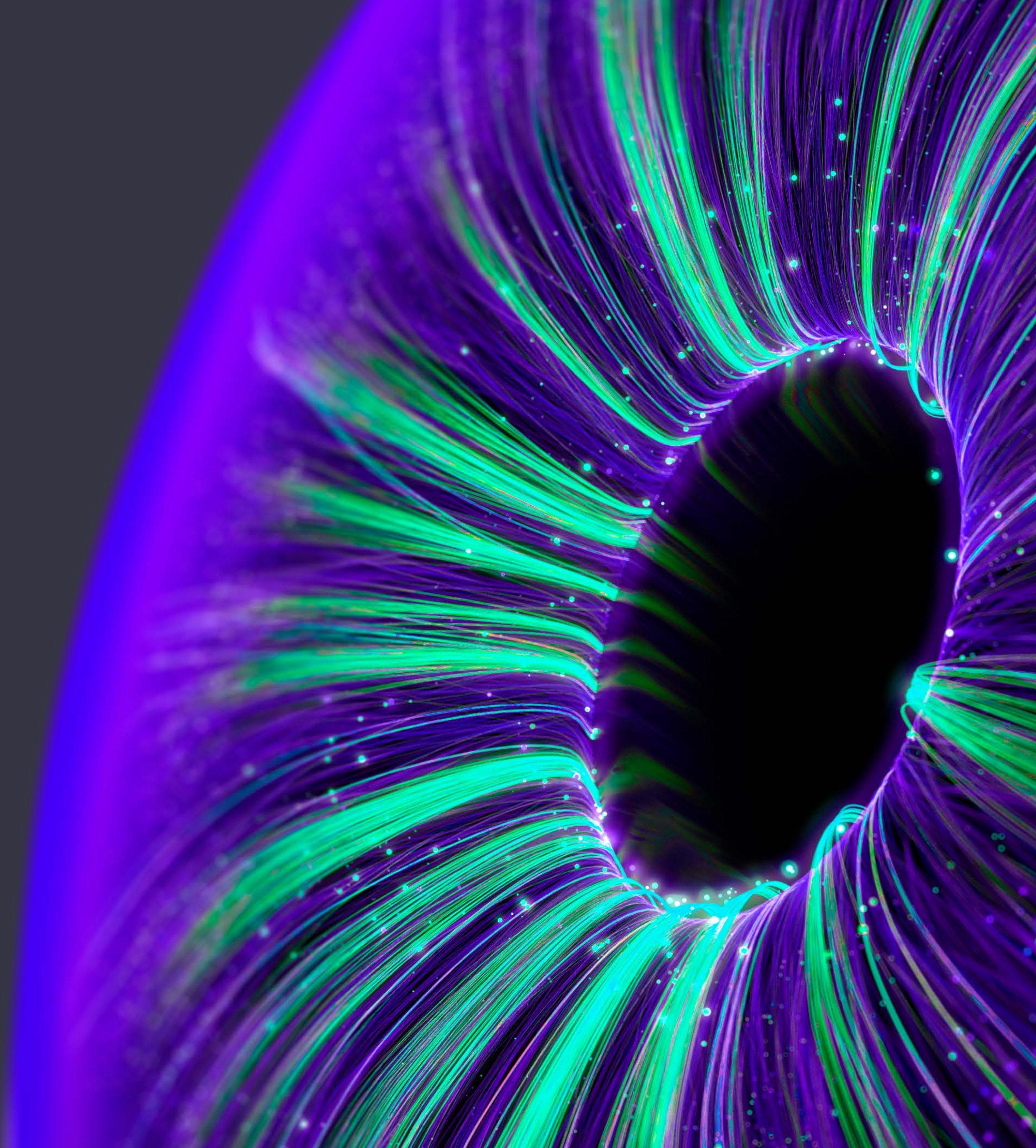
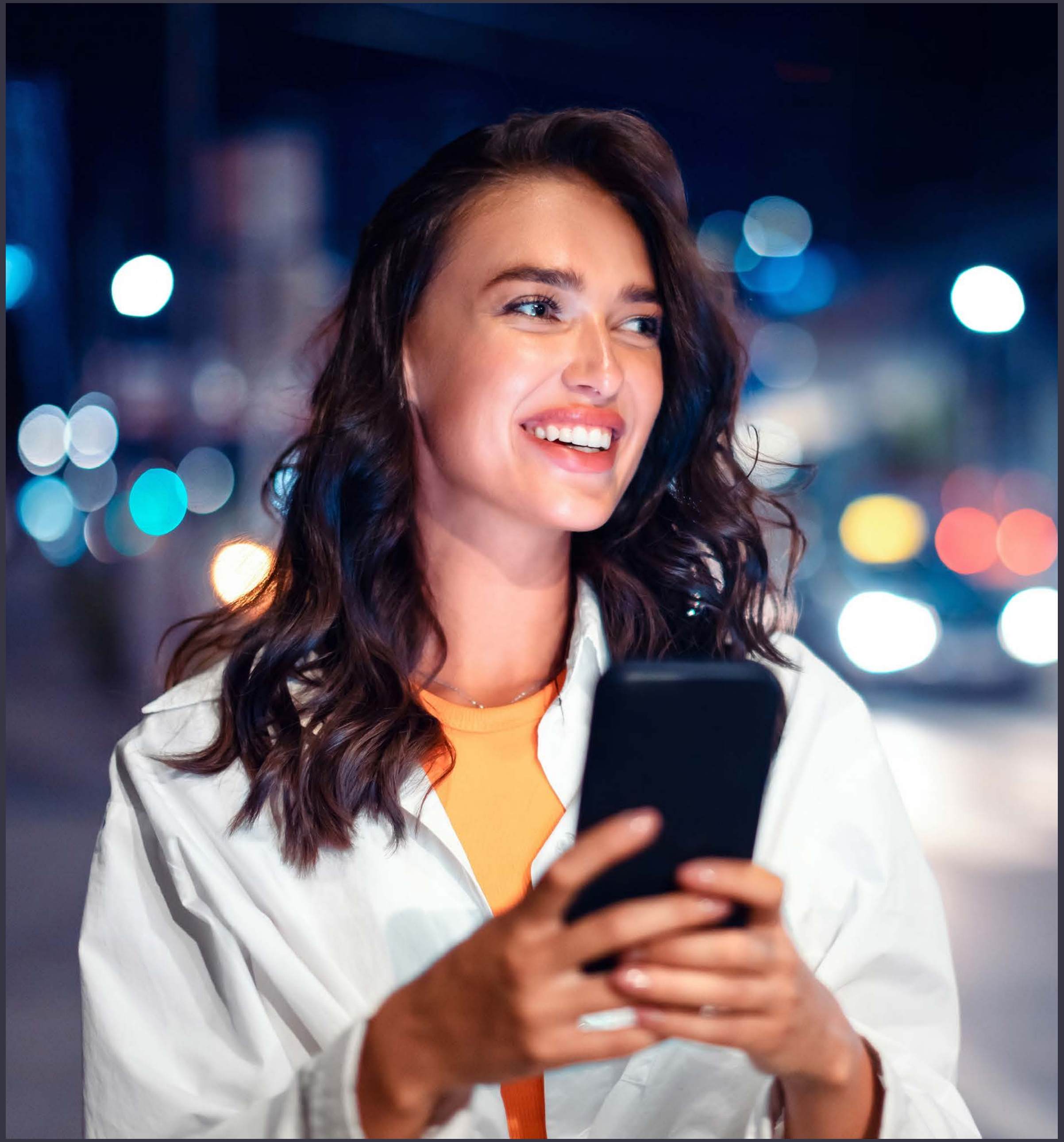
Softtek®

Self-Sovereign Identity: unlocking the future of trust



Index



01

Security and trust: The End of Identity as We Know It

In recent years, online security and privacy have evolved significantly. What was once an environment with little regulation and control over the use of data by companies has now given way to **stricter data security policies and more aware users**, who can now decide how and what information to share.

However, the path towards better privacy has just begun. Companies need clearer guidance to comply with current legislation, and privacy regulations must adapt to the fast pace of the digital industry. **Seizing these opportunities for improvement will be key to gaining customer trust and maintaining a competitive edge.**

In this context, **Self-Sovereign Identity (SSI)** has emerged as a revolutionary model that gives individuals full control over their digital identities. Its approach aims to reduce the risks of data breaches while reinforcing privacy and autonomy. Moreover, it promotes interoperability between platforms, allowing users to securely verify their identity across different contexts without relying on third parties. Therefore, it is a digital identity management model where **individuals and companies have exclusive ownership of their personal credentials.**

From an ethical perspective, the existence of SSI systems is driven **by individuals' right to represent themselves**, whereas traditional identity systems often operate under the obligation for people to be identified, reinforcing a top-down identity management approach.

