# Digital Identity Standards & Ecosystems

The evolving landscape of decentralized identity and identity wallets.

# Table of Contents

# Introduction

In a world where digital interactions increasingly define our daily lives, the concept of identity has undergone a profound transformation. We stand at the precipice of a significant shift in how identity functions across the digital landscape — moving from centralized, siloed systems toward decentralized ecosystems that promise to return control to individuals while enabling unprecedented interoperability across platforms and borders.

## The global adoption wave

Decentralized identity is no longer merely a theoretical concept championed by privacy advocates and blockchain enthusiasts. It has entered a phase of pragmatic implementation across diverse sectors:

Governments are exploring citizen-centric identity frameworks and corresponding regulations. They launch ID wallets to give citizens more control over their digital identity and credentials. Large institutions are exploring how decentralized identity can streamline customer interactions and processes while reducing data liability and ensuring regulatory compliance. Businesses are building new SaaS platforms to make the adoption of decentralized identity and ID wallets seamless for small and large organizations.

This global momentum isn't isolated to wealthy nations or tech hubs. Developing economies — often unencumbered by legacy identity systems — are leapfrogging directly to decentralized architectures,

recognizing their potential to address longstanding challenges in financial inclusion and service delivery.

## The critical role of standards

The decentralized identity landscape is being fundamentally shaped by the emergence and adoption of key standards. These standards aren't merely technical specifications. They represent the grammar and syntax of a new identity language that enables diverse systems to communicate seamlessly across organizational and geographical boundaries.

The importance of standards in this ecosystem cannot be overstated for several reasons:

- Interoperability: Standards like Verifiable Credentials (W3C), mobile driving license (ISO 18013-5) and OpenID4VC (OIDF) enable identity solutions from different vendors and jurisdictions to work together, preventing the formation of new walled gardens.
- Trust frameworks: Standardized governance models establish the rules of engagement between identity providers, verifiers, and subjects, creating predictable interaction patterns that build confidence in the ecosystem.
- Scalability: Well-designed standards allow for implementations that can grow from small pilots to national or global deployments without fundamental redesigns.
- Security: Standards and their extensions establish consistent mechanisms for threat mitigation. They help prevent common

attacks, ensuring secure and interoperable implementations across diverse systems.

- Regulatory alignment: Emerging standards increasingly account for regulatory requirements across regions, helping organizations maintain compliance while adopting decentralized approaches.

The organizations driving these standards have become the invisible architects of our digital future, their work determining the contours of how identity will function for decades to come.

## A framework for understanding adoption

This eBook is intended to help readers navigate the complex landscape of decentralized identity adoption by explaining the most important technology standards, regulations and map them to actual adoption patterns by governments and businesses globally.

The decentralized identity movement represents more than a technological shift. It embodies a fundamental rethinking of the relationship between individuals, organizations, and their data. This transformation promises to reshape digital interactions across every sector, creating new opportunities for privacy, security, and user empowerment in our increasingly connected world.

# Part 1 - Standards & Technologies

## It all started in walled gardens

Just a few years ago, the decentralized identity space looked very different. Every vendor was inventing their own (proprietary) technologies and they did so across the whole decentralized identity tech stack. This situation was born out of the need to fill a gap that had to be filled (there weren't any agreed upon standards and vendors had to implement something) and fueled by ideology as well as enthusiasm for complex and potent technologies. As a result, solutions were factually centralized. There was no interoperability and without interoperability, the promise of decentralized identity, including the free movement of data, is simply not possible.

The irony was palpable — technologies ostensibly designed to decentralize power and control were creating new silos, walled gardens, and vendor lock-in. Solution providers spoke the language of openness while implementing closed systems, fragmenting the very ecosystem they intended to be building.

## From fragmentation to coherence

The journey toward standardization has not been straightforward. It has involved complex negotiations between competing visions, reconciliation of seemingly incompatible technical approaches, and the delicate balance between innovation and stability. Throughout this process, the community has had to address critical questions: How

much standardization is necessary? Which layers of the stack must be interoperable? How can standards accommodate innovation while ensuring compatibility?

Today, we stand at a pivotal moment where core standards have matured sufficiently to enable meaningful interoperability while remaining flexible enough to adapt to emerging requirements. These standards - ranging from identifier formats to cryptographic suites, credential structures to exchange protocols - form the invisible infrastructure upon which the promise of decentralized identity can finally be realized.

