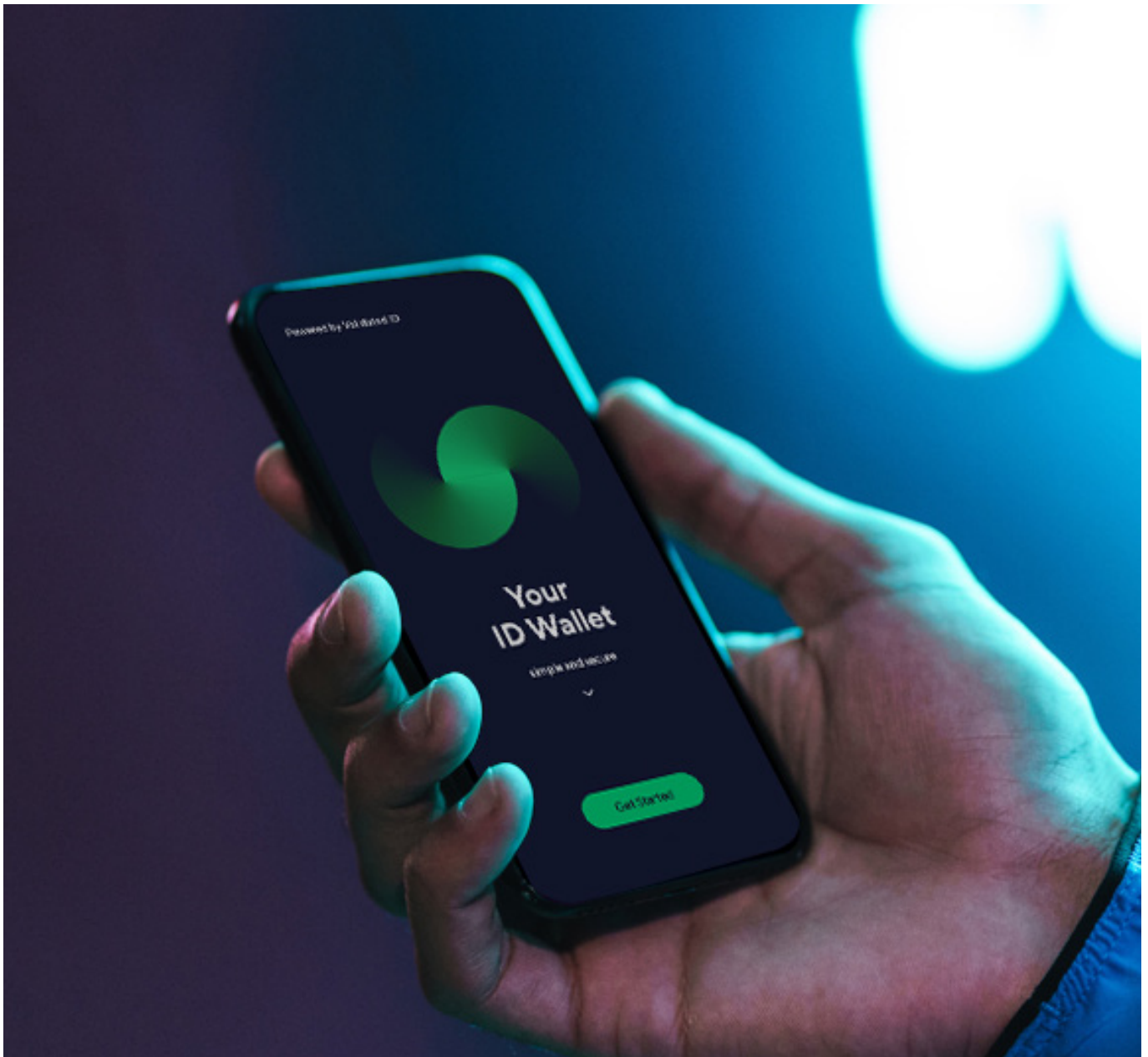
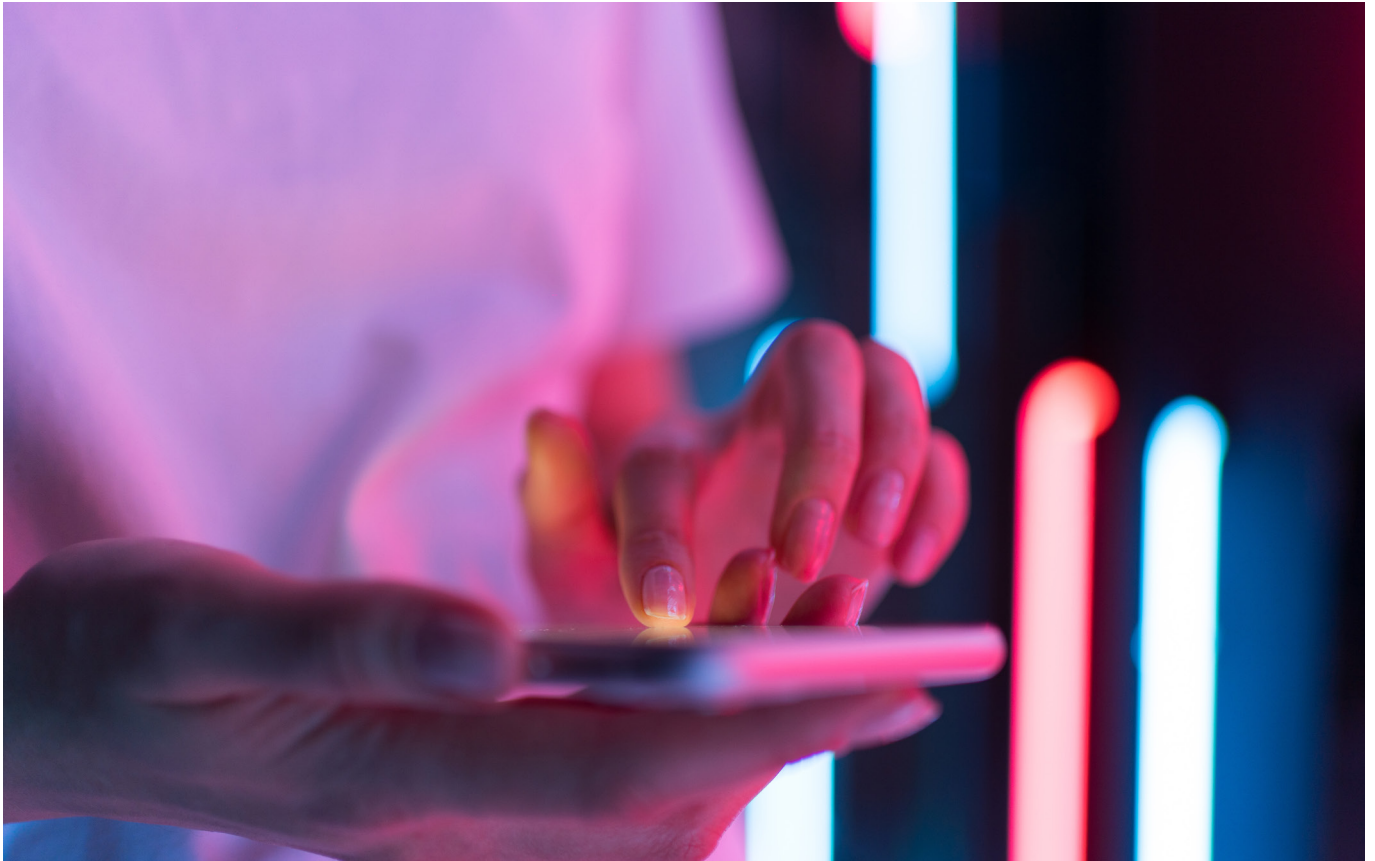


VIDidentity Whitepaper

Control your digital identity



Summary



Since the beginning of the online revolution, the secure validation of the real identity of people in the digital environment has presented itself as a problem – both for users, who have seen their privacy and control over their personal data jeopardized and for companies, who are constantly suffering the cost of inefficient identification and repeated security breaches.

To solve this, we are developing VIDidentity, which enables users themselves to own, control and manage their identity by means of a digital wallet (a mobile app), which acts as a digital record or container of identity attributes and transactions.