Indeed, SSI puts the **user in control of their own data**, enabling them to store it on their devices and provide it for verification and transactions without needing to rely on a central data repository. In this sense, self-sovereign identity gives users the ability to **decide what information to share, with whom, in what context, and for how long.**

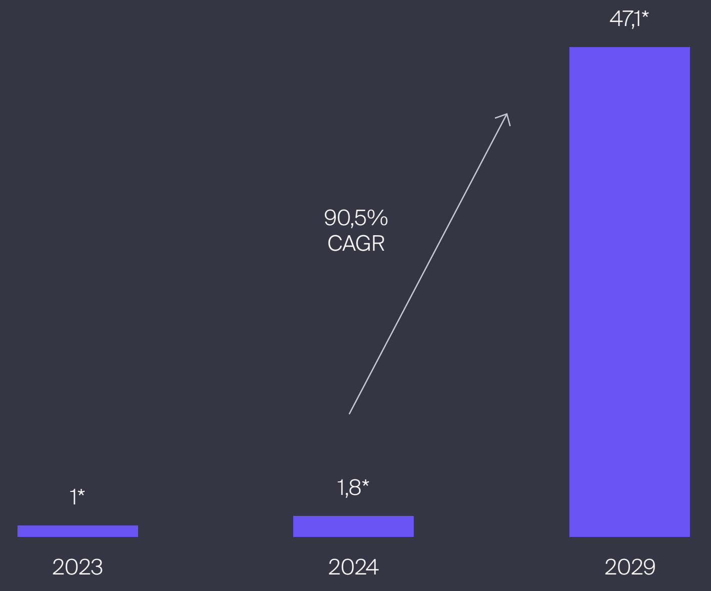
The Global SSI Market

~$1.000M

Global SSI Market Size in 2023

90,5%

CAGR of the Global SSI Market Between 2024 and 2029



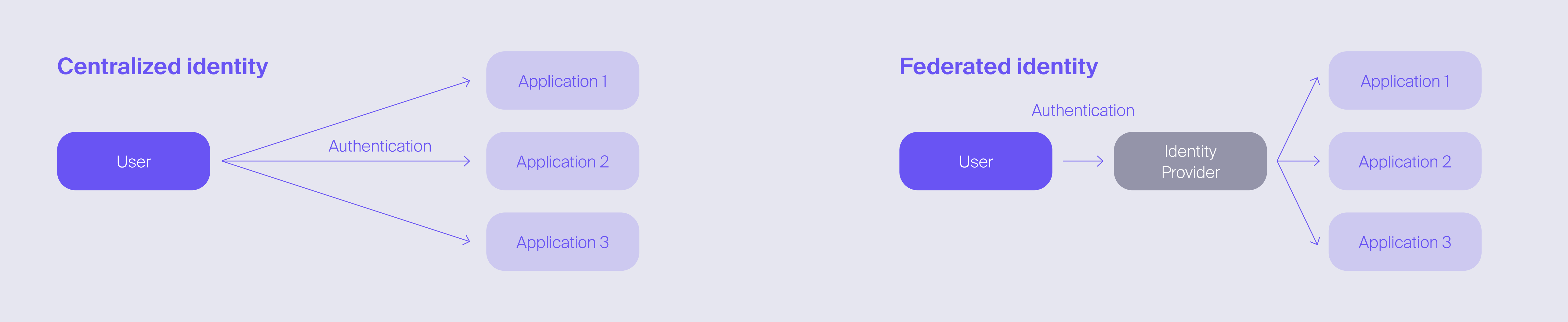
* In billions of US dollars

Traditional Models: Centralized or Federated?

Traditional identity management models, both centralized and federated, have long dominated how users access services and applications. On one hand, in the **centralized model**, personal identity data is stored in databases controlled by different service providers, which increases security and privacy risks. Each service has its own authentication system, forcing users to manage multiple credentials and exposing them to vulnerabilities, such as password theft or information leaks through centralized storage.

On the other hand, **federated identity management** emerged as a solution to simplify the user experience through Single Sign-On (SSO), allowing access to multiple services with a single credential managed by an identity provider, such as Google or Facebook. However, while it improves convenience and offers robust authentication, this model still raises concerns, as it **transfers control of identity to third parties.** This creates privacy risks and data leaks.

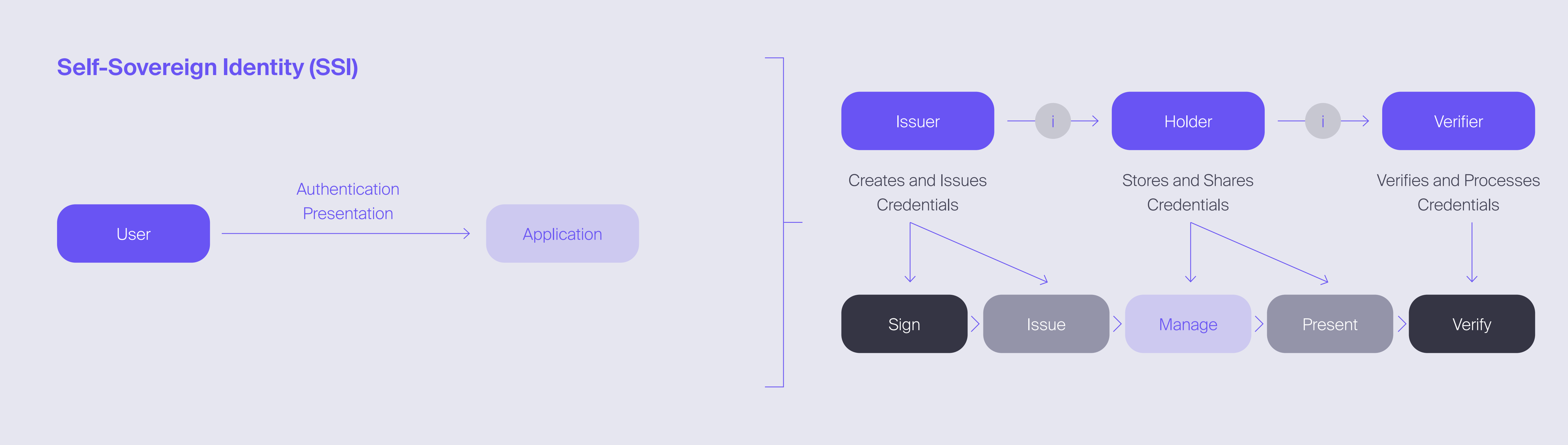
Despite the advantages they offered at the time, both centralized and federated models have shown numerous vulnerabilities. In this context, these methods have fallen behind in comparison **to newer, more secure, interoperable, and user-centric alternatives** that aim to give individuals full control over their digital identity.



Unlike traditional systems where data is stored and managed by third parties, **individuals gain full authority and control over their identity with SSI.** In this sense, self-sovereign identity (SSI) systems are typically decentralized, based on Blockchain technology, thus eliminating any centralized authority.

SSI simplifies the user experience by allowing data sharing in a straightforward way, replacing traditional methods such as forms or uploads with one-click interactions. Thanks to its user-centric architecture, it offers **total control over data storage, access, and portability,** providing independence by not being limited to specific platforms. Additionally, it fosters trustworthy interactions by **enabling data verification to prevent fraud and false identity**. SSI also enhances security by mitigating data leakage risks, eliminating passwords and centralized storage, and ensuring privacy through data minimization techniques, such as selective disclosure.

SSI also represents a step forward for businesses, as **they can offer their stakeholders smoother access to services or products**, leading to higher conversion rates, fewer customer service requests, and overall higher satisfaction. SSI allows organizations to **receive reliable and verified data** from trusted third parties, improving data quality. Furthermore, it helps prevent malicious behaviors such as spam, identity theft, and document forgery. SSI also **strengthens security by eliminating risk factors like passwords and centralized data storage** and ensures compliance with privacy and data protection regulations thanks to its user-centered and consent-based management.


Self-Sovereign Identity (SSI)
User
Authentication
Presentation
Application
Issuer
i
Holder
i
Verifier
Creates and Issues Credentials
Stores and Shares Credentials
Verifies and Processes Credentials
Sign
Issue
Manage
Present
Verify

The Great Challenge: Security, Privacy, and Trust

As of July 2024, the percentage of the global population with access to the internet reached 67.1%, and 63.7% had social media profiles. This increase in people's exposure to online spaces parallels a rise in their risk. In fact, nearly 7 out of 10 adults (68%) **worldwide felt more vulnerable to identity theft in 2022 compared to previous years.** Furthermore, **57% of internet users** globally considered it **impossible to protect their privacy online as of January 2023.**

In this regard, **30.7% of global internet users reported concerns about the misuse of their personal data** in the first quarter of 2024. As of January 2023, 83% stated that they would like to do more to protect their privacy, and 70% had taken at least one measure to address this insecurity.

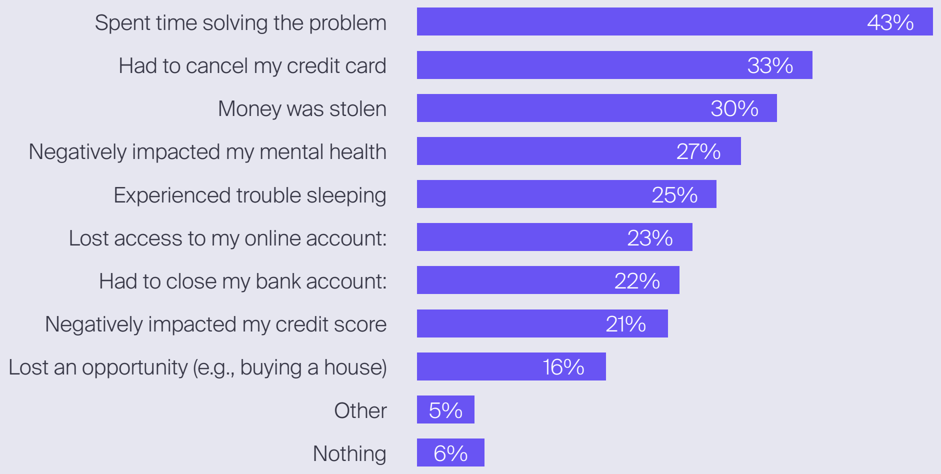
63%

Internet users were willing to accept risks to their online privacy for the sake of convenience, as of January 2023.

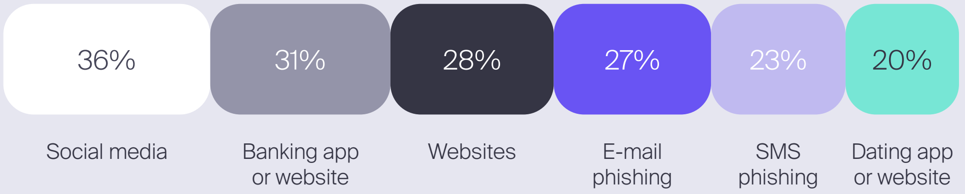
3.500M

Hours spent by cybercrime victims in 2022 resolving issues related to the crimes.