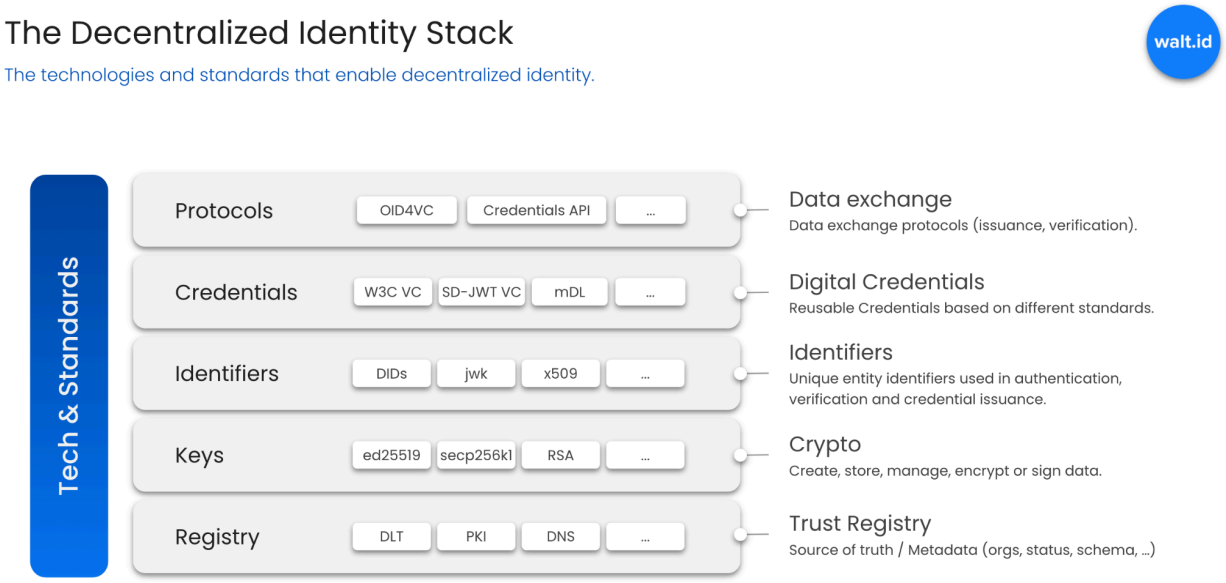
In the following sections, we'll provide an overview of:

- The core standards enabling decentralized identity today
- The relationship between standards and implementations
- Emerging standards that address gaps in the current landscape

Understanding these standards isn't merely an academic exercise. It's essential knowledge for anyone seeking to implement, integrate with, or participate in the decentralized identity ecosystem. As we'll see, these standards don't just enable technical interoperability; they establish the rules of engagement for a new model of digital relationships based on mutual trust, verifiability, and user control.

# Making sense of standards

Decentralized identity can be best understood through a layered technology stack architecture that consists of five interdependent levels, each building upon and extending the capabilities of those beneath it.




At the foundation is the Trust Registry Layer, which provides the underlying infrastructure for establishing trust. This includes technologies such as Distributed Ledgers or Blockchains, traditional Public Key Infrastructure (PKI), and the Domain Name System (DNS). These technologies serve as authoritative sources of truth and repositories for essential metadata.

The Keys Layer builds on this foundation, incorporating cryptographic standards like Ed25519, secp256k1, and RSA. This layer enables the fundamental security operations of data encryption and digital signatures that ensure integrity and confidentiality throughout the stack.

Moving upward, the Identifiers Layer leverages standards such as Decentralized Identifiers (DIDs), JSON Web Keys (JWK), and X.509 certificates. These technologies provide unique entity identifiers that are essential for authentication and verification, while directly mapping to corresponding trust registry technologies in the underlying layer.

The Credentials Layer further extends these capabilities through standards like W3C Verifiable Credentials (VC), IETF SD-JWT-based Verifiable Credentials (SD-JWT VC), and Mobile Driving Licenses (mDL/mdoc; ISO 18013-5). These frameworks enable the creation and management of reusable, portable digital credentials that can represent virtually any attestation about an entity.

At the apex is the Protocols Layer, which is tightly integrated with the digital credential standards below it. Technologies such as OpenID for Verifiable Credentials (OID4VC) and the Digital Credentials API define the rules for secure data exchange during credential issuance, presentation, and verification processes.

Together, these five interconnected layers create a comprehensive technological ecosystem that enables truly decentralized identity systems while maintaining security, privacy, and interoperability across diverse implementations and use cases.

In the following chapters, each layer and the corresponding standards will be briefly explained in a way that is useful for both technical and non-technical readers.

## Trust Registries

Generally, the idea of a registry is similar to the idea of a ledger. It is a place of record keeping, a shared source of truth. In the context of digital identity registries are usually referred to as “Trust Registries”, because they establish a framework for creating trust between people and organizations that typically don’t know each other - particularly trust that the identity information that originates from the ecosystem is correct.

The main purpose of Trust Registries is to enable discovery and the verification of identity data. As such, they are the single source of truth and act like a shared database for information that members of an identity ecosystem consult in order to trust each other (based on the identity data that is being exchanged).

Trust Registries can be implemented with different technologies like

- Traditional public key infrastructure (PKI),
- Domain Name Service (DNS),
- Permissioned/consortium blockchains,
- Public/unpermissioned blockchains.

Apart from the technology with which a Trust Registry is implemented, there are also different types, each of which enables the verification of identity data across a different dimension. For example:

- “Organization Registries” verify and provide information about organizations that act in different roles such as data sources (“Issuers”) or data consumers (“Verifiers”).

- “Schema Registries” establish standards for and provide information about semantics and data models to ensure reusability and interoperability of data sets.
- “Revocation Registries” are used to manage the lifecycle of data. In particular, they enable data sources (“Issuers”) to revoke data if it becomes invalid.

You can learn more about Trust Registries and the concept of ID ecosystems in our eBook: The rise of identity ecosystems. You can also learn more about the role of blockchain in our Decentralized Identity Playbook.