Simply put, VIDidentity is a self-sovereign identity on the blockchain, a permanent identity that can only be accessed in full by the person or entity to whom it belongs, yet portions of that identity can be shown to any individual, organization, or agency whenever it becomes relevant. Since self-sovereign identities are decentralized and encrypted, identity theft or incidents become much less of a problem.

The market is ready for this shift in paradigm in online identity. This is driven by worries about cybersecurity and compliance concerns, the need to digitize processes across all sectors, issues with the current digital identity management system and the COVID-19 impact on identity. Validated ID is very well positioned in this market, with 10+ years of experience, more than 2500 customers in 30 countries and an established network of partners and customers.

Regulation

VIDidentity is built on a new digital identification paradigm known as Self Sovereign Identities. Only you have complete control over your information on your own personal identity wallet, VIDwallet, using VIDidentity. To authenticate yourself online, you can add Verifiable Credentials to your VIDwallet. These credentials are made up of identifying traits that have varying levels of trust based on the source of the data and the authentication method utilized. The SSI ecosystem is complicated, with several technical stacks and distributed ledger technologies.

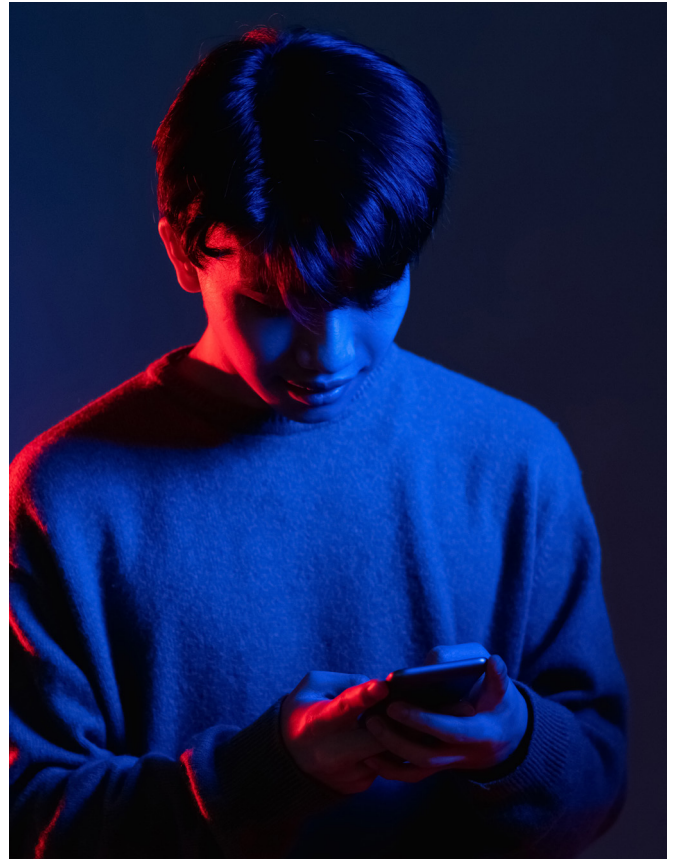
Validated ID is committed to provide an interoperable SSI solution that is independent of the infrastructure layer and compliant with various SSI technology stacks. We have already been accredited as a Trust Service Provider, and VIDidentity will be included in our TSP offering.

VIDidentity is the first SSI wallet that allows users to handle all their credentials, no matter which issuer and the SSI technology they use from the same wallet. The company works with several different international forums including: Alastria, Velocity Network, SOVRIN, Dalion, and the European Blockchain Services Infrastructure (EBSI).

Validated ID participated as an expert on PKI and SSI in the eIDAS bridge, an initiative of the European Commission. The main purpose of this program was to provide a bridge implementation and to test the interoperability between different provider implementations.

Validated ID is open to explore any use case that arises to any company, but we also review in this whitepaper some of the use cases and verticals where we anticipate a self-sovereign identity service will be a disruptive technology.

Finally, VIDidentity is already at work in several pilots and proof of concepts and has achieved several milestones that we want to share with you.



The Evolution of Digital Identity

The internet was created without a reliable way to manage your identity online. Since companies willing to offer online services or products must identify the users before granting access, it's a significant issue. As far as online identification is concerned, there have been three main models until now.

In the **traditional model of online identification** (or "siloeed"), **organizations issue digital credentials to users.** In other words, every time you interact with a new service or organization, you need to create a new credential, then remember the username and password. As a result, this model requires you to create and manage separate credentials for each relationship.

The second model (or "federated") **is where third parties act as identity providers** (such as Google or Facebook), issuing digital credentials that enable you to log in to other apps and services, providing a **single sign-on experience** (login with Google/Facebook/Apple, etc.). This allowed users to use the same identity for multiple sites.

Our current centralized systems are identity-centric and profoundly broken: companies misuse and sell personal ID information without consent, resulting in identity theft, data hacks, high cost of owning and managing personal data... **According to IBM¹**, data breach costs rose from USD 3.86 million to USD 4.24 million, the highest average total cost in the 17 years.

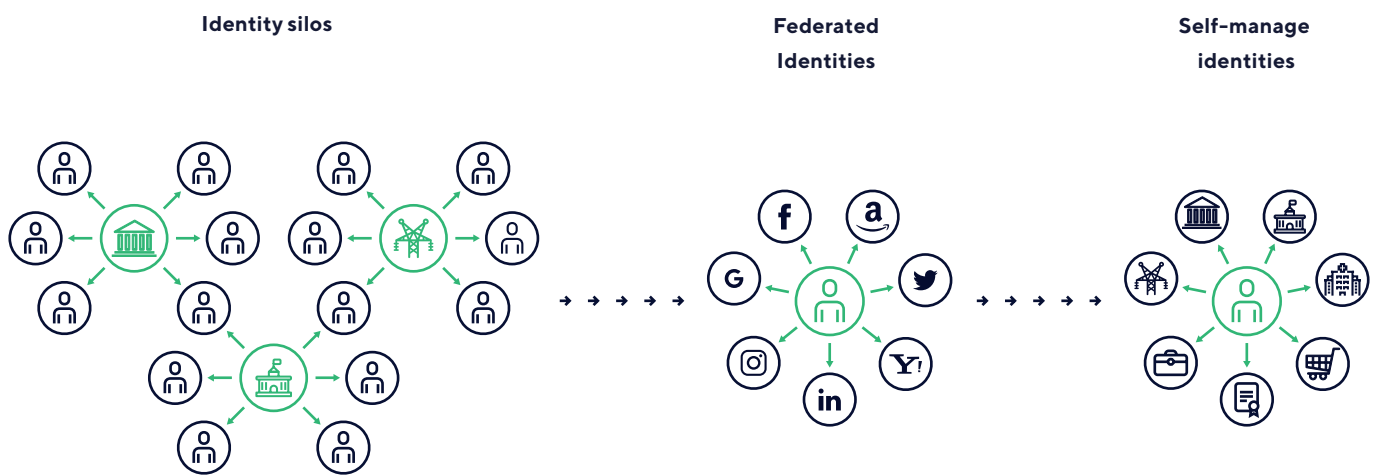
It is a nightmare for the user experience: 80% of users struggle to keep track of their passwords. An average email address is associated with at least 130 accounts and many people reuse weak passwords. One in five Europeans have experienced identity theft fraud in the past two years. Despite GDPR, **users can't control how their personal data is shared with third parties** by the identity providers with single sign-on models (GAFA). Neither of these centralized systems involve credentials that are verified or based on real life identities. In other words, **anyone can create a fake account.**

For the sake of comparison, **identification in the physical world** requires that an organization issues a **physical credential that attests who you are** to that organization. For example, your government will issue your national ID card that confirms that you are indeed a citizen of that country. There are currently some issues with physical credentials: it often requires a long, complex process and they can be **falsified or even lost**. In addition, they are **not private**.

If you want to get into a club, you need to prove that you are of legal age, so you show your ID at the entrance. This ID also lets them know your full name, your address, and in some cases even your parent's names. All this information is not needed for proving your age.

