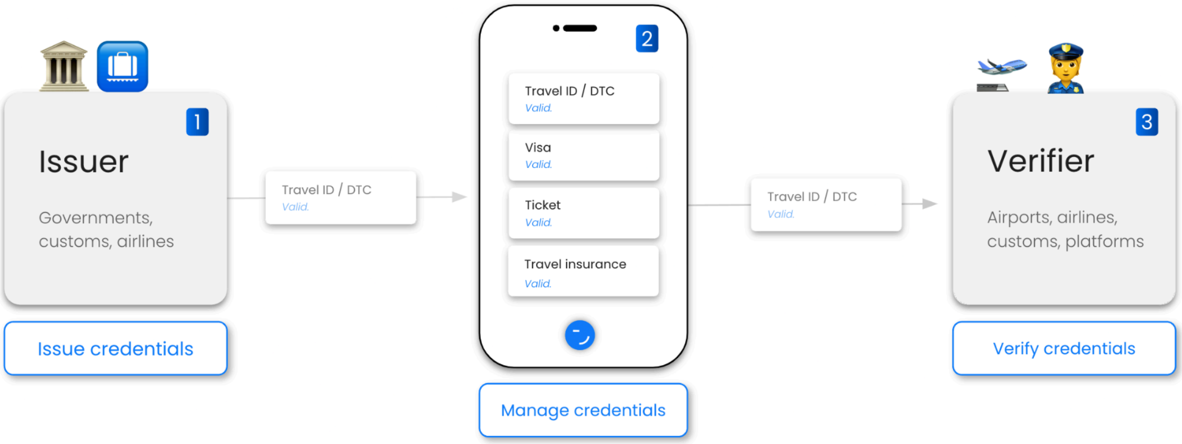
- **Better UX**: Effortless onboarding, access to digital services or job applications.
- **Lower costs**: Streamline processes (with employees, customers, investors) & reduce costs for identity-related services like auth or ID verification.
- **Better data quality**: Improve data quality with pre-verified digital credentials.
- **Prevent fraud**: Prevent SPAM and fraud like ID theft or document forgery.
- **User satisfaction**: Increase user conversion, retention and satisfaction.
- **New business models**: Launch new products or services (ID wallets, credential issuance/verification) to unlock new revenue opportunities.
- **Stronger security**: Mitigate the risk of data breaches by eliminating the risk factors like passwords or aggregated data storage.

Aviation

The aviation industry benefits from a unified digital identity wallet and credentials. Airline operators and airports are required to validate and confirm passengers' identity as part of the pre-flight identity proofing requirements. Today, this is a complex process given that each country can have a custom identity source.

As the wallet contains standardized identity credentials, attested by the issuing government, airlines and airports can rely on this to perform passenger ID proofing.

1. **Flight booking**: The wallet identity credential can be used to confirm identity information while booking a flight. This will allow a passenger to provide a government attested digital identity as part of the booking process.
2. **Ticket issuance**: The flight ticket can be issued electronically and directly in the digital wallet, making it easily available while benefiting from the security and privacy features of the wallet.
3. **Pre-flight check**: As the wallet provides a government-attested ID credential which can be used during flight booking, airlines and airport authorities can rely on it for pre-flight ID proofing and flight booking ID validation.
4. **Digital Travel Credential (DTC)**: The wallet can store a DTC, which is part of the International Civil Aviation Organisation standards and the digital equivalent of a passport allowing EU citizens to present the DTC during inbound border control, even when entering a non-EU country.