## Identifiers

An identifier is something used to uniquely name or label a person, thing or idea so it can be recognized and referred to. For example, in everyday life, we use names as identifiers for people or license plates as identifiers for cars. Usernames, email addresses, or website links (URLs) are typical identifiers in the digital world.

Some identifiers are public, like an email address, which can be used by others to get in touch. Others are private, like passwords, only known by a specific system. Identifiers can also be "resolvable," meaning they point to something, like clicking on a website link takes one to that site. Whether in real life or online, identifiers make it easier to organize, find, and interact with people, things, or information.

Today, in the context of digital identity, the most important identifiers are X.509 certificates and Decentralized Identifiers (DIDs). Both serve as mechanisms for verifying digital identities, but operate differently.

### X.509 certificates

The traditional X.509 certificates are part of a centralized public key infrastructure (PKI), where a trusted Certificate Authority (CA) issues certificates that bind a public key to an entity, such as a person, organization, or device. These certificates include information like the public key, issuer details, and validity period and they enable secure communication by verifying the certificate's authenticity through the CA's digital signature.

### W3C Decentralized Identifiers (DIDs)

In contrast, W3C Decentralized Identifiers (DIDs) are designed to work within decentralized systems, such as blockchain networks, allowing entities to create and control their identifiers without relying on a central authority. DIDs are typically associated with cryptographic key pairs and support decentralized identity models, giving users more control over their data while ensuring privacy and security.

It is worth mentioning that the DID standard is very broad. It defines the architecture, data model and processing rules, but deliberately leaves out implementation-specific logic, such as resolution and updating procedures and, therefore, allows for a great diversity of types of DIDs, called “DID methods”, which come with vastly different sets of capabilities and architectural assumptions, each with its own strengths and weaknesses. Examples include did:key, did:jwk, did:web, did:ebsi, did:cheqd or did:eth.

Both systems, X.509 certificates and DIDs aim to establish trust in digital interactions but differ significantly in their reliance on centralized versus decentralized trust models.

## Digital Credentials

A digital credential is like an electronic version of a certificate, ID card, or badge that proves something about someone, such as one's identity, skills or achievements. Instead of being printed on paper, it's stored digitally and can be shared easily online. Digital credentials are issued by trusted organizations, like schools, governments, or companies, and often include important details like who issued it, who it belongs to, when it was given, and a secure way to prove it's real.

Digital credentials are designed to be safe and hard to fake, typically using cryptography to make sure they can be verified by others without being tampered with. Digital credentials are becoming more popular because they are convenient and secure, making it easier to prove your identity or qualifications in the digital world.

Today, there are a number of digital credential standards which are used in the context of digital and decentralized identity. The most important ones are.

### ISO mDL 18013-5 (Mobile Driving License)

The ISO mDL 18013-5 standard has initially been developed to enable digital, mobile driving licenses and requires credentials to stay on the original device or an issuer-controlled server. While users control data sharing, issuers can retrieve credentials directly (with user consent), revealing when and where they are used. It prioritizes offline functionality and uses temporary session keys to prevent tracking. For example, a police officer scanning a digital license offline wouldn't expose one's full identity history. That being said, given this standard's maturity - compared to other digital credential standards - it is gaining

momentum as a credential standard to be used via ID wallets, particularly in the public sector and adjacent verticals and use cases.

It is important to mention that ISO 18013-5 is not coming out of the decentralized identity movement and as such assumes a more centralized architecture building on top of X.509 certificates and traditional public key infrastructure. As a result, not everyone categorizes this standard as a decentralized identity standard.

### W3C Verifiable Credentials

W3C Verifiable Credentials are a more novel invention and originate from the Self-Sovereign Identity (SSI) movement. These credentials let users store proofs anywhere, like an ID wallet, and share them without issuer involvement. A university-issued degree could be stored in one's phone and shared with employers without the school knowing. They use JSON or JSON-LD formatting and digital signatures to prevent tampering.

Today, there are two versions of this standard:

First, the Verifiable Credential Data Model 1.1 or **VCDM 1.1**, a W3C Recommendation (March 2022), has already seen growing adoption around the globe, surpassing other early decentralized identity standards like AnonCreds and was taken up by regulators (e.g. EU, UK).

Second, the Verifiable Credential Data Model 2.0 or **VCDM 2.0**, a W3C Candidate Recommendation Draft (January 2025) introducing a number of changes to its predecessor like improved terminology (context URL, property naming) explicit separation of the data model from securing mechanisms, enabling broader cryptographic flexibility or the allowance to secure credentials via widely adopted JSON/CBOR

signing standards among others. As such, this new version focuses on improving flexibility, security, and real-world applicability while maintaining compatibility with VCDM 1.1-based systems. It also aims at extending interoperability with more traditional ecosystems, such as those based on ISO 18013-5. Finally, new standards, such as in the badging and education industry, like Open Badges 3.0 and Comprehensive Learner Record (CLR) 2.0 build on VCDM 2.0 to improve the trust model of digital badges and structure learner records in a machine readable way.