¹ <https://www.ibm.com/security/data-breach>

Self-Sovereign Identities: a paradigm shift



Recently, there has been a paradigm shift. The latest advances in technology such as blockchain technology, decentralized identifiers, and verifiable credentials have paved the way for **a new identity model: Self-Sovereign Identity (SSI)**.

In SSI, a secure and digital peer-to-peer channel is established between ID Issuer, ID Owner and ID Verifier. It allows the **exchange of credentials in a private way**, as they are **encrypted** and therefore not even the Self-Sovereign Identity system provider knows what is being exchanged. The process of issuing credentials becomes **more efficient**. **Additionally, SSI addresses fundamental trust issues in identity management by benefiting from the properties offered by the blockchain technology**. Plus, it allows **selective disclosure**: the user can now select only the pieces of information that are required. In our previous example, going to a bar now would mean only showing your date of birth as opposed to showing the entire document.

The technology allows the **verification of credentials at anytime, anywhere**, and even if the organization that initially issued the credential is no longer active. The data is not stored on servers, but it is the user who stores the information. In this way, there is no longer a need to remember multiple passwords as you only need to remember the password to your wallet.

To understand how the technology works, it is important to understand three important pillars: and **Verifiable Credentials, Decentralized Identifiers, and blockchain technology**.

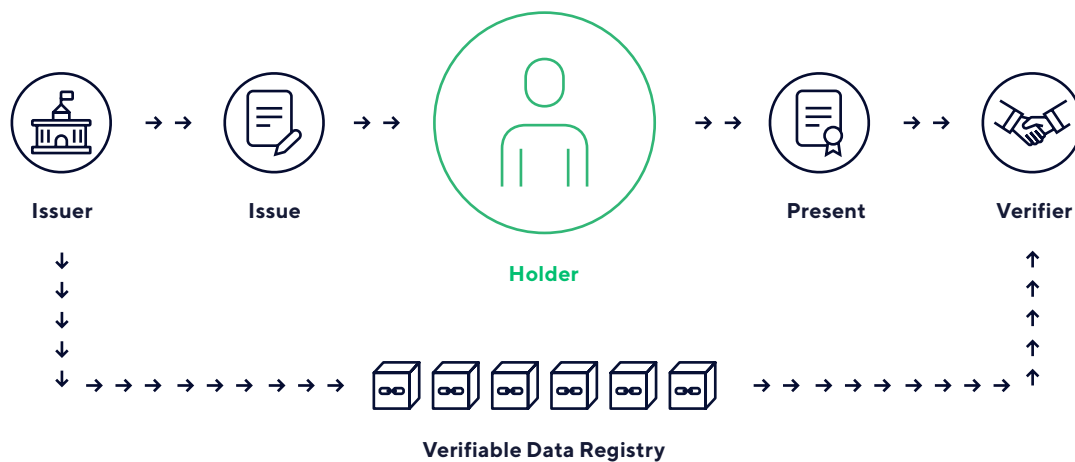
Verifiable Credentials

Verifiable Credentials (VC) are **the digital counterpart to a physical ID**: in the same way your national ID is a set of attributes such as your name, last name, date of birth, expiration date, address, etc; a Verifiable Credential is a data object that includes a set of attributes that are digitally signed through a combination of public key cryptography and privacy-preserving techniques.

With SSI, **the user is for the first time at the center of the identity transaction**. There are three roles involved in identity: the **issuer** who signs the different attributes and sends it to the **holder**; the holder or owner of the credential and the **verifier**, the institution or person that needs proof of identity and verifies the attributes. In this scenario, there is trust among all the roles.

VCs (Verifiable Credentials) are comprised of a set of attributes. The user can **selectively disclose** which credential he would like to share in any interaction minimizing the amount of personal data exposed.

In contrast to physical IDs, **Verifiable Credentials are easier and quicker** to obtain from the issuers, cannot be tampered with because they **are always verified and are entirely private** to the user.



Decentralized Identifiers

An identifier in the physical world is our name, our social security number, our id number, our phone number, or any other unique designation that links us with specific information.

On the Internet, our identifier is usually our email, our social network profile, etc., that often come from intermediaries like Google, Facebook, etc., which has important consequences for our privacy, since that data collected, and share are not under our control.

This changes in Self-Sovereign Identities by using Decentralized Identifiers (DIDs). There are two types of DIDs: **public or private DIDs**. Official institutions issuing official passports or IDs would issue a public DID when creating a Verifiable Credential to go with the document. **Private DIDs** are the identifiers of the users. A user can have more than one DID that can be created by himself without the need of a central authority. Because they are decentralized, they are always verifiable. This also means that all a person's data is not tied to a single individual profile, that could be lost, and can create as many profiles as they wish to protect their privacy.



Blockchain and Distributed Ledger Technology (DLT)

In a simplified way, a blockchain is a ledger or a transactions log, that everyone can have on the internet, where anything that you write on will not be deleted or changed and can be checked with everyone else's books to see if it is true. In other words, it is the **technology that allows to see changes in databases through a peer-to-peer network, that replicates itself across all nodes of the network.**

Distribute Ledger Technologies (DLT) are ledgers distributed on a network of nodes that can be build using the blockchain technology.

There is an important **distinction to be made between public and permission ledgers.** Both public and permissioned **ledgers** are decentralized: there is no authority that controls it. In public ledgers, anyone can participate and check any transaction. Sometimes this is not ideal, for privacy reasons or otherwise. **Permissioned ledgers** are networks where users need permission to join, and the operators can selectively place restrictions while configuring the networks. In addition, transactions are not visible for people outside the network.

For both types of blockchains, there are three different levels of access: read-only, read/write, and admin. For public blockchains, anyone can read the blockchain; however only write access is granted after providing a proof-of-stake or proof-of-work for the network (a consensus mechanism, an algorithm that determines who can add the next block of transactions to the chain). For permissioned blockchains, the administrators of the network define who has what level of access.

Translated to identity, **everyone** in a Distributed Ledger Technology network **can see which credentials are valid and who says they are valid** but without having to share the information. In this way, the institution or people who need to verify your credential, they only check the validity of your credential, and **if the issuer is valid.** In this way, **no personal data is stored** on the network, only DID documents or hashes of DID documents.

In our previous physical world example, when having to share your birthdate to show that you are of legal age, in this case the person checking your ID will not need to see if your birthdate is true, but rather, if the government's signature of your ID is valid, since the government issued your ID.

Characteristic of an SSI solution

- Decentralized system of identity.
- Standard protocols for data exchange and data modeling.
- Companies become trusted issuers (and client data become credentials).
- Client self-manages own credentials, building up his/her digital identity.
- Secure cryptographic verification through reliable immutable distributed registry (blockchain).
- Establishes a trust framework among the various parts playing a role in all digital interactions.
- Improves authentication and access procedures by securely eliminating repetitive password usage and slow bureaucracy, while respecting maximum privacy.
- DLT serves as Decentralized Public Key Infrastructure (DPKI).

The Benefits of Self-Sovereign Identity

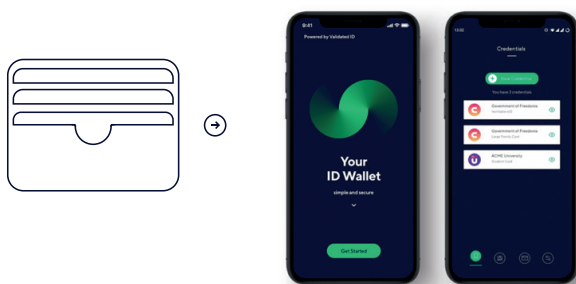
- **User-centric:** Users are in full control over their data.
- **Cost reduction:** Optimization of onboarding and KYC (Know Your Customer).
- **Global interoperability:** Faster identification of clients in global transactions through blockchain technology and a common credential ecosystem.
- **Privacy-by-design:** It supports compliance with GDPR (General Data Protection Regulation) due to not storing sensible data and considering user explicit consent from the very beginning.
- **Better UX/UI:** Secure one-click authentication.
- **Better user satisfaction:** Superior service, superior feedback.
- **Protection targeting anti-fraud and identity theft:** Secure processes of unchallenged identification of clients and consequent AML (Antimoney laundering) compliance.