94% of users who experienced online identity theft in 2022 suffered one or more of the following impacts



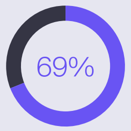
Most cybercrimes originated on apps or websites



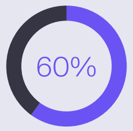
Despite the lack of awareness, internet users are increasingly taking measures to protect their online identity

While there is still widespread **lack of knowledge about online data privacy**, citizens are gradually becoming more aware of the need to educate themselves on this issue to ensure control and resilience over their personal information. In this regard, in response to the rise in cybercrimes and data breaches, internet users are implementing measures to protect their identity. In 2023, 36% of users employed parental controls, 20% had enabled multi-factor authentication, 28% had changed the default privacy settings on their devices, and as many as **27% had already used an identity theft protection service.**

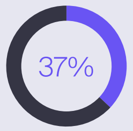
Most adults lack knowledge about online identity theft and do not have the tools to deal with potential theft



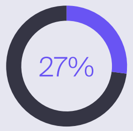
Internet users do not know how to check if their identity has been stolen.



Internet users would not know what to do if their identity were stolen.

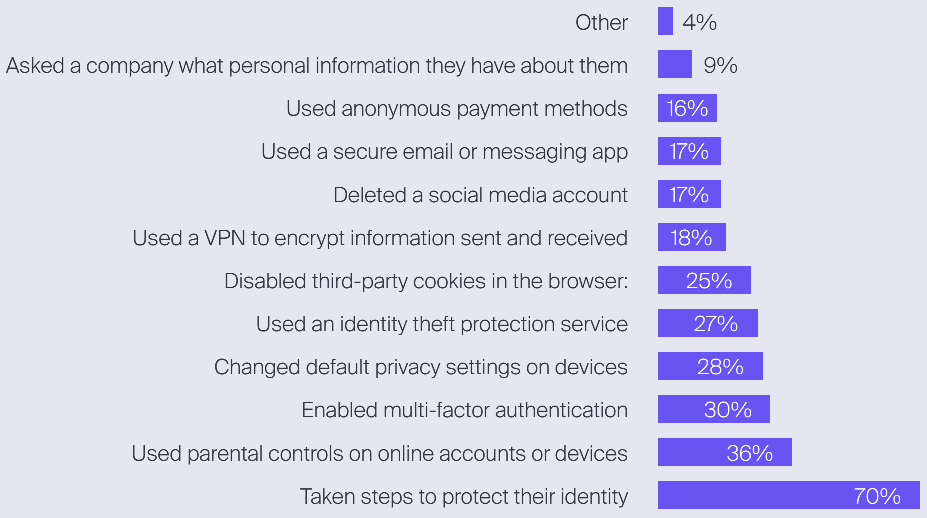


Internet users have not considered that they might have been victims of identity theft.



Internet users do not know what online identity theft is.

Seven out of ten internet users have taken some measure to protect their online identity



02

The User in Control: Self-Sovereign Identity (SSI) Redefines the Rules

SSI has the potential to reshape digital identity and place the user at the center of the system. With that focus, there are several factors driving its development and adoption:

Privacy and Data Protection

Citizens are increasingly concerned about the privacy and security of their personal data. SSI offers a way to maintain control over one's identity information, reducing the risk of data breaches and unauthorized access by minimizing dependence on centralized databases. In this regard, the right to privacy for individuals must be protected.

Security and Trust

Centralized identity systems are vulnerable to cybercrimes and identity theft. SSI uses cryptographic techniques and decentralized networks, such as Blockchain, to enhance security and build trust by ensuring that identity data is tamper-proof and verifiable.

User-Centered Approach

SSI places the individual at the center of the identity management process, allowing them to decide what aspects of their identity to share and with whom. It enables individuals to create portable identities that can be used across various contexts and platforms, fostering user convenience and autonomy.

Regulatory Compliance

Various regulations, such as the General Data Protection Regulation (GDPR) of the EU, emphasize individual data rights and consent. SSI aligns with these regulations by providing individuals with greater control over their personal data, facilitating compliance with privacy and consent requirements.

Business and Economic Benefits

SSI can provide cost savings for organizations by reducing the need for identity verification processes, data storage, and compliance with complex identity regulations. It can also enable new business models, such as identity-based services and decentralized applications.

Autonomy, Control, and Portability

Data privacy and security are at the core of self-sovereign identity, while also revolving around other principles such as transparency, consent, persistence, and minimization. Particularly prominent are the concepts of autonomy, control, and portability, based on empowering individuals to manage their own identity without relying on centralized intermediaries.

Firstly, **autonomy refers to the fact that individuals, as owners of their data, have the freedom to choose what information they share**. This principle allows users to have complete ownership of their digital credentials, securely storing them on their personal devices. This decentralized approach eliminates the need for third parties to control or store users' personal information, minimizing the risks of leaks, data breaches, and cyberattacks.

Secondly, **control refers to the individual's ability to decide which data to share, with whom, and in what context.** This principle is closely linked to another, access, as individuals must be able to access all their own data. Thanks to the SSI architecture, users can granularly select what information to disclose in each interaction, avoiding excessive data sharing. Furthermore, this control extends to the ability to revoke access to third parties at any time, enhancing the security and privacy of digital identity.

Finally, **portability is another key aspect**, as individuals must be able to transport their information and credentials in their digital wallet, without being restricted to specific platforms and **without the need to duplicate data or create new accounts** for each service. Alongside portability arises interoperability, as SSI promotes open standards and protocols, reducing redundancy and simplifying identity verification processes. Ultimately, credentials should be usable as broadly as possible by various stakeholders. Organizations, databases, and registries should be able to communicate quickly and efficiently on a global scale through a digital identity system.

There are other principles that inform SSI and ensure that the user has control over their data.

- **Transparency**
  The way identity systems are managed and updated should be publicly available and reasonably understandable.

- **Consent**
  In an interactive and informed process, the user gives explicit consent for the use of their data in each case.

- **Minimization**
  Individuals should be able to share the minimum amount of data necessary, avoiding the exchange of excessive information.

- **Persistence**
  Identity data should be durable, rooted in resilient infrastructures and sustainable models.

Regulation, a Key Driver: eSSIF, eIDAS 2, and GDPR

Europe is one of the most advanced regions in regulating issues related to digital identity and privacy, and several specific regulations impact the development of SSI: **the GDPR regulation, the eIDAS regulation, and the ESSIF initiative**, backed by the European Blockchain Service Infrastructure (EBSI).

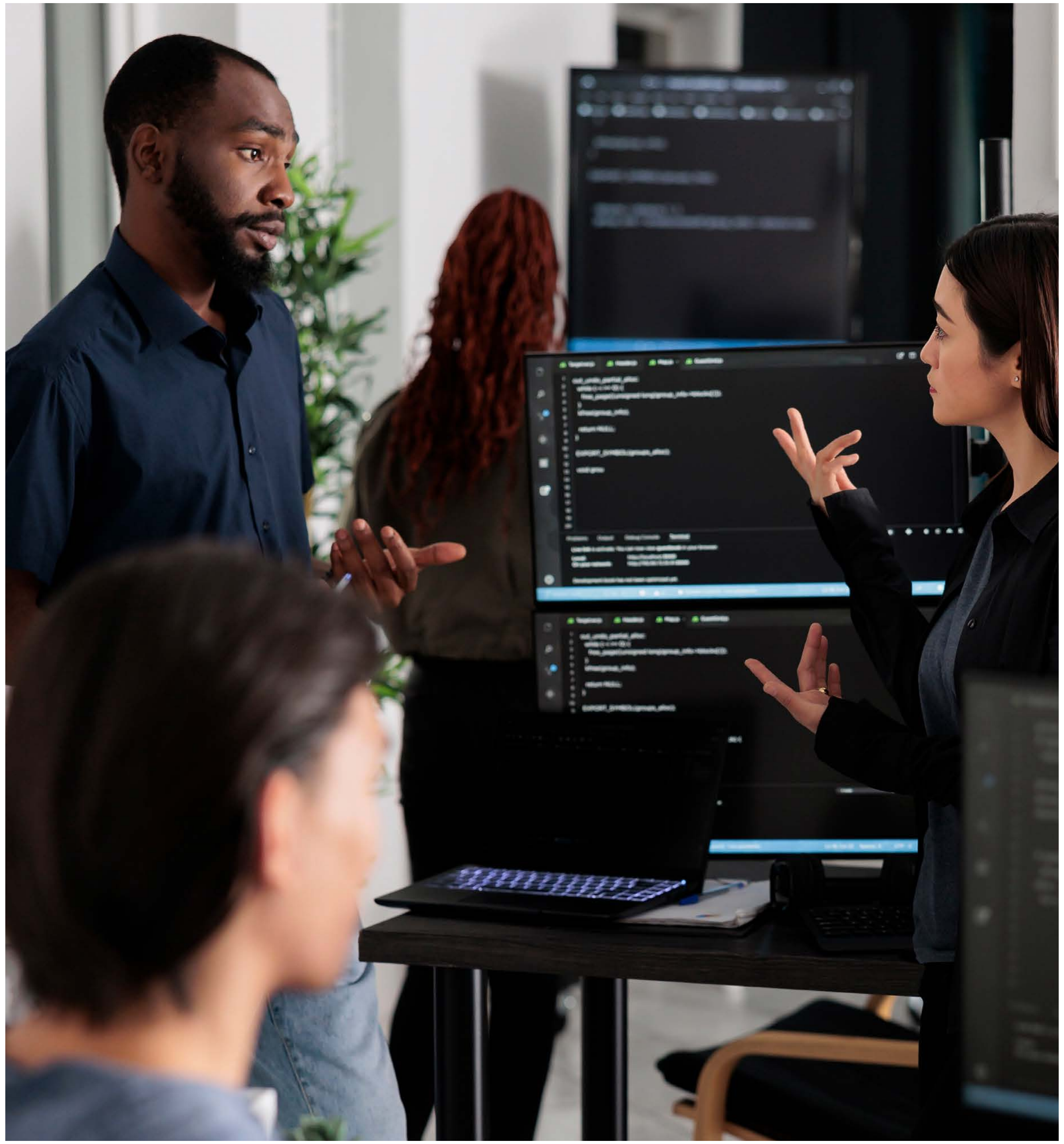
General Data Protection Regulation (GDPR)

It establishes that **control over personal data lies with the individual**, reinforcing the idea that each person should have the power to manage, control, and decide who can access their information.