### SD-JWT VC

SD-JWT-based Verifiable Credentials (SD-JWT VC) are using Selective Disclosure for JWTs (SD-JWT) and have been standardized by the Internet Engineering Task Force (IETF). This standard lets users hide specific credential parts. For instance, a respective credential might include name, age, and vaccination status but allows sharing only the vaccination proof. It uses hashing to lock hidden data, requiring verifiers to check only the revealed info against the hash. Given its privacy-preserving focus, SD-JWT VCs have recently gained a lot of momentum and are being adopted by a number of regulators (e.g. EU, Switzerland).

### AnonCreds

AnonCreds were born out of the decentralized identity movement. They looked very promising early on (until a few years ago) and spoke to a large part of the decentralized identity community, not at least due to their innovative character. Ultimately, AnonCreds failed to reach large-scale adoption and other standards (W3C Verifiable Credentials,

SD-JWTs, ISO 18013-5) surpassed AnonCreds which are hardly ever used anymore. One can say that the early strengths of AnonCreds, which spoke to technologists, prevented wider adoption, such as the use of zero-knowledge proofs (ZKPs) based on novel cryptography that has not yet been trusted by market participants and regulators.

### Authentic Chained Data Containers (ACDC)

Authentic Chained Data Containers (ACDC) are a more exotic approach towards digital credentials. Conceptually, these credentials are chained in a tamper-proof sequence and each credential update creates a new linked block, enabling auditors to trace changes without exposing raw data. While ACDC credentials may be useful for certain industries (e.g. supply chain) and use cases (e.g. tracking certified product origins over time), the technological complexity led to relatively low adoption, particularly in the current face of market development which is largely driven by regulatory action and early adopters focused on use cases for the general public.

## Exchange Protocols

Data exchange protocols provide mechanisms for securely issuing, sharing, and verifying digital credentials. Much like in the case of digital credentials, there exist a number of protocols and they differ in their approaches to communication, privacy and interoperability, catering to various use cases in the digital identity ecosystem.

### OID4VC

OpenID for Verifiable Credentials (OID4VC) extends the widely adopted OpenID Connect framework, is a family of protocols defined by the

OpenID Foundation or OpenID Connect Working Group, to support digital credentials like W3C Verifiable Credentials. It includes two main specifications: OpenID4VCI (OpenID for Credential Issuance) and OpenID4VP (OpenID for Verifiable Presentations). Both specifications are evolving at a fast pace and are available in different versions, the most important ones being Drafts 11 (February 2023) and 13 (February 2024) for OID4VC and Drafts 18 (April 2023), 23 (December 2024) for OID4VP.

OID4VC uses OAuth2-based flows for secure interactions between issuers, holders, and verifiers and emphasizes privacy and simplicity by leveraging existing authentication patterns while introducing cryptographic mechanisms to bind credentials to users. As a result, OID4VC is currently widely regarded as the most important standard for digital credential exchange and picked up by regulators globally.

### Digital Credentials API

Digital Credentials API is a web platform API designed to enable websites to request and verify digital credentials stored in user-controlled digital wallets. It focuses on interoperability across platforms and systems by providing a unified interface for credential-related operations. The API is protocol-agnostic, meaning it can work with various credential exchange protocols, such as OID4VP.

Digital Credentials API and OID4VC are closely related, as the API provides a standardized mechanism for credential exchange, while OID4VC defines the protocols for issuing and presenting digital credentials. In other words: The Digital Credentials API acts as a browser-based interface that facilitates credential interactions between websites and digital wallets, allowing users to securely store,

retrieve, and share credentials. OpenID4VC complements this by specifying how these credentials are issued (OID4VCI) and presented (OID4VP) using OAuth 2.0 flows.

### DIDComm

DIDComm is a decentralized communication protocol built on Decentralized Identifiers (DIDs). It focuses on enabling secure, private, and asynchronous messaging between parties without requiring user involvement in every interaction.

DIDComm supports various types of messages beyond credential-related ones, making it versatile for broader use cases like credential revocation or renewal. It can complement OID4VC by enabling persistent communication channels after credentials are issued or verified.

### Credential Handler API (CHAPI)

The Credential Handler API (CHAPI) is a browser-based protocol designed to facilitate the secure exchange of digital credentials between issuers, holders and verifiers. It provides a mechanism for digital wallets to interact with third-party websites, enabling credential issuance, storage, and presentation in a way that prioritizes user control, privacy, and interoperability.

Both DIDComm and Chapi gained popularity in the early days within the decentralized identity community, but have since lost relevance compared to OID4VC or the Digital Credentials API.

# Part 2 - Ecosystems & Regulations

## Introduction

### Regulations - The catalyst for global adoption

While standards provide the technical foundation for decentralized identity, it is regulatory frameworks that are rapidly becoming the primary catalyst for widespread adoption. As governments worldwide recognize both the potential benefits and risks of digital identity systems, they are increasingly establishing legal frameworks that mandate specific approaches with decentralized models gaining significant favor.

Unlike previous digital transformations that were primarily driven by market forces or technological innovation, the shift to decentralized identity is being significantly accelerated by regulatory intervention. This represents a fundamental change in how digital infrastructure evolves — with governments taking a more proactive role in establishing guardrails and requirements rather than simply responding to market-developed solutions.