As a result, there are huge opportunities for businesses in this industry:

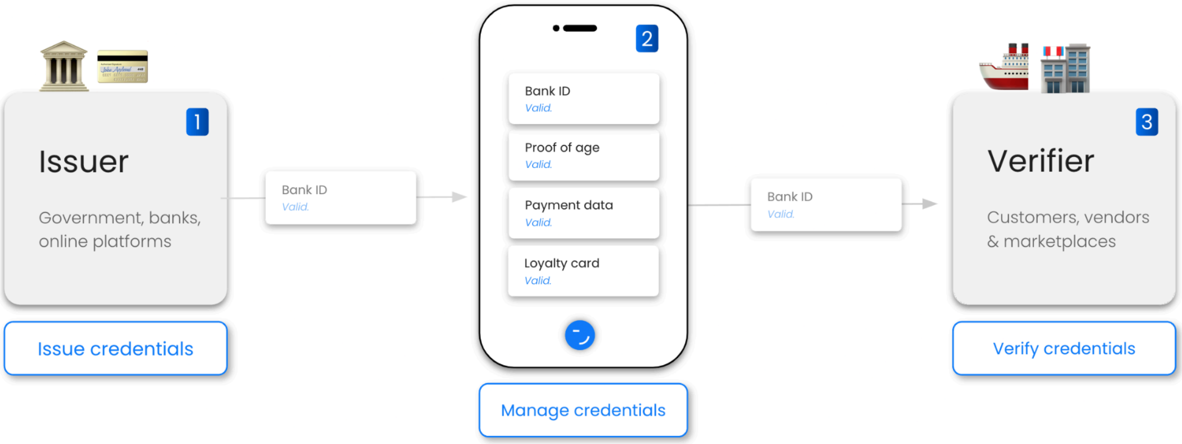
- **Better UX**: Effortless flight booking and flight boarding, including a digital boarding pass and digital passport credential (DTC).
- **Lower costs**: Streamline processes (with airline operators, flight booking systems, pre-flight identity proofing systems, airport authorities) & reduce costs for passenger identity proofing and inbound border control.
- **Better data quality**: Improve data quality with government attested digital credentials.
- **Reduce fraud**: Reduce identity fraud risks by leveraging the government attested digital identity.
- **User satisfaction**: Eliminate the need for manual identity data entry and streamlined booking and boarding experience.
- **New business models**: Launch new products or services (ID wallets, credential issuance/verification) to unlock new revenue opportunities.
- **Stronger security and privacy**: Mitigate the risk of data breaches by eliminating the risk factors like passwords or aggregated data storage and manual data entry.

eCommerce

eCommerce platforms and online retailers operating in the EU must comply with eIDAS2 for electronic transactions and consumer protection.

As a result, we're seeing the eCommerce industry getting started with decentralized identity to build new applications and use cases.

1. **Onboarding & check-out**: Businesses offer their customers more seamless onboarding and check-out experiences
2. **User verification**: Businesses offer their customers faster, simpler, cheaper and more reliable identity or age verification where required.
3. **Access**: Businesses offer users faster and easier access to products, services or exclusive communities by enabling users to easily share pre-verified data.
4. **ID wallets**: Businesses offer identity wallets to their customers - often via their existing applications - to own (what will soon be) users' most important shopping app.



As a result, there are huge opportunities for businesses in this industry:

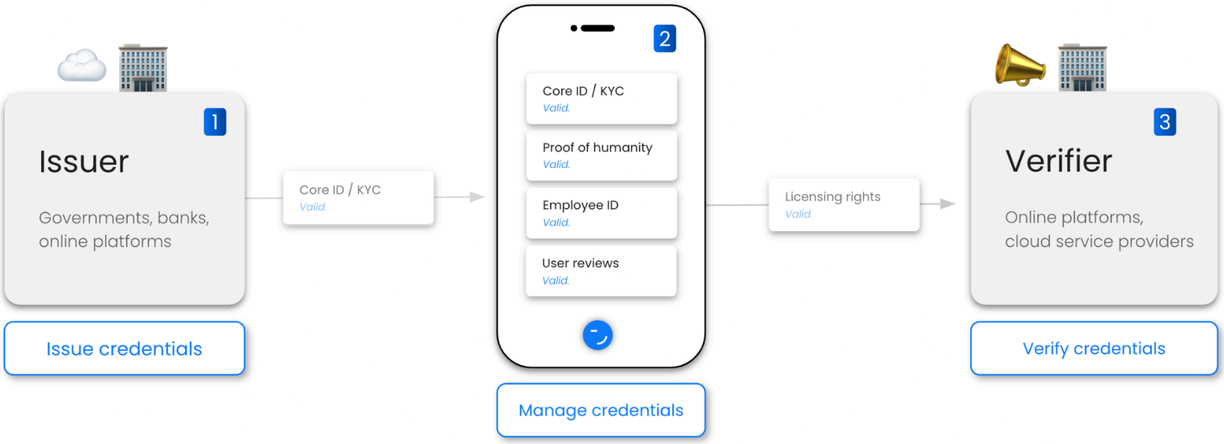
- **Better UX**: Offer more seamless onboarding, access to products or services.
- **Higher revenue**: Increase user conversion, retention and satisfaction by enabling users to share data with ease and piece of mind.
- **New business models**: Launch new products or services (ID wallets, credential issuance/verification) to unlock new revenue opportunities.
- **Lower costs**: Streamline processes with users & reduce costs for identity-related services like auth or ID verification.
- **Prevent fraud**: Prevent SPAM and fraud like ID theft or document forgery.
- **Better data quality**: Improve data quality with pre-verified digital credentials.
- **Verify authenticity**: Given the rise of AI, businesses can verify users (humanity) or prove the authenticity and provenance of content.
- **Stronger security**: Mitigate the risk of data breaches by eliminating the risk factors like passwords or aggregated data storage.

Online Platforms & Digital Service Providers

Digital service providers like cloud service providers and (large) online platforms are heavily impacted and need to comply with eIDAS2 for digital identity verification and digital transactions.

As a result, we're seeing digital service providers and platforms across industries getting started with decentralized identity to build new applications and use cases.

1. **User onboarding**: Businesses offer their customers more seamless experiences in the context of user onboarding or other digital interactions.
2. **User verification**: Businesses offer their customers faster, simpler, cheaper and more reliable identity or age verification where required.
3. **Access**: Businesses offer users faster and easier access to products, services or exclusive communities by enabling users to easily share pre-verified data.
4. **ID wallets**: Businesses offer identity wallets to their customers - often via their existing applications - to own (what will soon be) users' most important app.



As a result, there are huge opportunities for businesses in this industry:

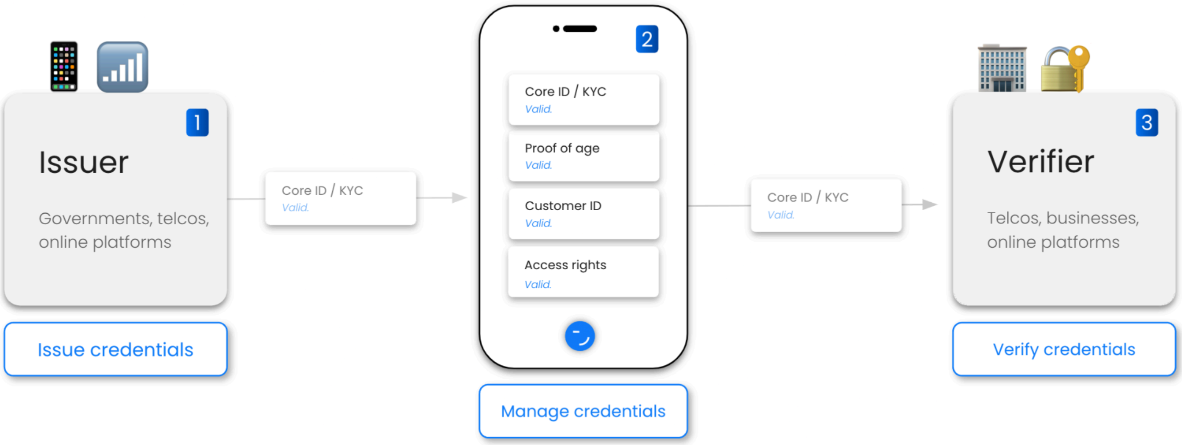
- **Better UX**: Offer more seamless onboarding, access to products or services.
- **Higher revenue**: Increase user conversion, retention and satisfaction by enabling users to share data with ease and piece of mind.
- **New business models**: Launch new products or services (ID wallets, credential issuance/verification) to unlock new revenue opportunities.
- **Lower costs**: Streamline processes with users & reduce costs for identity-related services like auth or ID verification.
- **Prevent fraud**: Prevent SPAM and fraud like ID theft or document forgery.
- **Better data quality**: Improve data quality with pre-verified digital credentials.
- **Verify authenticity**: Given the rise of AI, businesses can verify users (humanity) or prove the authenticity and provenance of content.
- **Stronger security**: Mitigate the risk of data breaches by eliminating the risk factors like passwords or aggregated data storage.