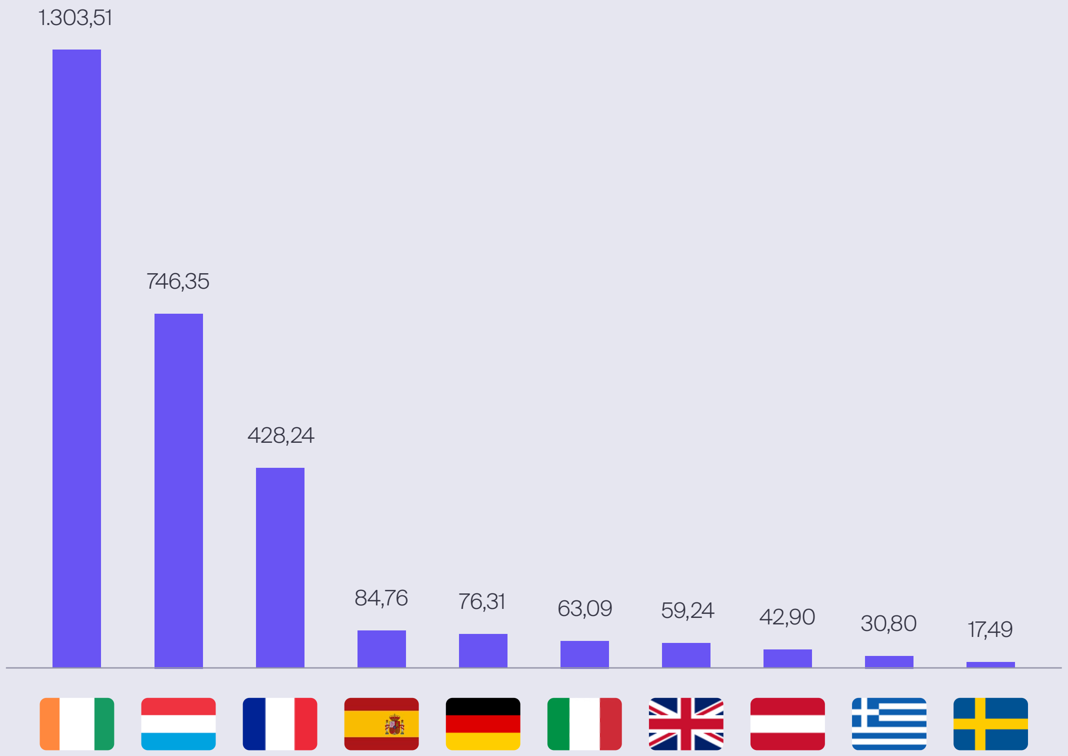
It establishes **privacy principles**, such as the right to be forgotten and data portability, which are key to the development of SSI.

It requires **clear and explicit consent** for data processing, aligning with the SSI principle that individuals must give their consent before sharing their data.

The **data minimization principle** ensures that only the necessary data is collected, an idea that SSI supports, as it allows users to share only the strictly necessary information.



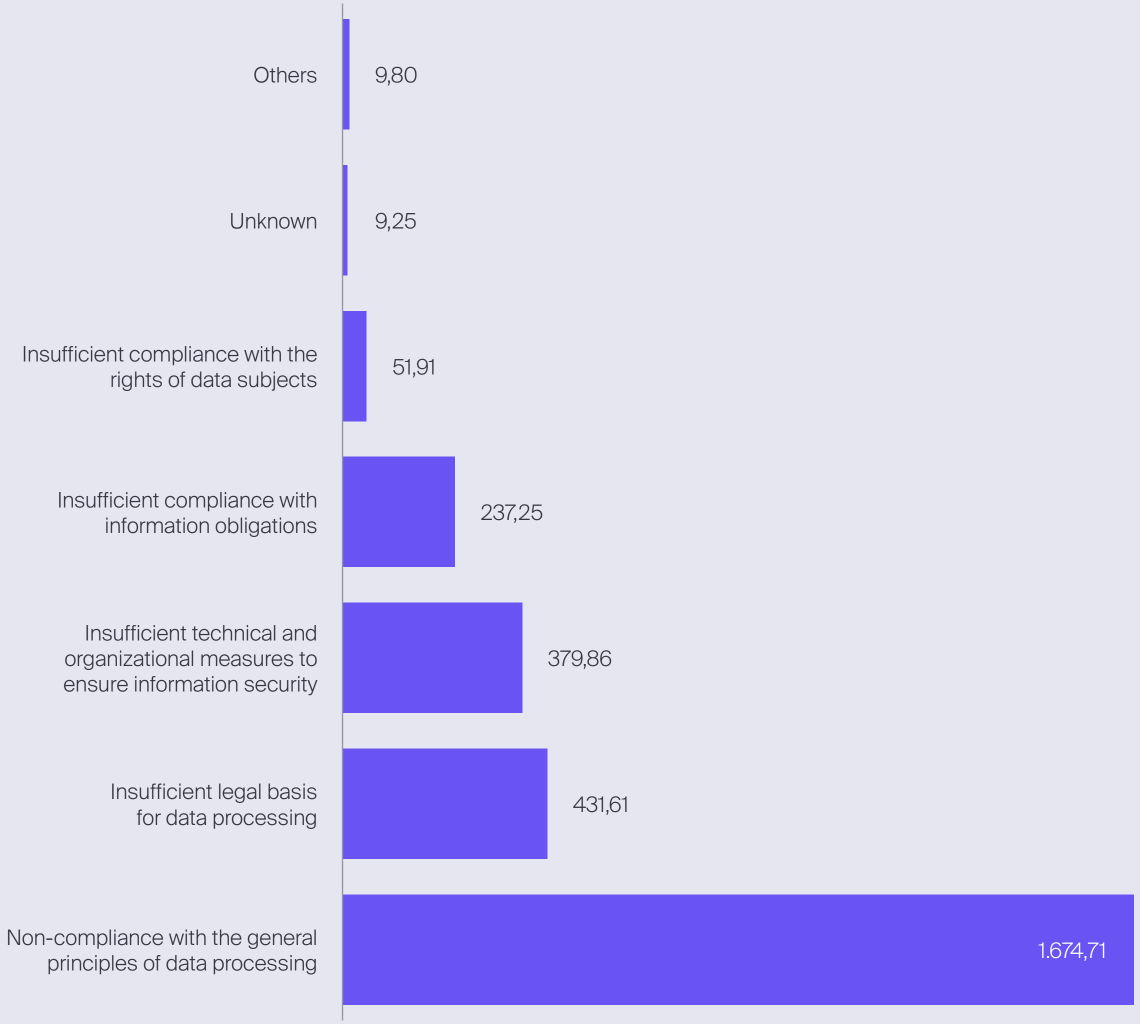
Added value of GDPR fines imposed in Europe between May 2018 and January 2023 (expressed in millions of euros)



€4.884M

Total volume of GDPR fines across the EU in September 2024.

Fines imposed for GDPR violations between May 2018 and May 2023 (expressed in millions of euros)



eIDAS 2, an update to eIDAS, establishes a legal framework for identification, authentication, and electronic signatures. The regulation is intended to **improve the security of digital transactions and identification services across all EU member states.** It introduces a European digital identity wallet that allows citizens to control their identity data and use it for both public and private services. Unlike eIDAS, which primarily covered electronic signatures and trust services, eIDAS 2 focuses on **broader applications**, such as cross-border recognition of digital credentials and stronger security features, aiming to achieve greater adoption throughout the EU.

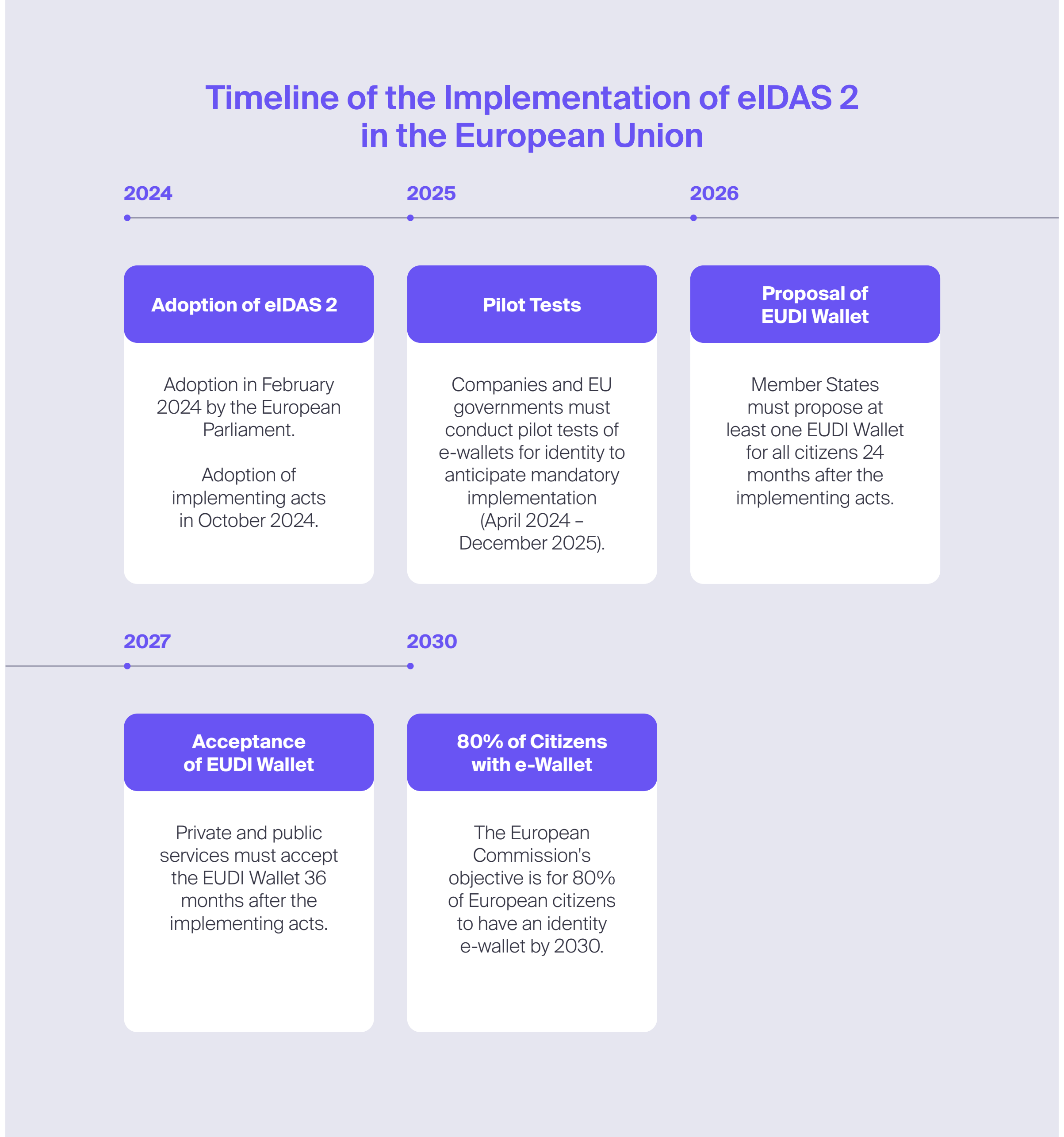
Electronic Identification and Trust Services (eIDAS)