VIDchain

VIDchain aims to solve the current digital identity related crisis by providing a service where you can own, control, and manage your own digital identity from your phone. **VIDidentity is based on a new paradigm of digital identity called Self Sovereign Identity (SSI)**, and it's built on top of blockchain technology.

With VIDidentity, only you have full control of your information on your own personal identity wallet, **VIDwallet**. You can have all your personal data (such as your driving license, your passport, your vaccination credential, etc.), on your phone.



In a similar way that you use your physical IDs to identify yourself in the real world, you can add Verifiable Credentials to your VIDwallet to authenticate yourself online.

These credentials are made of identity attributes, with different degrees of confidence depending on the origin of the information and the means of authentication used. From less reliable sources, such as social networks, to robust systems such as biometrics, official identification systems or even face-to-face identification. All these attributes are valid for different operations with different security requirements, and they allow a broad digital identity to be formed depending on the intended uses.

With VIDidentity, you can **share selected pieces of information from your credentials** that are requested to you by scanning a QR code, without disclosing all your personal information (for example, you can share only your birthdate from your national ID to prove that you are of legal age).

This way, instead of remembering hundreds of passwords, you will only need to login to your wallet. You can do so by setting up a password or by using biometrics.

The SSI ecosystem is complex and there are different technological stacks and DLTs (Distributed Ledger Technology). In terms of product, we are focused on delivering an **interoperable SSI solution, technology agnostic of the layer of infrastructure and compliant with different SSI technology stacks**. Most of our competitors are very blockchain-focused on low level and infrastructure layers. Our users will be able to handle all their credentials, no matter the issuer and the SSI technology they use from the same wallet.

VIDidentity is also unique **in bridging SSI with legacy IDs**. VIDidentity lets the user create SSI credentials from digital certificates or even physical IDs, and lets companies interact with decentralized identities with well settled protocols like OpenID.

In eIDAS 2.0, **all companies that issue or verify SSI credentials must be Trust Service Providers**. These certification processes are costly and time consuming. We are already certified as a Trust Service Provider and VIDidentity will be part of the offering as a TSP and will relate to the current services to enrich the portfolio. This is a significant entry barrier and most of our competitors will not cross the chasm.

Architecture

To solve the online identity problems, VIDidentity provides a service to own, control, and manage your own digital identity from your phone, built on top of blockchain technology. The VIDidentity architecture revolves around the following components:

1. **VIDcredentials:** With VIDcredentials, entities can issue verifiable credentials through a simple API without having to deal with the complexity of SSI.
2. **VIDwallet** is an app that helps users to manage all their personal data. The information remains confidential under the user's control.
3. **VIDconnect** helps entities interact with users by requesting credentials with a very simple integration. It is compatible, for example, with the well-known OpenID protocol.
4. The **VIDidentity API** is the core of the solution. It handles all messaging across all components, as well as core operations.
5. VIDidentity can work with different **decentralized networks** making it a **ledger agnostic solution**.

With these components, the necessary infrastructure can now be created to be considered for the issuance and acceptance of verifiable credentials with the following modules:

1. **Claims Issuer:** the issuer creates and certifies credentials in a portable and signed format on the blockchain, making them available to the holder via push messaging to their identity wallet.
2. **Claims Verifier:** when the user presents a credential, the claims verifier checks the cryptographic evidence stored in the credential.
3. **VIDwallet:** an app where the user holds all their credentials in one place and use them for authentication, authorization, identification, and other processes wherever these credentials are accepted.



Market

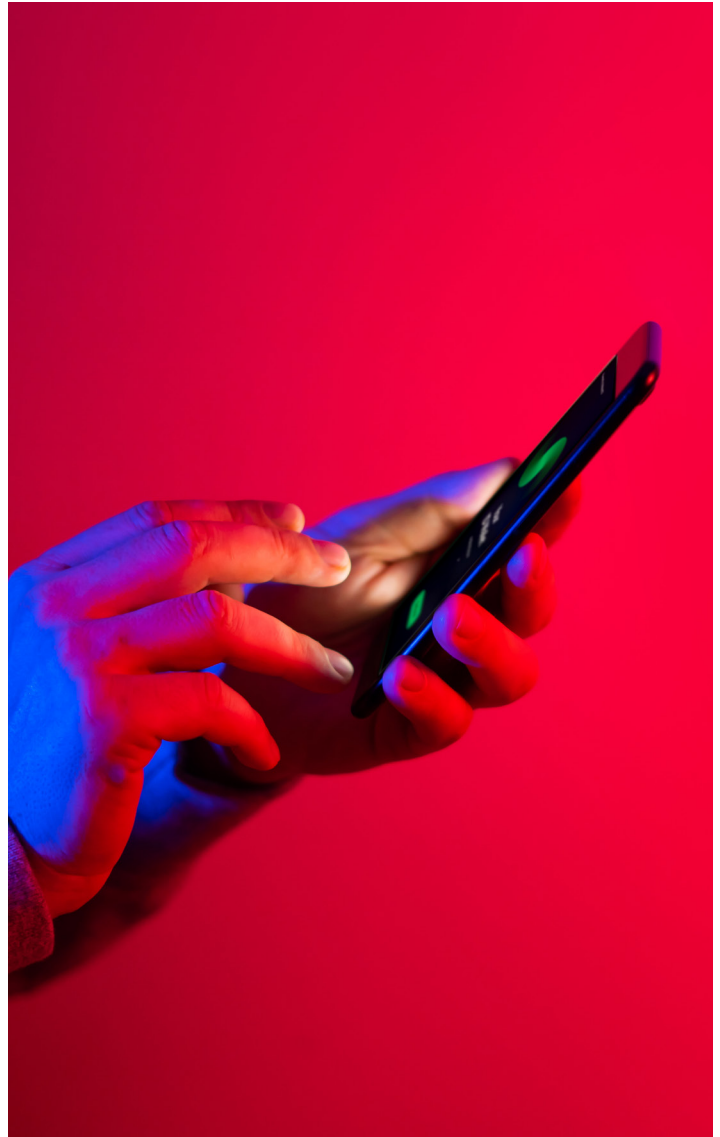
In today's economy, where our digital identity is at risk of being hacked and our data is constantly being exploited, having access to your own digital identity can improve your financial situation, protect your privacy, and give you instant access to services and opportunities that otherwise would have been inaccessible. According to our findings, the market is ready for this shift in paradigm. There are four market trends that are driving this technology:

1. Cybersecurity and compliance concerns

- A desire to improve privacy is being driven by worries about **deep fakes, artificial intelligence being exploited, and distrust of greater surveillance.**
- We are seeing many data breaches and cyber-attack cases happening lately. For example, according to Varonis, a data security company, **7 million data records are stolen every day.**
- According to Norton's research, in 2021, **208 million people in ten countries will experience identity theft.**
- According to Accenture, **a lack of trust costs global brands \$2.5 trillion each year** as customers abandon them in favor of competitors.
- Scandals such as Cambridge Analytica have demonstrated that current data management and data governance methods have serious flaws.

2. Digitalization across sectors

- In our increasingly digital society, we are growing **increasingly dependent on online systems** for storing and sharing our personal information. You can now easily **complete everyday tasks entirely online**, including online shopping, renting an apartment, applying for a job, opening a bank account, filing your taxes, etc.
- According to A2Z Research, in the United States, for example, seamless and secure sharing of medical information between companies increases productivity by \$205 billion (1% of the GDP).



3. Issues with the current digital identity management system

- Currently, most regulations for electronic transactions are focused on government-to-citizen transactions. As a result, private entities can provide legally enforceable, trusted, and qualified electronic services for identity, authentication, and authorization. This means that the current digital identity system does not allow individuals to control their identities.
- In the current system, you **need many physical documents to identify yourself**, such as national IDs, driver's licenses, passports, property titles, educational credentials, and birth certificates. Using self-sovereign identity, individuals can manage all their documents digitally and store them in a single digital wallet, allowing them to be portable.