Telco

Telecommunication companies must comply with eIDAS2 for secure digital communication and identity verification services.

As a result, we're seeing telecommunication companies getting started with decentralized identity to build new applications and use cases.

1. **User onboarding**: Telcos offer more seamless experiences in the context of user onboarding or other digital interactions.
2. **User verification**: Telcos offer faster, simpler, cheaper and more reliable identity or age verification.
3. **Access**: Telcos offer users faster and easier access to their products and services by enabling users to easily share pre-verified data.
4. **ID wallets**: Telcos offer ID wallets to their customers (via their existing apps) to own (what will soon be) users' most important app.



As a result, there are huge opportunities for businesses in this industry:

- **Better UX**: Offer more seamless onboarding, access to products or services.
- **Higher revenue**: Increase user conversion, retention and satisfaction by enabling users to share data with ease and piece of mind.
- **New business models**: Launch new products or services (ID wallets, credential issuance/verification) to unlock new revenue opportunities.
- **Lower costs**: Streamline processes with users & reduce costs for identity-related services like auth or ID verification.
- **Prevent fraud**: Prevent SPAM and fraud like ID theft or document forgery.
- **Better data quality**: Improve data quality with pre-verified digital credentials.
- **Stronger security**: Mitigate the risk of data breaches by eliminating the risk factors like passwords or aggregated data storage.

What eIDAS2 means for governments

TL;DR

The **eIDAS2** regulation **forces the adoption of decentralized identity and identity wallets by governments** in Europe. In other words, governments and public authorities will be required to:

1. provide citizens with ID wallets
2. issue digital identity credentials to citizens (ID wallets)
3. Enable electronic signatures with the legal equivalent to handwritten signatures
4. accept digital identity credentials & wallets for authentication & identification

That being said, **regulatory compliance** (eIDAS2) is only one of many reasons why governments adopt decentralized identity aligned with eIDAS2. Here are few more:

- **Better citizen experience**: Governments can offer more seamless experiences in citizen-government interactions.
- **Higher citizen satisfaction**: Governments can increase citizen satisfaction by enabling them to easily collect, manage and share data with peace of mind.
- **Interoperability**: In combination with the Only Once Principle, governments can use the provided wallet and ID credential to have a strong proof of identity of the citizen and reuse known information about the citizen.
- **Lower costs**: Governments can streamline processes and cut costs for providing services.
- **Less fraud**: Governments can reduce ID theft, document forgery and other forms of fraud.
- **Data quality**: Governments can improve data quality across different organizations and applications (which are currency "data silos").

As a result, identity wallets will become the main way for citizens to interact with governments and public authorities.