In 2024, the first regulation to force the adoption of decentralized identity and identity wallets was published by the European Union (EU). It is called "eIDAS2" and it introduces digital identity wallets for individuals and organizations in order to give them more control over identity data across all aspects of their life. As a result, the eIDAS2 regulation is expected to transform the digital landscape in Europe and

it is already being copied around the world. You can read more in our eIDAS2 ebook.

But it is not only European regulators looking at the introduction of identity wallets: In the US, a quickly growing number of states have already introduced mobile driving licenses and ID wallet apps. For example, Louisiana launched a digital ID in 2018, which is being used by more than 66% of eligible adults. In California, nearly 600,000 residents installed the mobile ID app within the first few months of the program's launch. Similarly, we see a lot of movement from governments in the UK, the middle east, various Asian countries, Australia, New Zealand and Africa.

This regulatory momentum creates both opportunities and challenges. For organizations, it provides clarity and certainty around implementation requirements, potentially reducing the risk of investing in new technologies. For technology providers, it establishes clear market demand while constraining certain design choices. For individuals, it promises greater data control while raising questions about how these systems will be governed and overseen.

The following sections will provide an overview of the current regulatory landscape and how it is reshaping digital identity across jurisdictions while mapping regulations to the corresponding ID ecosystems and standards. At the end of the day, understanding this regulatory landscape isn't just about compliance. It provides crucial insight into how decentralized identity will evolve from promising technology to essential infrastructure over the coming decade.

## Identity ecosystems - The networks of trust

While standards provide the technical foundation and regulations create the legal frameworks, identity ecosystems represent the operational heart of decentralized identity. These collaborative environments transform abstract capabilities into functioning networks that deliver tangible value across organizations, industries, and borders.

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 them some of the internet's biggest problems like privacy and compliance issues, user lock-in effects, rising fraud and identity theft.

In 2024, we witnessed one of the EU's ID ecosystems (the EU Blockchain Service Infrastructure, EBSI) mature, with several so-called "Large Scale Pilots" to demonstrate use cases across borders and industries. New consortia emerged in the private sector -like Ayra, IATA or CHEQD - as well as public and private partnerships in Europe, the US, the middle east and APAC. Moreover, large players in payment, banking and crypto are looking at (or have already started to work on) building their own ID ecosystems as a way to future-proof their business and create new products and services.

While it is still early for ID ecosystems, there is also a lot of movement making us optimistic about an exciting multi-ecosystem future over the next two to five years.

For organizations navigating the decentralized identity landscape, understanding these ecosystem dynamics is essential for making strategic decisions about which initiatives to join, how to leverage their capabilities, and where to invest resources for maximum impact.

## The relation between regulations and ID ecosystems

Regulations and ID ecosystems are closely connected, but they are not the same. In a way, regulations and ID ecosystems can be thought of as two complex, dynamic and mutually reinforcing phenomena.

### Regulations drive ID ecosystem adoption.

First, regulations mandate decentralized identity. Laws like the EU's eIDAS2 are directly forcing the adoption of decentralized identity technologies, specifically digital identity wallets. This is a significant shift, as it moves away from voluntary adoption to mandated implementation. By establishing a legal framework, eIDAS2 and similar regulations are creating a foundation for widespread use of these technologies.

Second, regulations are creating legal certainty and trust. They provide the necessary legal certainty and trust for individuals and organizations to embrace digital identity solutions. This is essential for building robust ID ecosystems. When governments establish rules and standards, it fosters confidence in the security and privacy of digital identity.

Thirdly, there is a global regulatory trend as more and more policymakers and regions explore and implement digital ID initiatives, indicating a worldwide recognition of the need for regulated digital identity frameworks.

### ID Ecosystems enabling regulatory goals.

First, ID ecosystems, especially those built on decentralized principles, empower individuals with greater control over their identity data. This aligns with the regulatory goals of enhancing privacy and data protection, as seen in eIDAS2. By moving away from centralized data silos, ID ecosystems address concerns about data breaches and misuse.

Second, ID ecosystems support cross-border interoperability. This is, for example, one of the explicit goals of the eIDAS2. The aim of enabling seamless cross-border digital interactions. ID ecosystems, particularly those with shared data registries and governance frameworks, are crucial for achieving this interoperability. The EU's EBSI is another example of an ID ecosystem designed to support cross-border use cases.

Third, ID ecosystems, with their security guardrails, can help combat fraud and identity theft, which are major concerns for regulators. Regulations can set standards for security and authentication within ID ecosystems, further strengthening their ability to prevent fraud.

## Conclusion

Regulations act as catalysts for the development and deployment of ID ecosystems. They create the necessary market demand and legal framework for these technologies to flourish.

As ID ecosystems mature, they can provide valuable feedback to regulators, helping to refine and improve regulations. The "Large Scale Pilots" of the EBSI are a good example of this interaction.

Today, it has become apparent that the world is looking at a "multi-ecosystem future", where various ID ecosystems coexist and interoperate. Regulations will play a vital role in ensuring that these ecosystems are compatible and secure. The involvement of the private sector, in creating ecosystems, shows that the regulation is creating a market that the private sector is willing to invest in.