Regulation established for the **creation of a legally recognized digital identity** across all EU member states, reinforcing interoperability.

It promotes the development of a **technologically neutral framework** that does not favor any specific technical solution for the implementation of electronic identification.

It establishes a clear legal framework for **individuals, businesses, and public administrations** to access services and conduct online transactions securely.

eIDAS r**egulates trust services** (Electronic Registered Delivery Services, ERDS), such as digital signatures and electronic seals, ensuring that verified data and identities under an SSI system meet legal and security requirements.



Timeline of the Implementation of eIDAS 2 in the European Union

2024

Adoption of eIDAS 2

Adoption in February 2024 by the European Parliament.

Adoption of implementing acts in October 2024.

2025

Pilot Tests

Companies and EU governments must conduct pilot tests of e-wallets for identity to anticipate mandatory implementation (April 2024 – December 2025).

2026

Proposal of EUDI Wallet

Member States must propose at least one EUDI Wallet for all citizens 24 months after the implementing acts.

2027

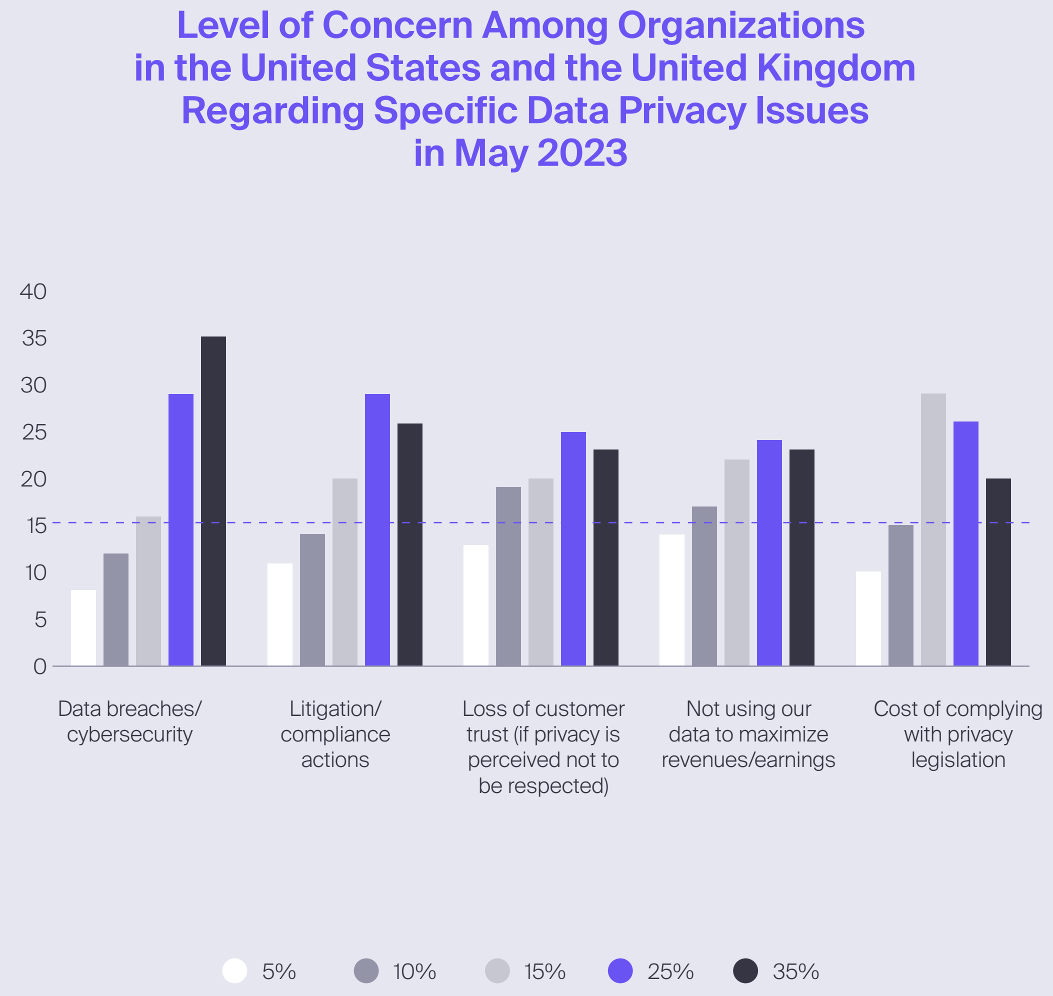
Acceptance of EUDI Wallet

Private and public services must accept the EUDI Wallet 36 months after the implementing acts.

2030

80% of Citizens with e-Wallet

The European Commission's objective is for 80% of European citizens to have an identity e-wallet by 2030.



The lack of non-EU regulation could hinder the advancement of SSI

Beyond the **European Union**, comprehensive regulatory frameworks that facilitate the development of SSI systems are scarce. In the **UK**, the inherited UK GDPR regulates data privacy, but there is no specific framework for SSI, aside from trust frameworks like the UK Digital Identity and Attributes Trust Framework.

In the **United States**, for example, there is also no specific federal regulation, aside from the proposed Digital Identity Act. Some state initiatives exist, such as in Wyoming, where laws recognizing digital identity and smart contracts have been enacted; in Illinois, where a pilot program has been launched to explore the use of Blockchain technology in identity management; and in California, with the California Consumer Privacy Act (CCPA), which grants consumers rights regarding access to and control over their personal data, similar to the GDPR in Europe.

In **Canada**, where there is also no specific regulation, the Pan-Canadian Trust Framework, led by the Digital ID and Authentication Council of Canada (DIACC), serves as a guide for the adoption of digital identity technologies, including SSI-based solutions. Additionally, Canada has data protection laws such as the Personal Information Protection and Electronic Documents Act (PIPEDA), which establishes principles for the collection and use of personal information by private organizations.

Meanwhile, the **Australian** Parliament adopted the Digital ID Bill in May 2024, scheduled to be implemented in November. The law introduces a national Digital Identity system with strict privacy and security measures, voluntary participation, and local data storage to streamline online transactions and ensure the protection of personal information.

Outside the EU, there is regulatory scarcity. In the U.S. and the UK, major companies are particularly concerned about potential data breaches and privacy litigation.

Key Actors: Issuers, Verifiers, and Holders

In the context of self-sovereign identity, there are three key actors that interact within the system:

1. Holders

Individuals or organizations that own and control their own digital identity. These holders have the ability to **store and manage their credentials** on secure devices and decide when and with whom to share their information. They are the owners of their data and can provide proof of their identity in a decentralized manner, without relying on intermediaries.