Enabling public sector innovation

eIDAS2, identity wallets and decentralized identity are crucial enablers of public sector innovation. For example::

- **Access**: Governments offer citizens seamless access to eGovernment services by enabling them to authenticate in a 1-click process via their wallets.
- **Digital identity documents**: Governments issue digital identity credentials - like passports, driver's license, proof of residence or visas (among others) - that can be easily managed and shared by citizens via ID wallets.
- **ID Wallets**: Governments offer ID wallets to citizens, which they can use to collect, manage, store and share identity data securely and privately.
- **Data exchange**: Citizens can easily share government-issued credentials with other governments (e.g. travel, relocation), public authorities (e.g. police, local administrations) or businesses (e.g. banks, insurance, telco, utility, online platforms…) in order to access products or services.
- **Content consent & signage**: Issued digital identity wallet will allow the citizen to electronically sign documents. This will enable a citizen not only to use the wallet for identification and authentication purposes when interacting with governments, but also to formally sign documents or forms.

The following sections outline implications of eIDAS2 for selected use cases.

Tax Filing

Tax filing and tax collection is one of the most complex processes and applies to a substantial part of a nation's population. Governments can leverage digital identity wallets to dematerialize, optimize or interconnect existing government systems.

The digital identity wallet provides strong user authentication capabilities allowing reliable user identity verification which offers citizens faster and easier access to their information and tax filing requirements by leveraging pre-verified data and a mobile user interface.

Social Security

Social Security is a key government task that affects every citizen. Digital ID wallets can be used to store digital proofs of social security status and scope for citizens.

Governments and social security agencies can use the digital identity wallet to issue social security documents for citizens and their children. The digital identity wallet provides strong user authentication that can be linked to social security status documents. This provides a secure and easily accessible proof to any government agency of social security support of the citizen and their children.

Law enforcement

Law enforcement deals with citizen identity on a daily basis and is required to be able to confirm the identity of citizens. Online and offline identity fraud cases are substantially increasing, which can be mitigated by the digital identity wallet.

Law enforcement can rely on digital ID credentials stored in the wallet for citizen ID validation. Additionally, wallet theft or credential validity can be validated securely to confirm the provided ID credential.

The wallet will only disclose required information to law enforcement, related to for example the citizen identity, driving license, vehicle registration and insurance documents. Given the wallet incorporates and enforces strong security and privacy mechanisms, the requested information is only released after confirmation that the identity request is actually coming from law enforcement.

What to do now?

The following chapter outlines a proven six-step approach.

Step 1: Get familiar with eIDAS2

When it comes to digital identity and trust services, eIDAS is the reference legal and regulatory framework for organizations and governments operating in the EU. Combined with the applicable European norms and standards (e.g. ETSI en CEN/CENELEC), eIDAS provides a toolbox of services that allow a standardized approach across borders, while providing the legal foundation and recognition of these services in all member states.

Given its pragmatic approach, combining a legal and standardized technology framework, eIDAS is becoming the digital identity and trust services framework beyond the borders of the EU. Organizations and governments globally are adopting eIDAS principles and standards to future proof their economy vision and strategy.

To leverage eIDAS, it is essential to have a good understanding of what eIDAS entails, how it can be leveraged and implemented.

A good starting point is the documentation by the European Commission which provides an overview of the electronic identity[1] and electronic signature[2] building blocks defined in eIDAS. If you want to dive deeper into the subject matter, an inventory of relevant legal and standardization documents can be found here.

Secondly, reaching out to subject matter experts is essential for having a successful implementation of your eIDAS digital identity and trust services projects. eIDAS is a legal framework and comes with its legal and regulatory requirements. It requires a profound understanding of what the legal and regulatory frameworks entail and how it can be translated and applied to your organization's needs. Obtaining the advice and support of an experienced subject matter expert will reduce implementation lead time and can avoid potential legal or standards conflict during implementation or operation of your services.

[1] https://ec.europa.eu/digital-building-blocks/sites/display/DIGITAL/eID

[2] https://ec.europa.eu/digital-building-blocks/sites/display/DIGITAL/eSignature

Step 2: Identify opportunities & compliance risks

Start by defining your business opportunities and goals. To do so, it is helpful to focus on specific categories or areas of your operations.