In essence, regulations and ID ecosystems are mutually reinforcing. Regulations provide the legal and policy framework for ID ecosystems to thrive, while ID ecosystems provide the technological infrastructure to achieve regulatory goals.

In the following sections, we'll look at different regions and jurisdictions to better understand their current state of affairs with regards to the adoption of decentralized identity and identity wallets.

# Europe

Europe has been among the driving forces for regulating digital identity and identity wallets. Just like in the area of privacy and data protection with the General Data Protection Regulation (GDPR) in 2018, Europe is proactively regulating the digital world and setting a global standard that inspires replications by policy makers around the globe.

## European Union (EU)

After the first eIDAS regulation established an ecosystem for digital signatures that could be used for authentication, identification, and signing with legal validity across borders, the EU took a significant leap forward with eIDAS2, which went into force in May 2024, and represents the first regulatory framework that introduces digital identity wallets for individuals and organizations. As such, it follows Europe's consistent philosophy of putting citizens' rights and data sovereignty at the center of digital transformation. By establishing legal requirements for user-controlled identity, eIDAS2 addresses fundamental challenges of the digital economy including privacy concerns, fragmented identity systems, and the growing problem of identity theft.

In the EU, there are two identity ecosystems  that emerged from and are driven by the public sector.

### eIDAS2 & EUDI Wallet

A main goal of the eIDAS2 regulation is to provide citizens and organizations with ID wallets and, as a result, user-centric digital identities that are secure, private, and trusted enough to reduce fraud

and enable digital interactions across borders, organizations, and applications. Also, eIDAS2 forces governments and businesses to adopt ID wallets, creating a massive market for decentralized identity solutions, with estimates suggesting that over 450 million European citizens will have access to these wallets within five years.

### EU blockchain Service Infrastructure (EBSI)

EBSI is a consorted effort by the EU to introduce a shared blockchain infrastructure for all EU member states. Naturally, digital identity has always been one of the main use cases for early adopters. As a result, EBSI is also being used by a number of so-called “Large Scale Pilots” where governments and businesses demonstrate cross-border use cases to showcase the value of EBSI.

The relation between these two ecosystems can be thought of as complimentary. Simplified speaking, eIDAS2 may be understood as the system used for use cases with high failure costs (i.e. required a high level of trust and assurance) and comes with a relatively limited set of digital credentials. EBSI has the potential to fill the gaps and provide an infrastructure for use cases that are not directly covered by eIDAS2.

From a technical and standards perspective, the EU is leveraging a broad variety of standards. For example, on the credential layer all major standards are being utilized, including **Mobile driving license (ISO/IEC 18013-5)**, **SD-JWT VC** for selective disclosure and privacy preserving data sharing and **W3C Verifiable Credentials (VCDM v1.1 and v2.0)**. On the protocol layer, the EU’s if focused on **OpenID4VC** (OID4VCI, OID4VP) and potentially **Digital Credentials API** and on the layers of identifiers and registries, both tradition and novel technologies and

standards are being used from **X.509 certificates** and **traditional PKIs** to **Decentralized Identifiers** (e.g. did:ebsi, did:key) and a permissioned **blockchain** (EBSI).

*Note that the table above only represents a subset of the standards aligned with the focus of this eBook. The full list can be found here.*

## Switzerland

While the EU has been working on decentralized identity and ID wallets for a couple of years now, Switzerland has been carefully watching and working on their own ID ecosystem. While remaining aligned with the core premises of the EU's ecosystem there are certain differences in terms of technologies and standards.

For example, on the layer of credentials, Switzerland is proposing the use of **SD-JWT VC** to allow for privacy preserving data sharing (and potentially W3C Verifiable Credentials in combination with BBS+ signatures) in combination with **OpenID4VC** (OID4VC, OID4VP) on the protocol level and **Decentralized Identifiers** (e.g. did:tdw; did:webvh) combined with **OpenID Federation** which uses JSON Web Tokens (JWTs) to create "trust chains" that assert public keys and include rich metadata to allow for privacy preserving credential life cycle management and verification.

## UK

The UK government published a first (alpha) version of its “digital identity and attributes trust framework” on February 11, 2021 - an important first step towards establishing a national approach for digital

identity solutions. This initial prototype of rules and standards was intentionally released as an unfinished version to allow interested parties to provide input and shape its development. In this sense the UK took a comparable, yet slightly different approach from the EU with regards to involving the private sector into the regulatory process (e.g. EBSI's "Early Adopters"; EBSI's and eIDAS2 "Large Scale Pilots").

Following the publication of the alpha version, the government continued to refine the framework. In mid-2021, a public consultation was launched to gather views on how the digital identity system should operate. In mid-2022, an updated (beta) version of the trust framework was published.

As of 2025, the government has been working on this framework for over four years, collaborating with industry, academia, civil society groups and members of the public to refine and improve it. Based on the latest information published by the UK government, the main standards that are being used include **W3C Verifiable Credentials (VCDM v1.1)** on the credential layer combined with **OpenID4VC** (OID4VC, OID4VP), on the protocol level.