4. COVID-19 impact on identity

- Restoring social confidence and allowing safe movement will be priorities soon, as government lockdowns are removed, and individuals and businesses return to normalcy. This can be done by using **digital identification and immunity credentials**.
- People **learn, acquire skills, and work in novel ways** because of digital technology, such as online courses, virtual recruiting, collaborative tools, and remote work. This will require frictionless interaction between individuals, companies, and technologies, improving trust and transparency.
- To **revive the travel and tourism industry**, government and business efforts are needed. Every day, tens of millions of passengers pass through airports and other transportation hubs worldwide.

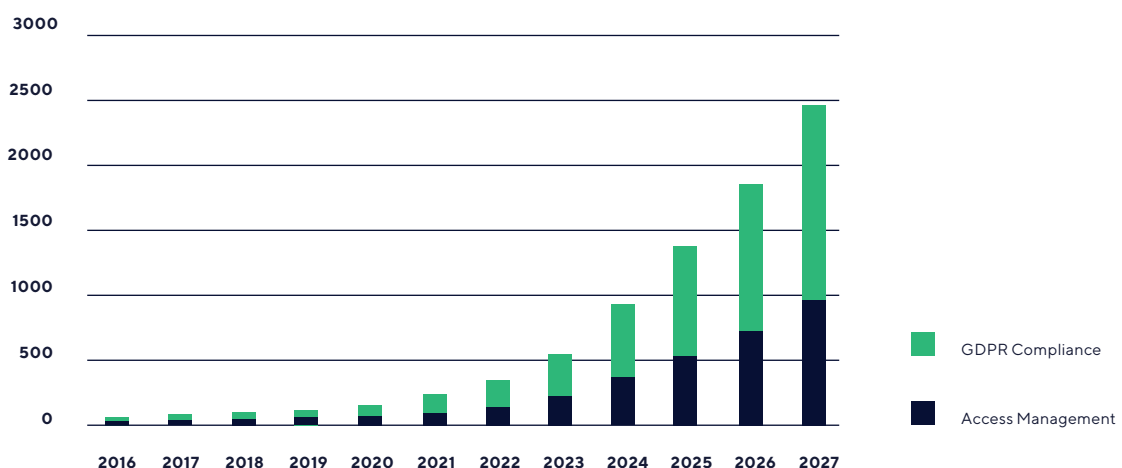
Market Share

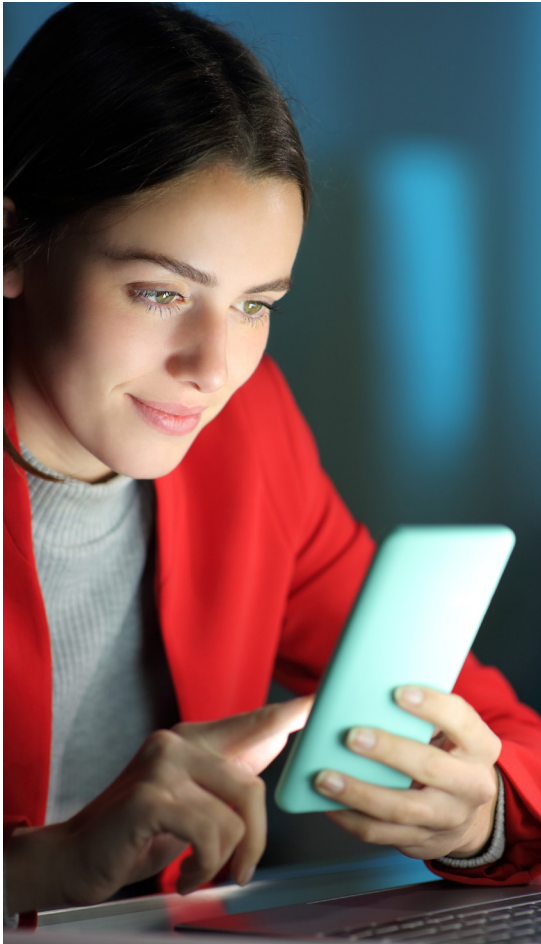
According to A2Z Market Research, the global Self-Sovereign Identity market share revenue will grow from **348.1 million USD in 2022, to 2 467 million USD, a 609 % growth.**

By application, access management represents 61 % of the market share, while GDPR compliance applications represents the remaining 38 %.

By sector, the biggest market share is represented by the banking industry (20 %), followed by air travel and government.

Global Self-Sovereign Identity Market Share Revenue, By Application, USD Million





Our experience

At Validated ID, we have experienced the rise of this market. We have been involved in several PoC (Proof of concept) and pilots as described in the Projects and milestones section. While there is some concern regarding the new regulation (the new eIDAS), as SSI becomes mandatory for private companies in strategic sectors (Health, Banking, Insurance, Energy), many players are already open to this technology, and understand the impact. In addition, many companies are willing to improve the time and cost of client onboarding and solve the lack of security and legal binding of business processes through the internet. **We envision that in the future, decentralized Self-Sovereign Identity and Verifiable Credentials will disrupt the way we do everything on the Internet.**

Although SSI is a relatively new technological development, Validated ID is a well-established, solid company with 10+ years of experience and brand recognition. We are **an experienced player** delivering digital signature services to more than 2500 customers in 30 countries through more than 200 distributors. As a result, we have a network of partners and customers of our TSP services where we can upsell, and cross sell. Validated ID has a dedicated team (+50 people) with market and product experience in the topic. In addition, we are present in SSI forums such as **Decentralized Identity Foundation²**, **Trust Over IP³**, Inatba, etc., where SSI decisions and knowledge are made. We already have a production-ready solution.

Other competitors in the space are the KYC industry. Know-Your-Customer processes are the steps required to verify customers' identity to do any transaction. The requirements vary across regulations and types of transactions, from face-to-face interviews, to uploading a picture of an ID card, depending on the risk involved. The main purpose of KYC is to prevent money laundering, financial fraud, and the financing of terrorism. In the European Union, this is regulated under eIDAS and AML5 regulation. As a result, KYC is a costly and time-consuming issue.

This is where Self-Sovereign Identities technology comes in, as Verifiable Credentials can be reused for KYC processes. Therefore, the KYC industry will experience a major blow with the introduction of eIDAS 2, which forces SSI technology for onboarding processes.

² <https://identity.foundation>

³ <https://trustoverip.org>

Regulation

The European Council is determined to make the current decade the **Digital Decade of Europe**⁴ by prioritizing among other actions to enable the **European Digital Identity**⁵ for all citizens of the Union. As part of the roadmap for this initiative, the proposal for the "eIDAS 2" (**European Digital Identity Framework**)⁶, currently under development, was presented on June 3, 2021.

"Every time an App or website asks us to create a new digital identity or to easily log on via a big platform, we have no idea what happens to our data in reality. That is why the Commission will propose a secure European e-identity. One that we trust, and that any citizen can use anywhere in Europe to do anything from paying your taxes to renting a bicycle. A technology where we can control ourselves what data is used and how."

Ursula von der Leyen, President of the European Commission, in her State of the Union address, 16 September 2020.

This initiative involves **the deployment of its European Electronic Identity, which will be of mandatory recognition by all agencies of the Member States of the Union**, at the same level as with digital certificates with the current eIDAS regulation; but it will **also be mandatory for private companies in strategic sectors** (Health, Banking, Insurance, ...). It is **based on the new paradigm of Decentralized Identities**, in the format of Verifiable Credentials (through registration and validation protocols in a blockchain) and designed so that the person can manage them and carry them in a cryptographic Wallet in their mobile, like the physical wallet with cards and cards of all kinds in the physical.