The following framework offers guidance to help you on your journey.

Category	Description
User Experience	Analyze your customer or stakeholder interactions like onboarding or check out processes. Typically, these will require passwords, forms or multi-step verification processes that create friction. Decentralized identity aligned with eIDAS2 can streamline user flows by replacing multi-step processes with a simple 1-click experience.
Data Quality	Do you face data quality or data consistency issues? Are customers providing wrong information, intentionally or due to human error? Decentralized identity aligned with eIDAS2 can ensure high data quality based on ID information verified by trusted third parties.
Security & Privacy	Analyze your current security practices in the context of user authentication, identification and the handling of user data. For example, which user data do you request and store? Do you use passwords or similar approaches that create attack vectors? Decentralized identity aligned with eIDAS2 enables more secure authentication and identification while ensuring data minimization.
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? Decentralized identity aligned with eIDAS2 facilitates compliance with these regulations via user-centric data and consent management, wallet-based user identification and automatable fulfillment of data provision requests.

Process Automation	Analyze your current strategy for process automation against opportunities created by machine-readable digital ID data. Decentralized identity aligned with eIDAS2 unlocks reliable, machine-readable user data to enhance process automation.
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. While Decentralized identity aligned with eIDAS2 already creates significant value in interactions between only two parties (like your organization and your customers), the more stakeholders involved the better as multi-party processes are inherently challenging to support with existing centralized systems.

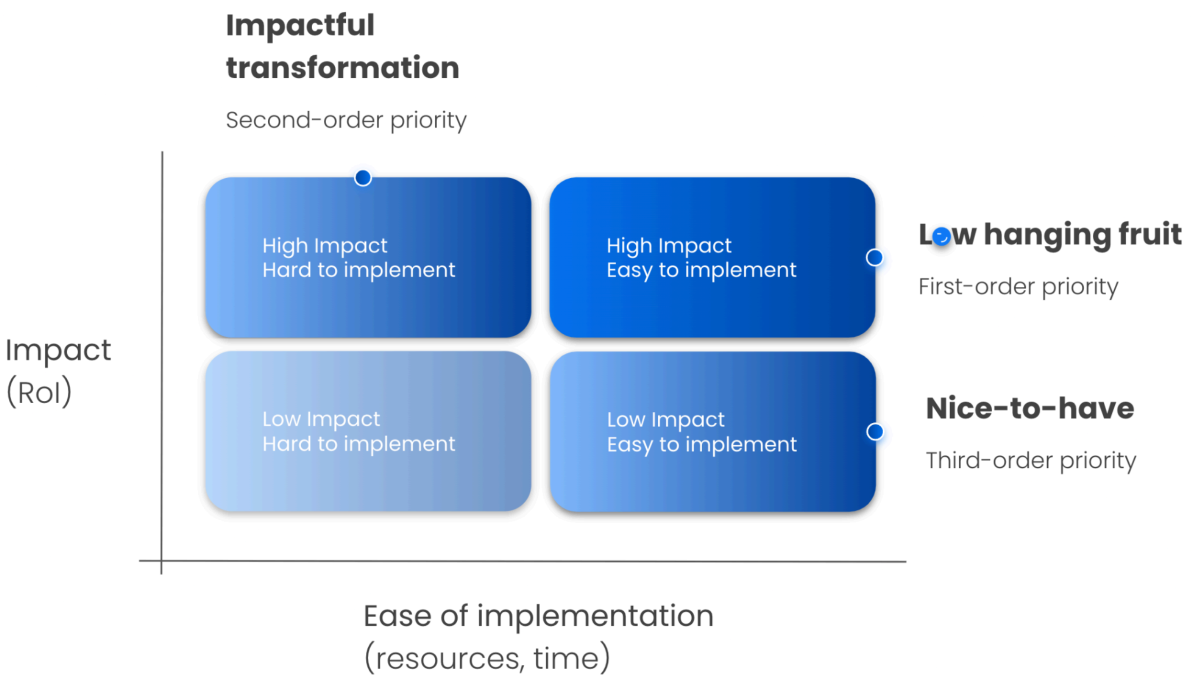
This framework does not provide a conclusive list of categories so will likely discover additional areas specific to your organization or industry.