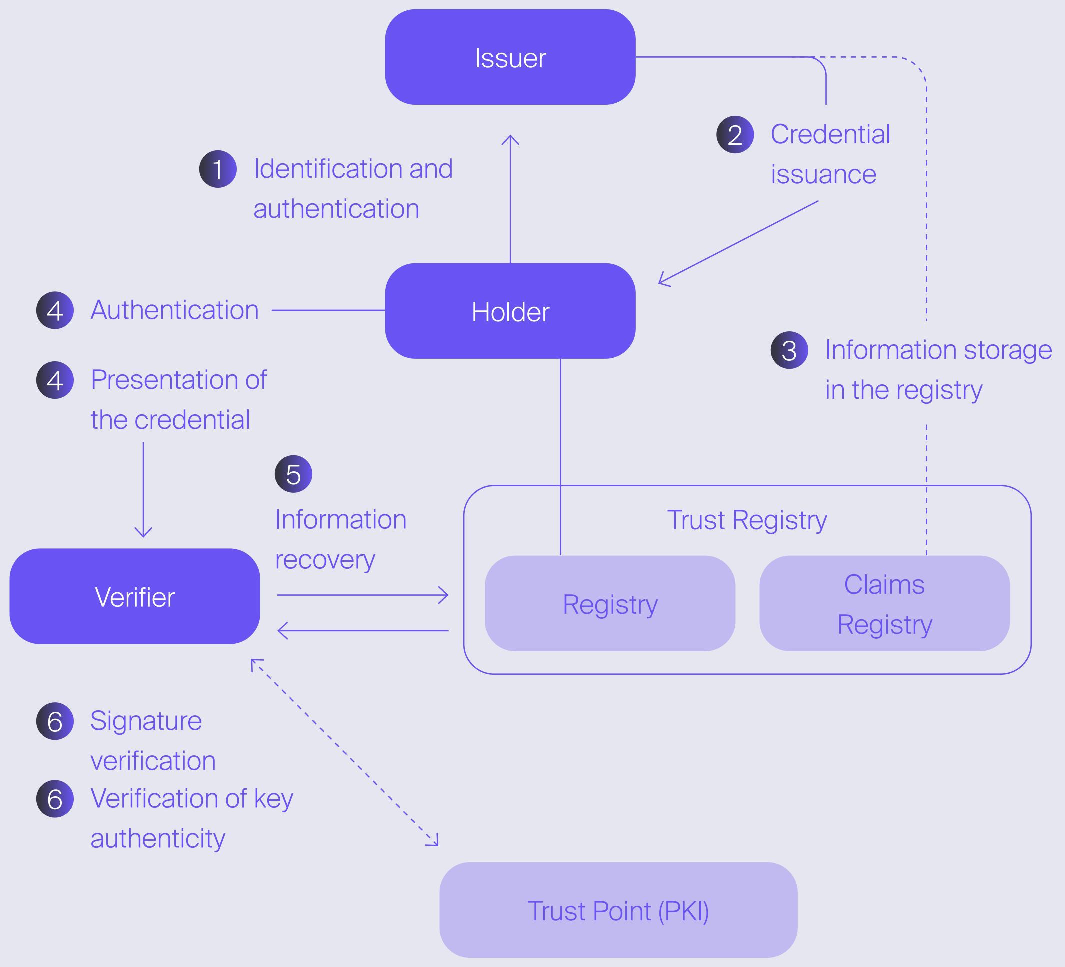
2. Issuers

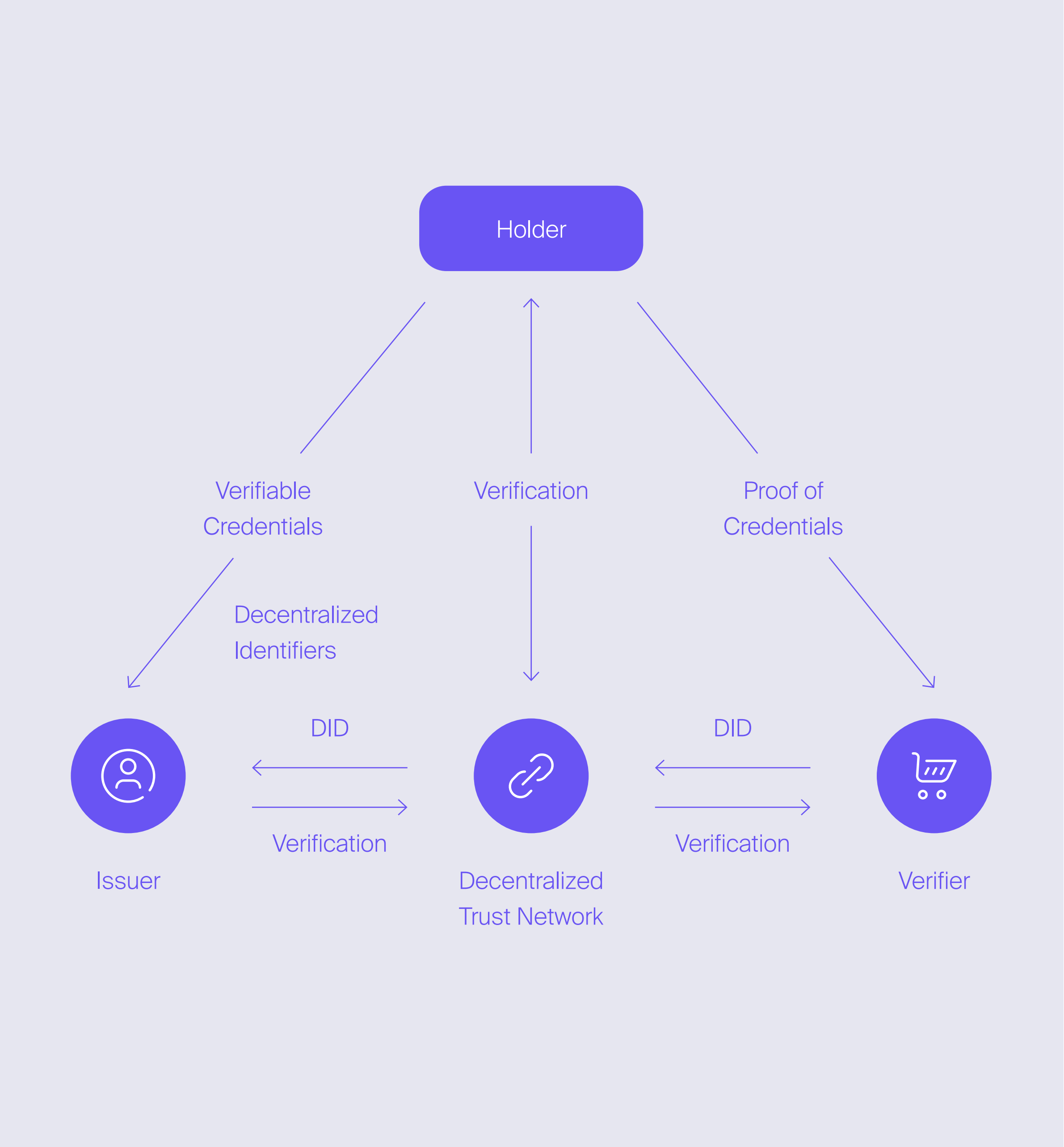
Entities that create and issue verifiable credentials to holders. These credentials can be any type of document or digital certification. Issuers are **responsible for ensuring the authenticity and accuracy** of the credentials they issue.

3. Verifiers

Entities that receive, review, and validate the credentials shared by holders. They use cryptographic mechanisms to verify the **authenticity of the credentials** without needing to communicate directly with the issuer, while maintaining the holder's privacy.

SSI Infrastructure





Blockchain, DIDs, VCs, and Cryptography

The technology behind SSI is based on **blockchain** technology **and distributed ledgers (DLT)**, which allows users to create secure and verifiable digital identities that are cryptographically protected. By using pairs of public and private keys, data can be signed and encrypted, enabling selective and secure information sharing.

In summary, several essential technological concepts interact in SSI to ensure the security, control, and privacy of digital identity:

- **Trust Registries**
  They act as a shared "trust layer," where reliable information, such as references to credentials or authorized issuers, is recorded. Although they do not store personal data, these registries ensure that interactions and verifications occur with trusted entities, without relying on a centralized third party.

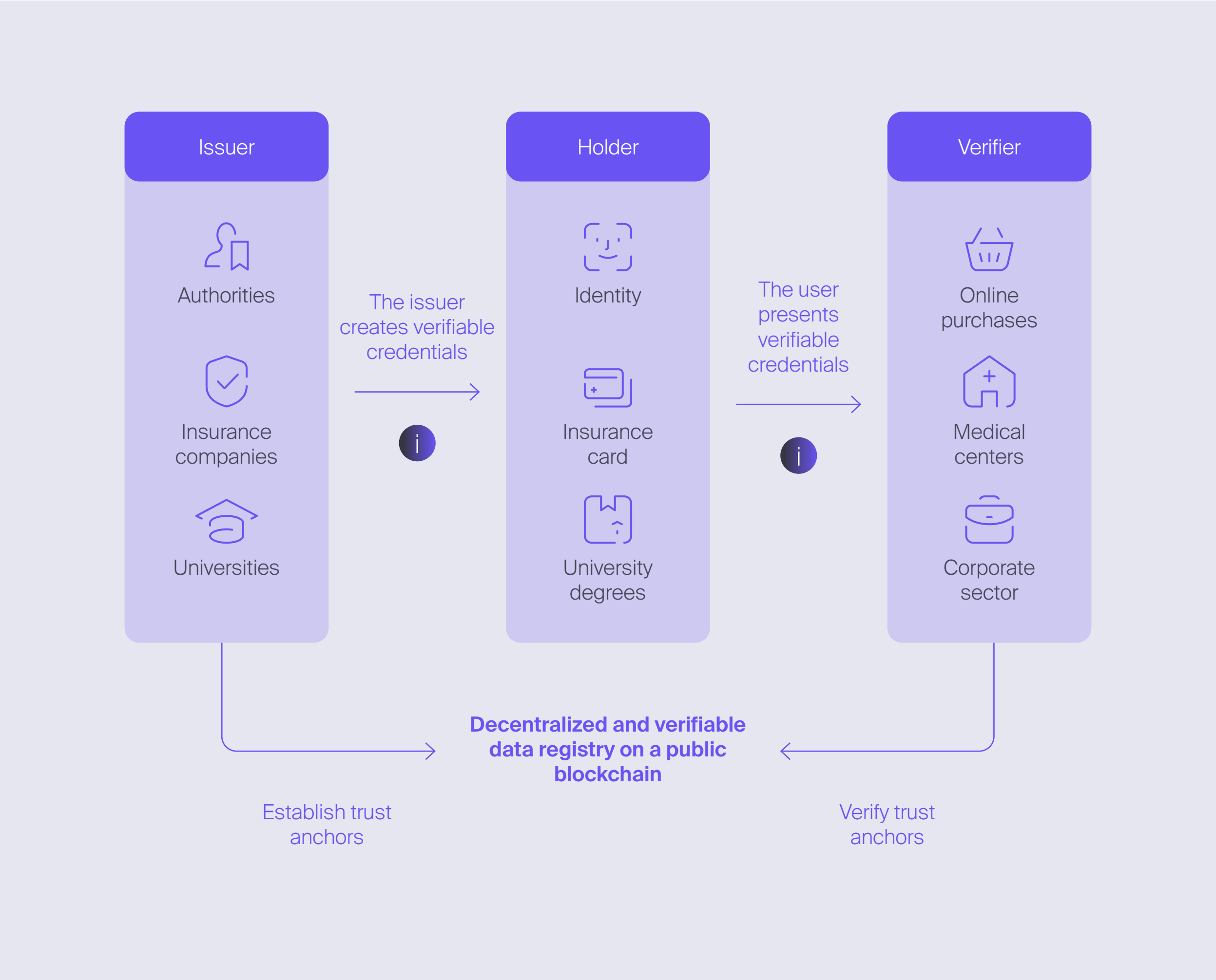
- **Cryptographic Keys**
  Cryptographic keys, both public and private, are fundamental for identity control in SSI. They allow the user to authenticate and encrypt the information being shared. The private key, held by the user, ensures that only they have control over their identity, while the public key enables third parties to verify its authenticity.