# North America

## United States (USA)

In the US, we witnessed different adoption streams that utilize different technologies and standards. That being said, particularly the **Mobile driving license (ISO/IEC 18013-5)** standard has seen significant adoption as various US states are rolling out ID wallets with mobile driving license as the initial use case (e.g. Arizona, California, Colorado, Delaware, Georgia, Louisiana, Maryland, Mississippi, New Mexico, Oklahoma, Utah). In line with state-level government action, major technology companies like Google and Apple (among others) are providing the wallet infrastructure to support these new credentials standards, but are also pushing certain protocol standards like the **Digital Credentials API**.

But adoption is not only limited to this use case, considering developments in industries like education, employment and health care among others that utilize different standards like **W3C Verifiable Credentials** (e.g. Open Badge 3.0, CLER 2.0) and **OpenID4VC** (OID4VCI, OID4VP) on the protocol layer.

## Canada

Canada has been pioneering decentralized identity and ID wallets early on. For example, British Columbia's Verifiable Credential Issuer Kit, which was a proof-of-concept project aimed at demonstrating how governments can use self-sovereign identity (SSI) technology for secure credential issuance or TheOrgBook, a beta project launched in BC that aimed at allowing businesses to access digitally signed permits and incorporation documents online. The city of Vancouver has implemented digital credentials for permitting and licensing services issued via the BC Wallet mobile app. Similarly, Ontario's Digital Identity (DI) program aims to provide residents with a secure and convenient way to store and use government-issued IDs through a digital wallet app.

Today, Canada is starting to procure solutions enabling decentralized identity and ID wallets for the country utilizing of **W3C Verifiable Credentials, SD-JWT VC** and **Mobile driving license (ISO/IEC 18013-5)** on the credential layer, **OpenID4VC (OID4VCI, OID4VP)** on the protocol layer and **Decentralized Identifiers** as well as **X.509** certificates on the level of identifiers.

# APAC

## Australia

Australia has been making big strides towards establishing a new digital identity ecosystem which was established under the Digital ID Act 2024 and combines a voluntary accreditation framework with a government-managed identity verification system. The infrastructure prioritizes privacy, security and interoperability while avoiding prescriptive technical mandates for credential formats.

In this context, Austroads, the association of Australian and New Zealand transport agencies, is leading a significant project to develop a Digital Trust Service (DTS) for digital credentials, with a primary focus on digital driver's licenses and proof of age credentials. This initiative aims to harmonize digital identity across jurisdictions and ensure international interoperability and uses the **Mobile driving license (ISO/IEC 18013-5)** standard. While W3C Verifiable Credentials are not implemented, the selective disclosure principles align with DTS attribute-based verification. Also, Austroraods is participating in OID4VC standardization efforts. All of this shows the interest of Australian policy makers in the development of several standards (beyond mDL) and their possible application in the future.

Together the Austroads Digital Trust Service (DTS) project and the Digital ID Act 2024 complement each other and illustrate forward thinking initiatives that aim to enhance Australia's digital identity ecosystem.

## New Zealand

New Zealand is making significant progress in developing its digital identity ecosystem, with recent initiatives aimed at creating a secure, user-centric and interoperable framework for digital identity services.

The New Zealand government has finalized and implemented the Digital Identity Services Trust Framework (DISTF), which took effect on November 8, 2024. This framework establishes rules and standards for digital identity services, aligning with international best practices. Key aspects of the DISTF include privacy and security requirements for service providers, user consent-focused model and decentralized architecture for credential storage.

The DISTF aims to facilitate secure information sharing, protect against identity theft, and give users greater control over their personal data. To achieve these goals DISTF intends the use of **Mobile driving license (ISO/IEC 18013-5)** - and potentially **W3C Verifiable Credentials** and **SD-JWT VC** - on the credential layer, **OpenID4VC** (OID4VCI, OID4VP) on the protocol layer and **X.509 certificates** as well as **Decentralized Identifiers** on the level of identifiers.

## Thailand

Thailand is pioneering a transformative digital identity ecosystem through its National Digital ID (NDID) platform, which leverages blockchain technology to create a secure and collaborative infrastructure for digital transactions and identity verification. The system integrates multiple components, including a mobile app called ThaID and mobile network identification services to provide a comprehensive approach to digital identity management across public and private sectors.

The NDID platform connects various service providers with identity providers, primarily banks, enabling users to verify their identities electronically for a wide range of services including financial transactions, insurance, and digital lending.

With 9.2 million registrations as of March 2025, the system has shown significant growth and is actively expanding its reach to corporate sectors and government agencies, while also exploring potential cross-border digital ID services through strategic partnerships.

Today, Thailand is already working on enhancing their ecosystems with decentralized identity and ID wallets. The mains standards that being used include **W3C Verifiable Credentials (VCDM v1.1)** on the credential layer, **OID4VC** (OID4VCI, OID4VP) on the protocol layer underpinned by **Decentralized Identifiers** (did:ndid) and a trust registry based on Tendermint as **permissioned blockchain**.

# MENA

The Middle East and Africa are in a special position with regards to the adoption of new technologies. Considering that prior waves of innovative technologies have not been adopted at the same pace and degree as in other parts of the world like Europe, the US or APAC, these regions are “leapfrogging” from a relatively low level of technological advancement to a very high level, skipping intermediate steps.