Step 3: Select & prioritize use cases

Based on the opportunities and risks you identified, list all use cases relevant to your organization. (The use cases outlined in prior sections may serve as inspiration.)

Once you have a list of all use cases, prioritize them based on your organization's strategy, challenges and product or service portfolio.

The following 2x2 matrix offers a simple way to prioritize your use cases based on their impact on your organization (Return of Investment) and the ease of implementation (resources, time).



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

1. Impact

The most important criteria for the selection of your use case is its potential impact on your organization. Consider the following types of benefits:

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 personal data processing (e.g. based on the EU General Data Protection Regulation, GDPR) to avoid high penalties 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.

Prevent falling behind competitors: Finally, consider the impact on your business if competitors adopt SSI before you do.

2. Ease of Implementation

The effort required to implement your use case will vary depending factors such as:

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.

Step 4: 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:

1. Use cases

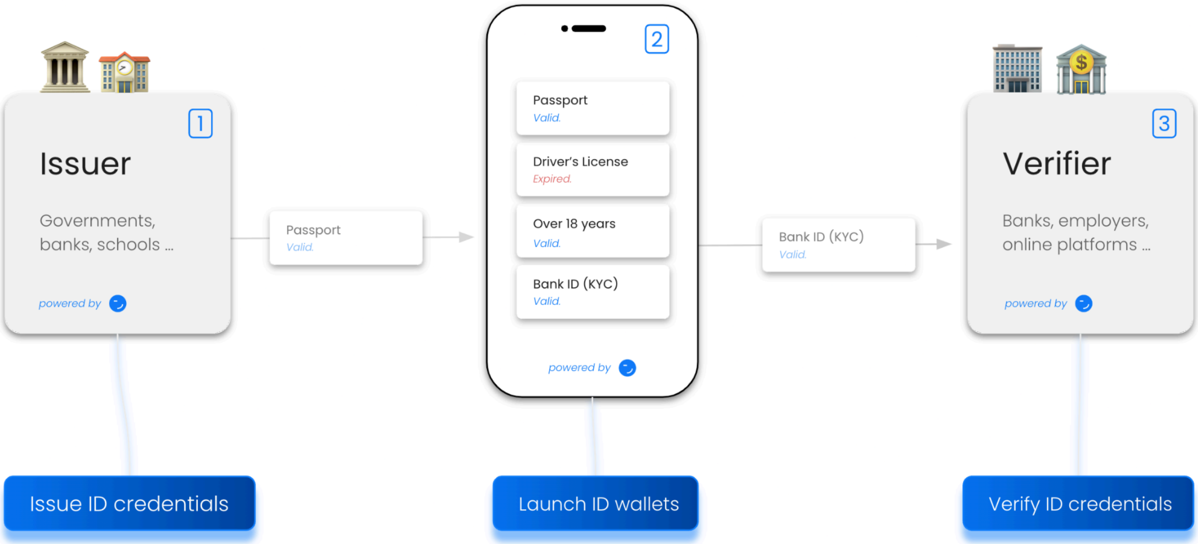
Your requirements will differ depending on your use cases. Also, use cases will differ in terms of complexity ranging from simple, reusable to highly customized patterns. The definition of user journeys down to user stories are a helpful way to formalize your use cases and define your business requirements.