- **Decentralized Identifiers (DIDs)**
  DIDs are unique and decentralized identifiers that do not rely on any central authority. They are linked to cryptographic keys and allow different parties to interact with each other securely. These identifiers are the foundation of the public key infrastructure in SSI, as they connect digital identities with cryptographic keys in a decentralized manner.

Blockchain, DIDs, VCs, and Cryptography

- **Verifiable Credentials (VCs)**
  Verifiable credentials are digital documents that can be easily shared and verified by any entity. They allow for the verification of their validity, integrity, and authenticity without compromising the user's privacy. It is important to note that these credentials are not stored on a blockchain, which protects privacy and ensures regulatory compliance.

- **Wallets or Digital Wallets**
  Digital wallets or wallets are applications that store cryptographic keys and verifiable credentials. These wallets allow the user to manage their digital identity and share credentials securely and in a controlled manner, always maintaining control over what data to share and with whom.



In summary, these technological elements work together to provide a **secure, decentralized, and user-centered digital identity system.** The use of trust registries, cryptographic keys, DIDs, verifiable credentials, and wallets ensures the user's privacy and autonomy in every interaction.

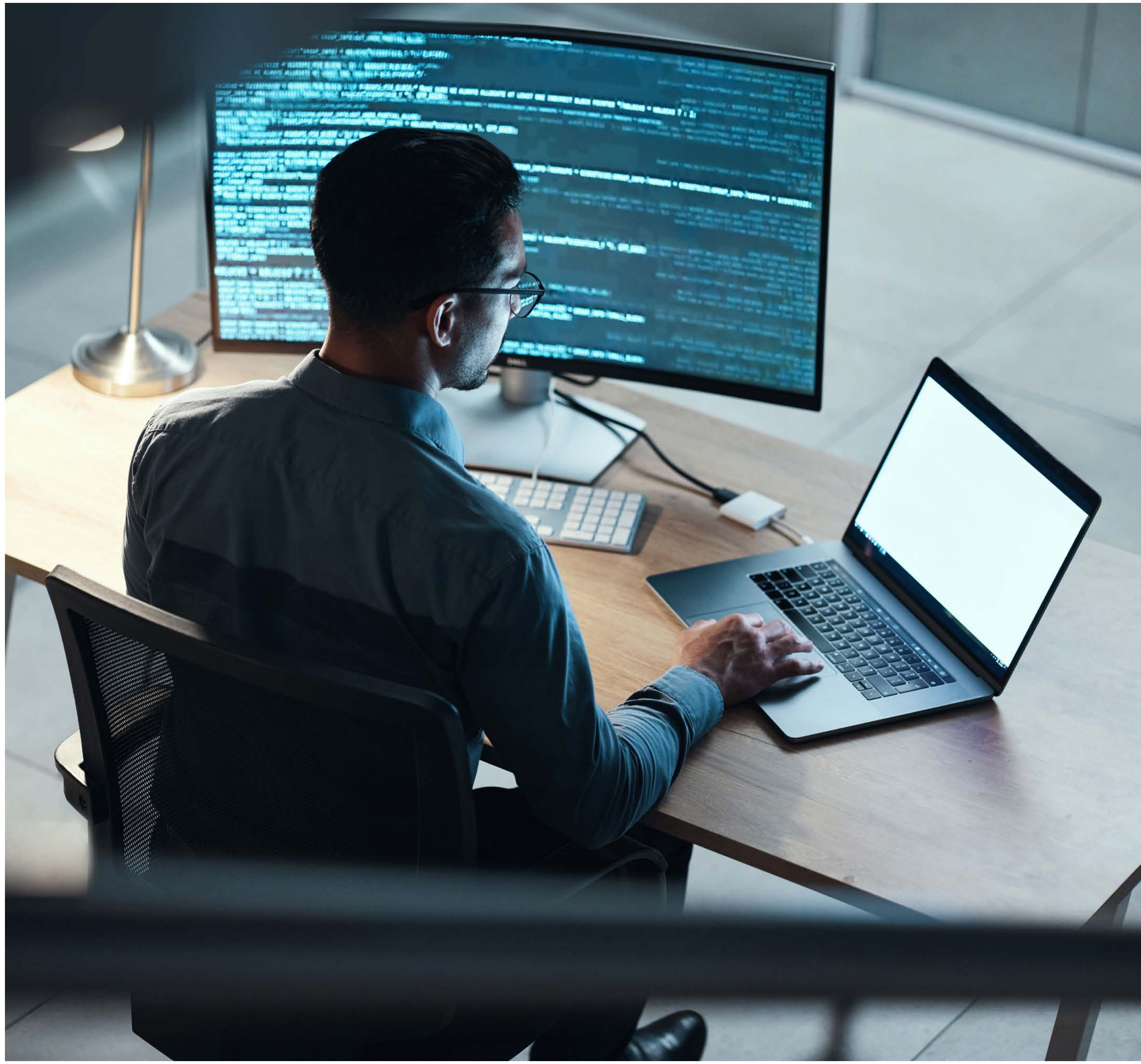
By 2025, it is estimated that **20% of total digital identification** will be conducted using **DLT/ Blockchain** technology, compared to 5% in 2020.

Operational Efficiency
vs. Scalability

Advantages of SSI

SSI systems offer significant **benefits, positively impacting operational efficiency, customer trust, and regulatory compliance.** By eliminating passwords and forms, **SSI simplifies authentication**, which reduces the burden on customer service and improves conversion rates by removing friction from the user experience. Additionally, the data shared through SSI is verified by trusted entities, such as governments, significantly reducing the risk of fraud and identity theft.

Regarding regulatory compliance, **SSI facilitates adherence to data protection regulations** by providing user privacy-centric identity management. This reinforces trust between businesses and users by ensuring that only necessary data is shared. Another key benefit is the **reduction in the risk of security breaches and data leaks**, as decentralizing data management decreases organizations' exposure to cyberattacks and reduces the costs associated with information protection, making SSI an attractive and secure solution for both businesses and users.



Challenges of SSI

Despite the numerous benefits of SSI systems, they present significant challenges, primarily related to **interoperability and security.** The lack of interoperability among different SSI platforms and applications can fragment the ecosystem, forcing users and businesses to manage their digital identities across multiple systems. This complicates the mass adoption of SSI, as it **requires the establishment of shared standards and mutual trust across various jurisdictions and platforms.** Furthermore, users bear greater responsibility for the security of their credentials, which can pose **risks in situations of loss or failures in devices** such as mobile phones, which are essential for verifying their identities. Losing access, whether due to a damaged or lost device, can compromise the user's ability to interact with services.

The scalability challenge goes beyond interoperability, also involving the **technical capacity to support an increasing number of users and large-scale transactions.** Organizations implementing SSI will need robust and flexible infrastructures that can efficiently manage this identity model without compromising speed or security. For SSI to be a viable long-term solution, it must **adapt to multiple sectors, from healthcare to finance.** This challenge demands close collaboration among developers, regulators, and businesses to create a common framework that addresses technical issues and ensures the system can scale effectively, fulfilling the promise of providing a truly global and self-sovereign digital identity.

A Future That Is Already Here: The Cases of Singapore and Estonia

This theoretical framework on SSI systems has already been extensively tested by governments around the world. In fact, this disruptive model has been successfully implemented in countries like **Singapore and Estonia**, where the adoption rates of the Singpass and e-Residency systems, respectively, are very promising. Following these success stories, numerous organizations are launching products and services based on self-sovereign identity.

National Digital Identity (NDI) in Singapore

Government initiative that provides citizens and residents with a secure means of authentication in public and private digital services.

- Electronic signature of public and private documents with biometrics.
- Online identity verification to reduce fraud and identity theft.
- Secure digital access to government, banking, healthcare, and educational services.

4,2M
Users of the Singpass app

41M
Transactions per month

+2,7K
Services it provides access to

e-Residency in Estonia

Digital identity program of the Estonian government launched in 2014, legally binding for citizens and residents. It includes a physical card for storing cryptographic keys.

- Signing documents and filing electronic taxes.
- Company registration, business management, and access to global banking services.
- Authentication and protection of identity and personal data in online services.