Wallet in their mobile, like the physical wallet with cards and cards of all kinds in the physical world. In addition, **all companies that issue or verify SSI credentials must be Trust Service Providers.**



⁴ https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_es

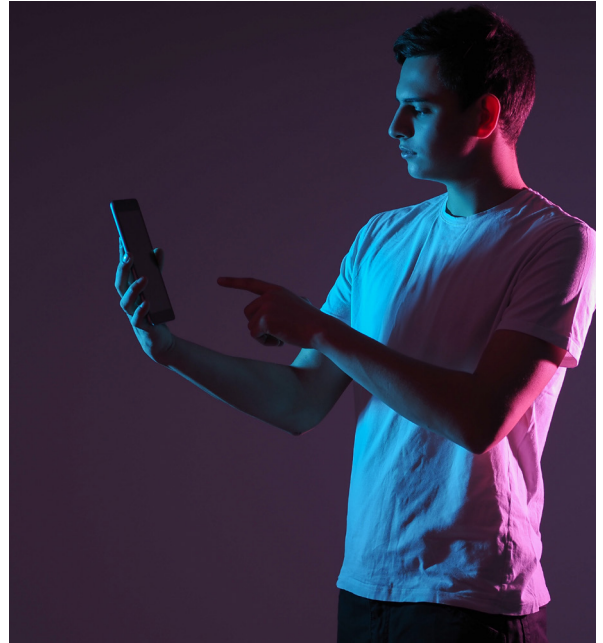
⁵ https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_es

⁶ <https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation>

Ecosystems

As we have introduced, nowadays there are different SSI ecosystems relying on different ledgers. There is not yet a full interoperability over those ecosystems, although the SSI community is working into this direction. From the user perspective, that means that you need to handle different wallets depending on the credentials, issuers, and verifiers you would like to relate with. That is a big pain in terms of user experience. VIDidentity is unique in having the ability to **work with different standards and Blockchain networks** to deliver a superior user experience. Our users will be able to handle all their credentials, no matter the issuer and the SSI technology they use from the same wallet.

- **Alastria**⁷ is the biggest Spanish blockchain Consortium with members such as Banco Santander, Telefonica, Deloitte, Ernst and Young, Everis and T-Systems.
- **Dalio** is a collaborative project, arising from the Alastria consortium and composed of large Spanish companies, aiming to help individuals autonomously manage their personal data digitally for use in any public or private setting.
- **SOVRIN**⁸ is a foundation with the mission to create the Internet's long-missing identity layer and provide a global public utility for digital identity to people, organizations, and things.
- **Velocity Network**⁹ is a blockchain-based open-source verifiable credential exchange utility layer that provides standardized communication protocols, governance, compliance, and payment rails, enabling trusted, private and secured exchange of career and education credentials between individuals and organizations.
- **The European Blockchain Services Infrastructure (EBSI)**¹⁰ is a joint initiative from the European Commission and the European Blockchain Partnership (EBP) to deliver EU-wide cross-border public services using blockchain technology.



⁷ <https://alastria.io/en/>

⁸ <https://sovrin.org>

⁹ <https://www.velocitynetwork.foundation>

¹⁰ <https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Home>

eIDAS Bridge

Public key infrastructure (PKI) has been, and is still, an essential technology that we use every day without even noticing. Although this mature technology has been available for decades, it has never become mainstream among society for identifying end users. This is where Self Sovereign Identity (SSI) comes in: this revolutionary paradigm aims to bring the control to the end users by means of using Verifiable Credentials (VC).

Although there are many credential wallets under development and several companies like us are looking forward to this prominent paradigm, the reality is that the legal framework is still not fully mature. The current regulation is the eIDAS regulation, mostly focused on traditional PKIs (Public Key Infrastructure) and Certificates. In June 2021, the European Commission (EC) approved a new draft of this regulation that states that the next generation identities of European citizens will be based on the SSI principles and backed by identity wallets.

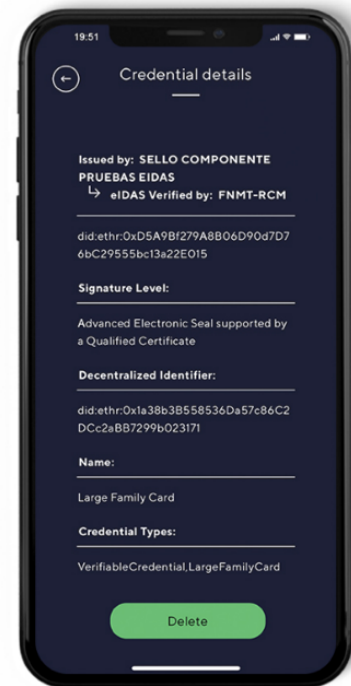
Therefore, the eIDAS bridge has been raised as an intermediate step. Validated ID participated as an expert on PKI and SSI in the eIDAS bridge, an initiative of the European Commission. The EC developed eIDAS bridge to promote eIDAS as a trust framework for the SSI ecosystem. The main purpose of this program was to provide an eIDAS bridge implementation and to test the interoperability between different provider implementations.

The eIDAS bridge consists of an API that allows you to sign and validate credentials using Qualified Electronic Certificates (QEC). Therefore, this tool is called a "bridge" since it connects the world of certificates with SSI credentials.

It should be easy to use for an end user, since the API provides three endpoints for three steps:

1. In the process of issuing Verifiable Credentials (VC), the issuer sends the certificate and associates it with the DID. The API stores the certificate in Confidential Storage.
2. Using his/her previously stored certificate, the issuer requests the API to sign a VC, and the API produces a VC with a CAdES signature.
3. The verifier sends a VC with CAdES signature to be validated, and the API returns the results.

The three steps outlined above illustrate the main functionalities developed for the eIDAS Bridge project and the interoperability of VC signed with our implementation. Therefore, we have included this code in our VIDidentity API, so our users can use their certificates when issuing VCs and validating VPs (Verifiable Presentation) containing QEC signatures.



User Journey

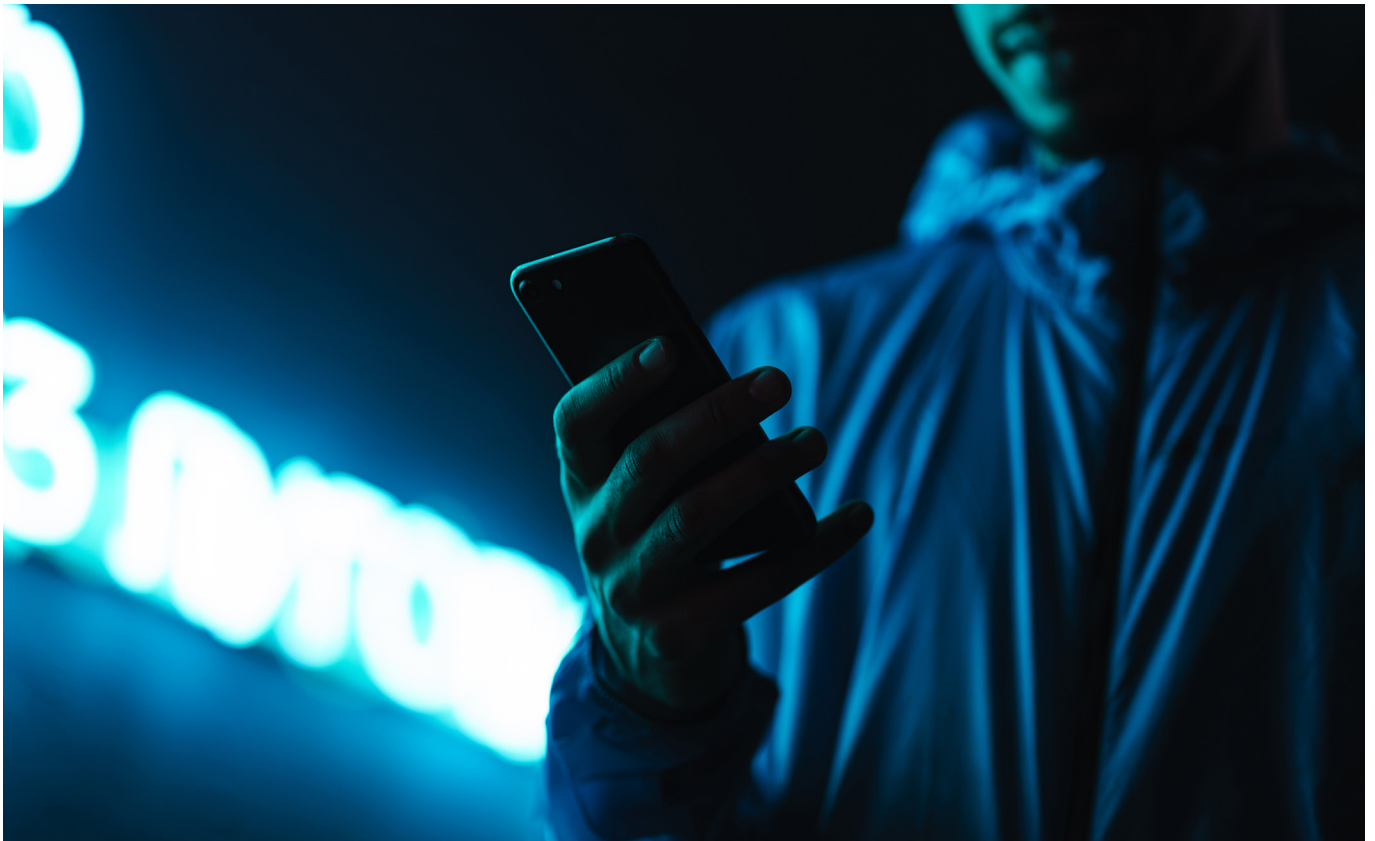
The user journey for VIDidentity is designed to be easy and straightforward so that our users can quickly and efficiently access their digital identity and use VIDidentity to perform identity-based services. When it comes to managing your digital identity, your login credentials are the first step. Here you can visualize the steps to successfully use VIDidentity for the first time:

- **Step 1:** First, when you visit a website for the first time, you are presented with the smart login screen. The smart login screen simply asks you to log in using your VIDidentity wallet. This way, you provide explicit permission to access your digital identity and provides you with a secure way to log in to websites and services.
- **Step 2:** Download the VIDwallet app on your phone. Once download, open the app and scan the QR code. You will see a request to add the new credential. Please, accept it.
- **Step 3:** Your credential is added to your wallet, and you can now login to the service.

Next time, you will only need to scan the QR code and unlock your wallet via PIN code or biometrics (for example, FaceID).



Demo



" <https://try.VIDidentity.net/demo>

We invite you to download VIDwallet and follow the tutorial/user journey demo from the link **<https://try.VIDidentity.net/>**." In this demo, you will be able to:

- a) Download and install the latest version of VIDwallet. The application is available for Android and iOS.
- b) Create a new credential by verifying your ID.
- c) Sign into a fake government portal using your credential and request a Large Family credential.
- d) Request a new university student card credential and apply for a discount with your Large Family credential.

Use cases

Validated ID proposes to your organization to start exploring this new electronic identity now, before it becomes mandatory, getting ahead to know the benefits of its implementation. In this regard, we offer you our knowledge, experience and technical-legal background to address the advantages of Decentralized Identities and Verifiable Credentials. We are very open to examining any other scenarios that may arise, but these are some of the use cases that we have identified:

Verticals

Cybersecurity and IAM Processes (Identity & Access Mgmt)

- Identification.
- 2FA Authentication: VIDidentity facilitates passwordless 2FA Authentication. VIDidentity can now be used for strong authentication for access to your portal.
- Authorization.
- ABAC: Access based on verifiable attributes (e.g., IoT).
- Issuance of verifiable credentials.
- Validation of credential submissions.

Compliance

- GDPR: The user manages and shares his data.
- Privacy by Design, implementation of zero-knowledge testing (ZKP).
- KYC & ALM: legal binding.

Interoperability and automation

- Interoperability-based e-Trust Ecosystems.
- (Government-University-Health-Health-Insurance-Banking-Utilities, ...).
- Automation of business rules based on Programmable Smart Contracts.

Verifiable credentials and e-signatures

- Good Health Pass.
- Issuance of competence diplomas.
- GDPR.
- Sales contracts.
- Employment contracts.
- Public Administration forms, electronic office.
- Informed consents, medical reports, etc.

Use Cases

Examples of using VIDidentity



Universities

Enables students' interaction with multiple schools for enrollments and tasks.



E-commerce

Streamlines and improves the security of purchasing processes.



Financial services

Optimize onboarding, KYC or AML processes with legal certainty.



Public Administration

It offers high-level solutions for remote digital identification.



Human Resources

Drastically improve employee onboarding times for certificates, diplomas, trainings and employment credentials.



Healthcare











Digital Verifiable Credentials bind an individual's identity to their test result or vaccination certificate COVID19.

Projects and milestones

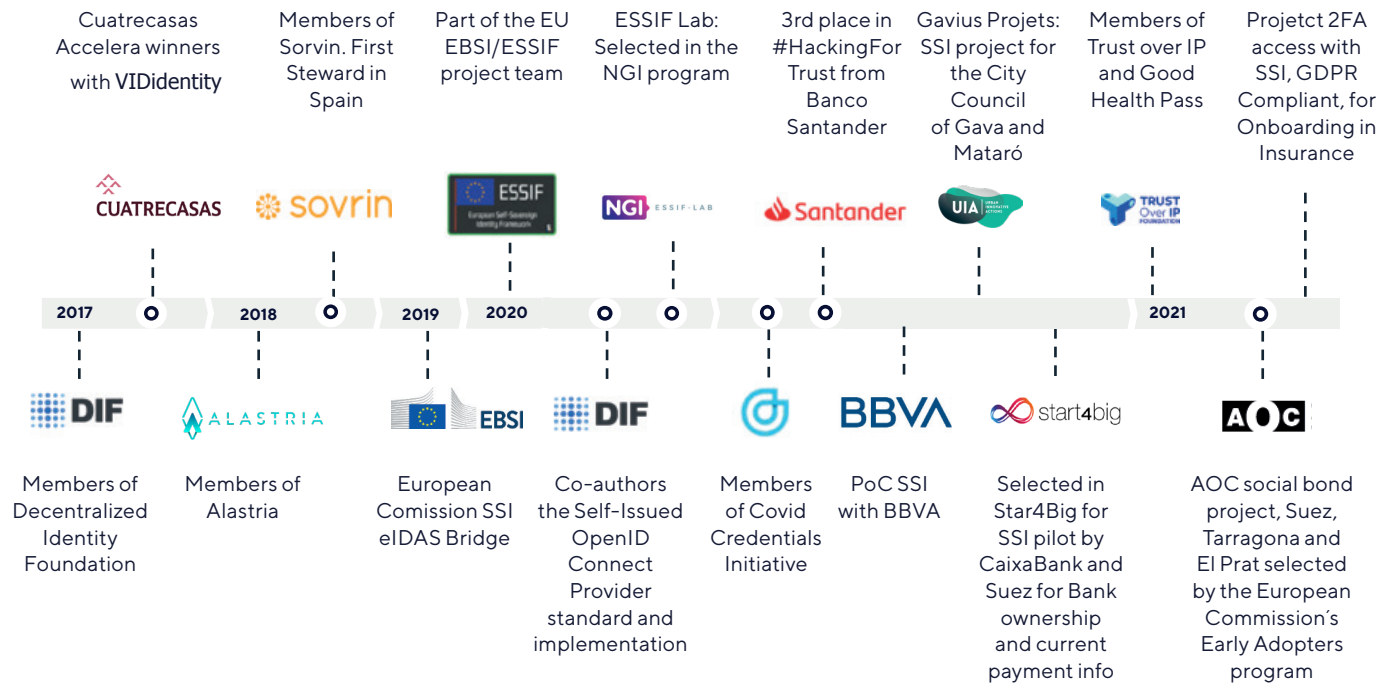
VIDidentity is already at work in several projects and has been awarded with multiple recognitions. We would like to introduce you to some of the more relevant ones.

Milestones:

We received the Horizon 2020 Seal of Excellence by the European Commission, 1st place at 2018 acceleration program of Cuatrecasas (2018 most innovative law firm in Europe by Financial Times) and Telefónica Open Future (world leading telecom company), 1st place at Alastria Open Call (leading Spanish blockchain consortium), winners of Start4big (innovation initiative), selected by Blockers as a top project, selected by the NGI eSSIF Lab Call 2, winners in the hackathon Hacking for Trust organized by Banco Santander.

	Seal of Excellence by the European Commission.		Among 1st European partners of Microsoft SSI unit.
	Winners of Alastria Open Call and of Cuatrecasas and Telefónica Open Future Accelerator program.		eIDAS Bridge & ESSIF Members (European Commission).
	Among the 1sts European partners of Decentralized Identity Foundation (DIF) and the Covid Credentials Initiative (CCI).		Selected project for EU funded ESSIF-LAB and Start4Big.
	1st Spanish partner of Sorving and members of their Stwards Council.		Top 8 out of 170 projects selected by Blockers.
	Members of Alastria Spanish consortium.		Building the Internet of Careers®.