2. Roles

Your requirements will differ depending on whether your organization is acting as

- **Issuer** - Organizations who identity credentials to users' wallets,
- **Wallet Provider** - Organizations who provide wallets to users,
- **Verifier** - organization who verifies identity credentials from users' wallets
- a mix of these three roles.

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).



3. 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.

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?

Step 5: 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?

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 your time to market.

Start by 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 (compared to starting from scratch). 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).

Since technology and vendor selection can be complex, we distilled a few criteria against which organizations across industries evaluate their options:

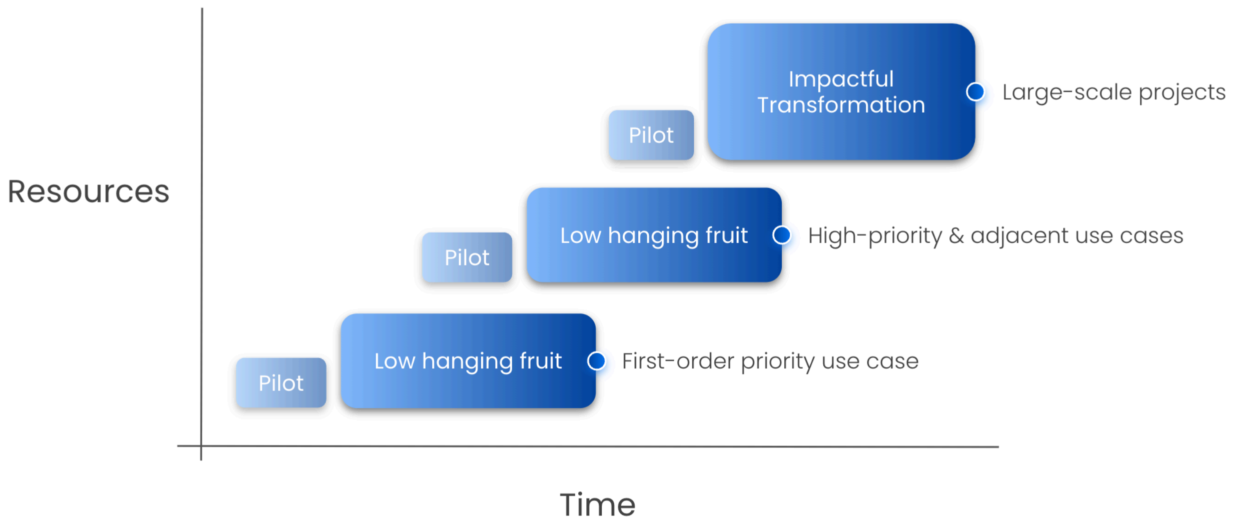
Criteria	Description
Use Cases	Ensure that your solution fulfills your business requirements and can be used to implement your use cases.
Compliance	Ensure that your solution complies with all regulations required by your business operations (eIDA2, GDPR, AML, TFR...) .
Ecosystems	Ensure that your solution 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.

Step 6: 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").

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.

TRUSTSCAPE

About the authors

walt.id

walt.id offers **holistic open source digital identity and wallet infrastructure** used by thousands of developers, governments and businesses across industries. All solutions **ensure compliance with eIDAS2**, various identity ecosystems like EBSI and standards (W3C, ISO, IETF, OIDF).

In addition, walt.id **extensively worked with the EU and Member States**, co-authoring EU's new ID standards (EBSI, eIDAS2) or serving as technology provider in several EU Large Scale Pilots.

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

Trustscape

TrustScape provides expert advice on eIDAS Digital Identity & Trust Services and serves as a trusted advisor for public and private organizations. We advise on the legal and regulatory requirements for eIDAS Wallets, Electronic Identity and Trust Services as well as national digital identity programmes for EU Member States and beyond.

In addition, Trustscape helps with the development of new legal & regulatory requirements and standards development related to eIDAS.

- Website: https://trustscape.eu
- Contact: https://trustscape.eu/contact
- Resources: https://trustscape.eu/resources
- Community: LinkedIn