Today, there exist a myriad of digital identity systems, including digital ID applications which are being extended with decentralized identity technologies to improve their utility and interoperability.

## Middle East

The Middle East’s digital identity initiatives are quite advanced. For example, the United Arab Emirates (UAE) stands out with its comprehensive digital ID system. The UAE's Emirates Digital Identity (Emirates ID) is a mature platform that serves as a comprehensive digital identification solution, integrating both physical and digital services. Saudi Arabia is also rapidly developing its digital ID infrastructure as part of its Vision 2030 digital transformation strategy.

Today, we see this area adopting **W3C Verifiable Credentials (VCDM v1.1)** on the credential layer, **OID4VC** (OID4VCI, OID4VP) on the protocol layer underpinned by **Decentralized Identifiers**.

## Africa

Africa's digital identity ecosystem is rapidly evolving, with countries across the continent prioritizing the development and implementation of digital ID systems to improve service delivery and foster economic growth. Over 500 million people in Africa currently lack official identification, hindering access to crucial services and exacerbating economic inequalities. The launch of the Decentralised Identity Foundation (DIF) Africa Special Interest Group in September 2024 further demonstrates the continent's commitment to advancing decentralized identity technologies

Today, African governments and other initiatives are looking into decentralized identity and identity wallets as a way to provide African citizens with holistic digital identities based on **Mobile driving license (ISO/IEC 18013-5)** and **SD-JWT VC** on the credential layer, **OpenID4VC** (OID4VCI, OID4VP) on the protocol layer and **X.509 certificates** as well as **Decentralized Identifiers** on the identifier layer.

# Conclusion

Decentralized identity is seeing growing adoption around the globe.

On a high-level, it makes sense to think about the “waves of adoption” for decentralized identity solutions and ID wallets. Given the special nature of identity, governments are a core enabler of this new technology. It is regulations that are creating new billion dollar markets - not only the superior user experience, higher privacy and security guarantees that are promised by decentralized identity. But there is something else that puts governments in a special position as enablers of adoption: They are highly trusted sources of a broad range of identity data. Therefore, governments are uniquely positioned to issue digital identity credentials to citizens and offer - or at least enable - identity wallets that are directly populated with such credentials to provide end users with immediate utility. Apart from governments, large enterprises like Google, Apple, Microsoft or Amazon are rolling out solutions to support the adoption of ID wallets. Similarly, vendors of traditional identity solutions are preparing offerings for the market and their existing customer base.

Zooming out and refocusing on emerging regulations and ID ecosystems driven by the public sector, there are regional differences. For example, a different level of top-down adoption such as in the EU on a multi-national level compared to national-level (e.g. Switzerland, UK, Australia, New Zealand, Middle Eastern countries) or state-level (e.g. US). While regulators are pushing for the adoption of decentralized ID globally, the private sector is being involved in the process of policy

making and roll-out, such as in the case of EU's Large Scale Pilots or public-private partnerships as in the case of Thailand.

That being said, the US has rapidly achieved adoption of ID wallets via the introduction of Mobile Driving License (ISO 18013-5) in a growing number of US states, whereas Europe has been leading regulatory efforts but is still preparing for the large-scale roll-out until 2027.

Below you can find a table that illustrates which standards are adopted in which regions.

| Region | Registry Layer | Identifier Layer | Credential Layer | Protocol Layer |
|---|---|---|---|---|
| Europe | Traditional PKI (X.509), Blockchain (EBSI) | X.509, DIDs (did:ebsi) | W3C VC (v1.1, v2.0), ISO mDL, SD-JWT VC | OID4VC; ISO 18013-7 and Digital Credentials API (in evaluation) |
| Switzerland | OpenID Federation | DIDs (did:tdw, did:webvh) | SD-JWT VC | OID4VC |
| UK | - | - | W3C VC (v1.1) | OID4VC |
| USA | Traditional PKI (X.509) | X.509, | ISO mDL, W3C VC (v1.1, 2.0; Open Badge 3.0, CLER 2.0) | OID4VC; ISO 18013-7 and Digital Credentials API (in evaluation) |
| Canada | Traditional PKI (X.509) | X.509, DIDs | ISO mDL, W3C VC, SD-JWT VC | OID4VC |

| | | | | |
|---|---|---|---|---|
| Australia | Traditional PKI (X.509) | X.509 | ISO mDL (alignment with W3C VC principles) | OID4VC (standardization efforts), potentially ISO 18013-7 |
| New Zealand | Traditional PKI (X.509) | X.509, DIDs | ISO mDL, W3C VC, SD-JWT VC | OID4VC |
| Thailand | Blockchain | DIDs (did:ndid) | W3C VC (v1.1) | OID4VC |
| Middle East | Custom | DIDs | W3C VC (v1.1) | OID4VC |
| Africa | Traditional PKI (X.509) | X.509, DIDs | ISO mDL, SD-JWT VC | OID4VC |

You can also learn more about decentralized identity, global adoption and how to get started in our Decentralized Identity Playbook.

# What to do now?

If you want to start your journey adopting decentralized identity and identity wallet standards, if you have any questions or want to contribute and help us keep this document up-to-date please *contact us* or start building with our open source infrastructure here.