Projects



BBVA

The financial sector is burdened by the requirements of Know Your Customer regulations, which aim to prevent money laundering. These regulations call for different verification measures depending on the identity of the parties involved in a transaction and their perceived risk of criminal activity. As such, Know Your Customer processes are costly and time-consuming. Self-Sovereign Identities can streamline this process by reducing the amount of information required to complete KYC verifications.

This is where Self-Sovereign Identities technology comes in, as Verifiable Credentials can be reused for KYC processes.

BBVA Innovation Lab, formerly BBVA Labs, conducted a proof of concept (POC) on Secured Signatures Infrastructure (SSI) using VIDidentity technology. The POC demonstrates the ability to enroll new users who consume verified credentials, such as a proof of bank account ownership credential.

This highly requested feature for online transactions is not well solved by banks. They often issue an unsigned PDF, that can be tampered with. This is a safety issue that can be easily solved by issuing a Proof of Bank Account Ownership Verifiable Credential.

The demo of the PoC is available [here](https://www.youtube.com/watch?v=zSBPAkklpCA&feature=youtu.be)¹².

¹² <https://www.youtube.com/watch?v=zSBPAkklpCA&feature=youtu.be>

**Start4Big**

Start4big, the first European multi-sector open innovation initiative promoted by Aigües de Barcelona, CaixaBank, Naturgy, SEAT and Telefónica, has selected the winning startups of its second open call of innovation.

During the open call, 6 startups were selected to build Proof of Concepts using blockchain technology in order to find new ways of working for companies and public entities. VIDidentity was selected by two companies: CaixaBank and Suez.

As a part of the Dalion ecosystem (see Ecosystems), CaixaBank is already working in the Self-Sovereign Identity domain, with their own SSI solution built on top of Alastria. CaixaBank selected this solution to create a PoC to test the interoperability between different SSI ecosystems. The PoC will help build a solution of identity for big corporates.

The PoC tested two main use cases. In the first use case, CaixaBank issues a digital credential which proves that a person owns a bank account in CaixaBank. This credential is going to be presented to Suez in order to send charges to this account.

For the second use case, Suez issues a scoring credential about the user's payment habits. The user then can present this credent to the bank to improve their scoring and get access to financial products.

EBSI Early Adopters Program

The European Blockchain Services Infrastructure (EBSI) is a joint initiative from the European Commission and the European Blockchain Partnership (EBP). Since 2018, they have been building the European Blockchain Services Infrastructure (EBSI) to deliver cross-border services for public administrations.

In 2021, Validated ID was selected as part of the EBSI Early Adopters Program. This program is aimed at increasing the adoption of the SSI within the EBSI project. It allows some projects to pilot use cases on top of EBSI infrastructure.

AOC (Open Administration of Catalonia) has participated in the Wave 2 of this Early Adopters program, with the support of Validated ID as an expert in SSI and EBSI. In this POC, users can generate a Verified Credential of their identity from an existing official digital identity (national ID card, qualified certificate, etc.) With this VC, users can authenticate to the data hub of the AOV (MyGov). Once logged in, they can obtain proof of information regarding their identity as a Verified Credential from the municipal census (in the demo, a large family credential). The user can save this credential to their wallet, to later use it in another transaction (for example, to apply a discount as a social voucher in the water bill).

We are proud that VIDidentity is the first solution to become EBSI compliant as part of EBSI's Early Adopters programme.

Other projects:

- Gavius project.
- VIDidentity as a 2FA for Insurance.

Industry Associations and Consortium:

We are working together with other members of the identity industry to ensure new standards. Validated ID is part of national and international consortia, such as Sovrin, Decentralized Identity Foundation, and Alastria, INATBA (International Association for Trusted Blockchain Applications), Velocity Network, TrustOverIp and the GoodHealthPass Initiative.



European Commission: EBSI/ESSIF v1/v2 eIDAS Bridge: linking SSI with eIDAS.



Exchange of credentials Caixa – AGBR Certificate of bank ownership and current payment info with VIDidentity on Alastria.



GAVIUS SSI Project with AOC, Ay. Gaviá, Mataró and BBVA KYC credentials integrated in electronic Headquarters.



AOC Project with Agbar, Aytos. Tarragona and El Prat Optimizing and processing of social vouchers for water companies.

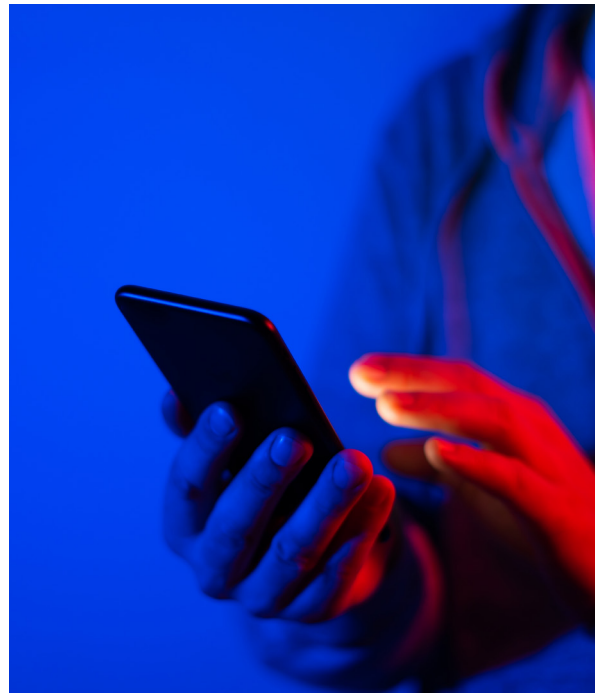


Company overview

Validated ID is Spanish tech start-up founded in 2012 in Barcelona, Spain, providing secure trust services with VIDSigner eSignature and VIDidentity self-sovereign identity.

The company has three main lines of business:

- 1. VIDSigner** is a B2B SaaS (Software as a Service) multichannel eSignature platform covering all use cases, from remote to face to face scenarios, with maximum security, legal compliance, and usability. A unique integration enables the use of any of the following signature methods:
 - Biometric: For face-to-face and Mobility environments
 - Centralized: Sign with your digital certificate stored in the cloud.
 - Remote: For anyone and anywhere.
 - NFC: Qualified signature with electronic ID cards.
 - Stamper: To simplify automated processes.
- 2. VIDidentity** is the new self-sovereign identity solution targeting user digital identity verification in KYC and onboarding procedures in need of better user workflow, security, privacy, compliance (GDPR, PSD2, AML) and lower than current traditional ID solutions.
 - SP4i enables companies to invoice their contractors and European public administrations, inside and outside their country of origin, in compliance with the laws 25/2013 and 9/2017 on the requirements for electronic invoices.
- 3. SP4i** enables companies to invoice their contractors and European public administrations, inside and outside their country of origin, in compliance with the laws 25/2013 and 9/2017 on the requirements for electronic invoices.



Thanks to a top-notch team, state of the art technology and successful market proven service, Validated ID efforts have resulted in +2,500 clients, +200 global partners, +20 million eSignatures performed, constant 3-digit growth and funding by Caixa Capital Risc, Randstad Innovation Fund and Cuatrecasas.

50 +

Full-Time Employees

30 +

Countries Served

2,500 +

Current Customers

200 +

Global Partners

20m +

Signatures Delivered

110% +

Net Revenue Retention

€ 3m

ARR (2021E)

80% +

ARR Growth Rate (2021E)

80% +

Recurring Revenue (2021E)

The **Validated ID team** consists of enthusiasts from the world of identity and eSignatures, with vast professional experience in countless, often complex, identity and signature projects.



Barcelona

C/ Aragó 179, 4º piso
08011 Barcelona
Tel: +34 900 828 948

Madrid

Paseo de las Delicias, 30 planta 7
28045 Madrid
Tel: +34 900 828 948

info@validatedid.com
validatedid.com