96%
of the population has a valid identity card

+339M
Digital signatures completed

03

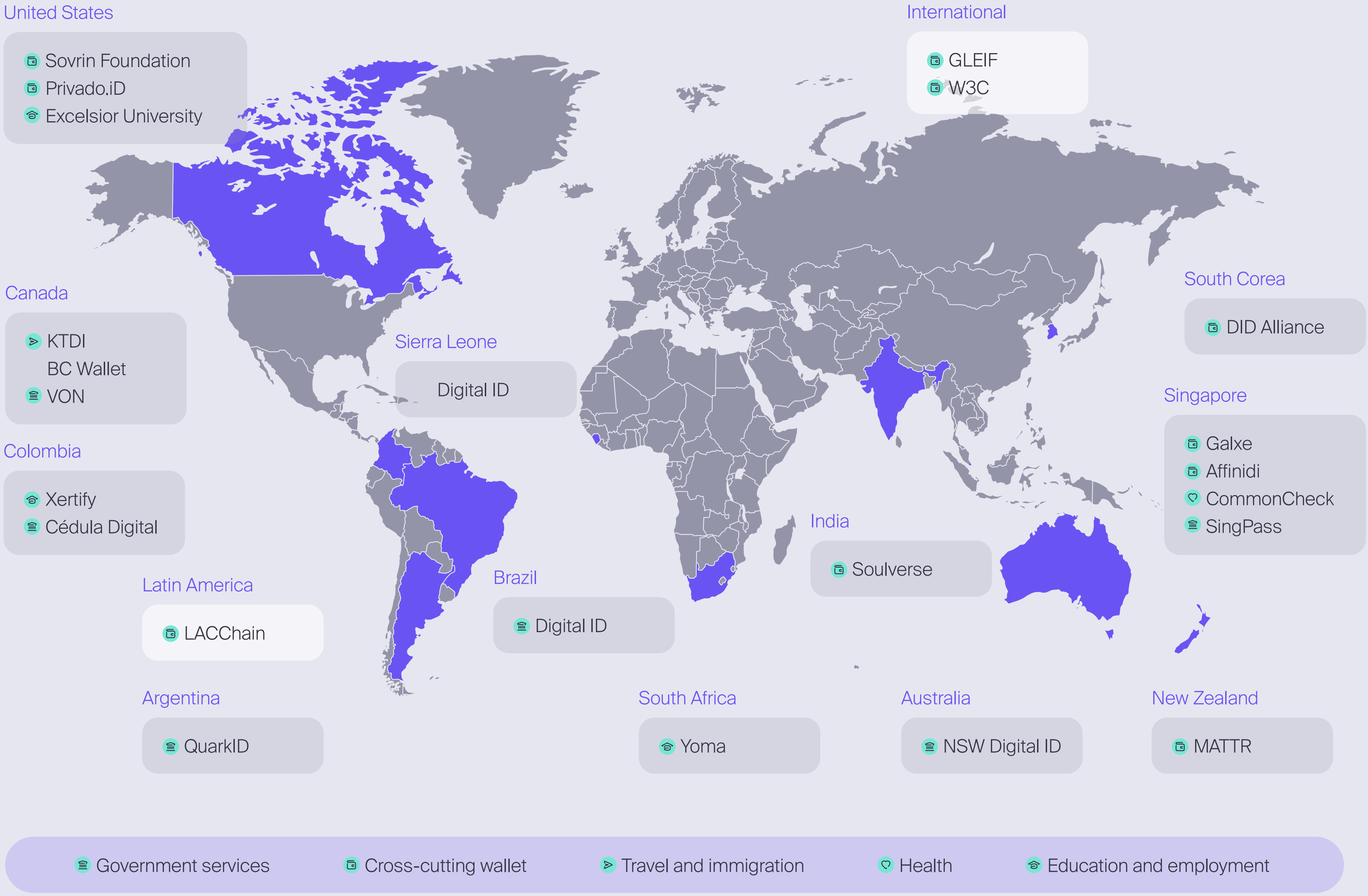
Beyond Borders: SSI Conquers All Continents

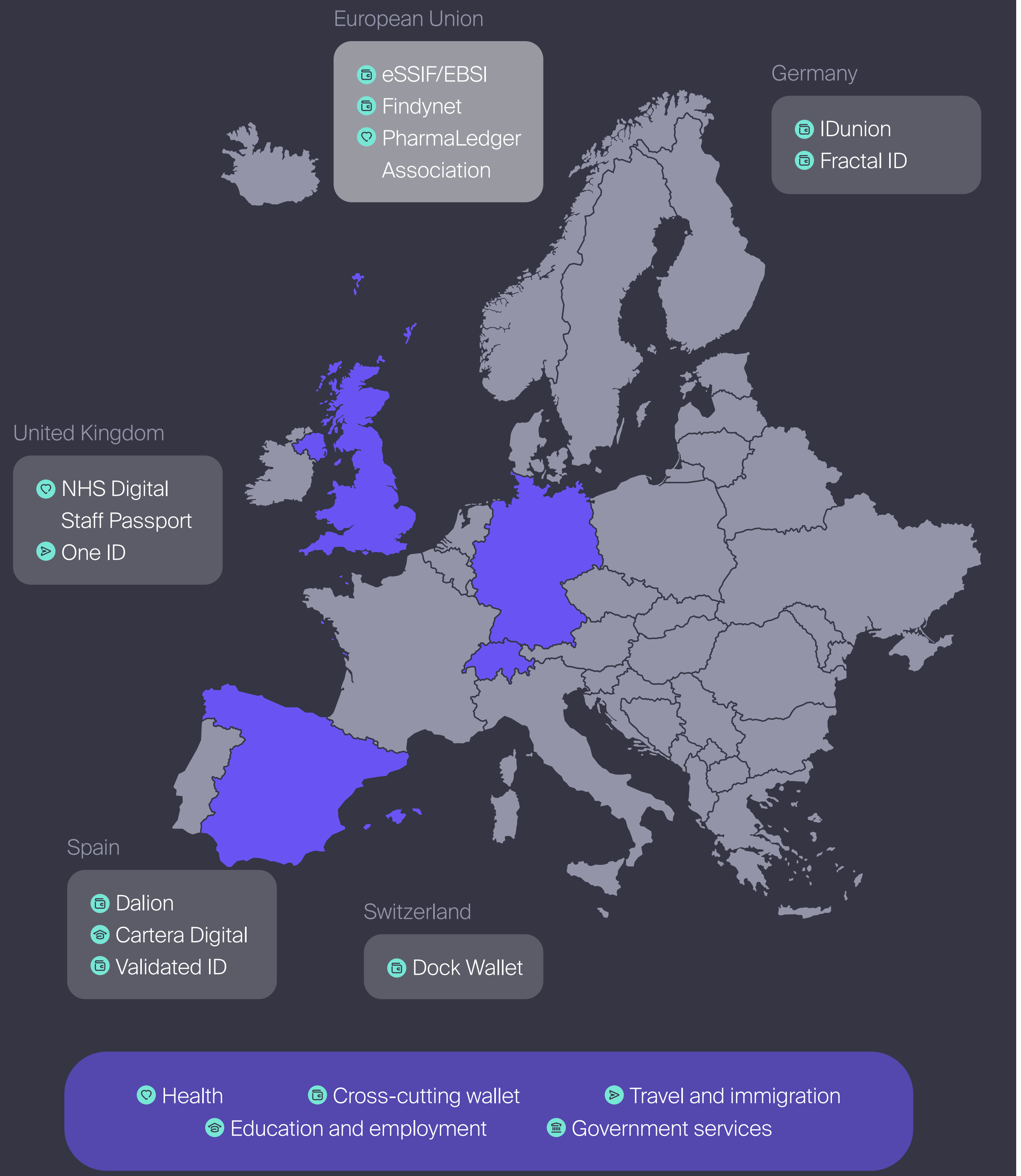
Private entities around the world have begun to devise and implement SSI models. In the United States, one of the most reputable platforms originated: the **Sovrin Foundation.** The foundation has three SSI networks, based on Hyperledger Indy, each consisting of between 4 and 25 nodes operated by Sovrin administrators. Additionally, it acts as a Governing Authority and operates the network as a whole, overseeing and enhancing its performance.

Throughout North America and South America, there are other initiatives such as the Colombian **Xertify**, which is educational in nature, and the Argentine **QuarkID**, a multichain SSI application from the city of Buenos Aires whose protocol is anchored in the zkSync, Ethereum, Polygon, and Rootstock networks.

In Africa and Asia, projects have emerged such as the South African educational platform for youth, **Yoma**, and the Indian e-wallet, **Soulverse**. However, Singapore predominates regionally, with numerous projects in progress.

Ultimately, Australia and New Zealand have joined the SSI wave through regional government projects **(NSW Digital ID)** or private solutions **(MATTR)**.





European Union
- eSSIF/EBSI
- Findynet
- PharmaLedger Association

Germany
- IDunion
- Fractal ID

United Kingdom
- NHS Digital Staff Passport
- One ID

Spain
- Dalion
- Cartera Digital
- Validated ID

Switzerland
- Dock Wallet

Health · Cross-cutting wallet · Travel and immigration · Education and employment · Government services

Europe Leads the Change: From Regional Initiatives to National Ones

Europe is the region where the largest number of initiatives and projects related to SSI have emerged globally. In fact, it is home to numerous public-private collaborations in the fields of governmental digital identification, cross-cutting e-wallets for various purposes, and initiatives in health, travel, and education. At the regional level, the European Union has been a pioneer not only in regulatory matters but also in launching practical SSI projects. **The European Self-Sovereign Identity Framework (eSSIF)** is an initiative aligned with the GDPR and eIDAS 2, aimed at providing EU citizens with more direct and secure control over their digital identity, based on blockchain technologies to ensure that digital identities are verifiable and reliable, without the need for an intermediary entity. It allows identities to be **interoperable** across the European Union, improving transparency and **reducing bureaucracy in administrative processes** such as document issuance and verification of educational credentials. Implementation is set to begin in 2026, with expectations that by 2030, 80% of the population will have access to a European identification system.

Finally, there are other regional private initiatives in Europe such as **Findynet**, which allows users to collect receipts, tickets, permits, certifications, and other proofs to facilitate and strengthen interactions, or **PharmaLedger**, which aims to create a secure digital ecosystem for the health sector.

At the national level, pioneering projects include **Dalion**, a Spanish SSI system resulting from a consortium of private companies based on the **Alastria** digital identity model, and the German **IDunion**, which aims to create a global and decentralized ecosystem for identity management based on European values. Meanwhile, One ID is the British initiative founded by IATA to streamline travel through the digital advance exchange of information, and **Dock Wallet** is the Swiss platform that enables organizations to issue, manage, and verify credentials effectively and securely.

04

Cross-Sector Opportunities: What Does SSI Mean for Your Industry?

Self-sovereign digital identity offers cross-sector opportunities that can transform multiple industries. Generally speaking, it directly impacts five aspects:

1. **User Experience:** SSI can simplify customer onboarding processes by replacing complex procedures with simple one-click processes, significantly improving the user experience.

2. **Data Quality:** In the face of potential issues with data accuracy or consistency due to typos or incorrect information provided by customers, SSI ensures high-quality data based on information verified by trusted third parties.

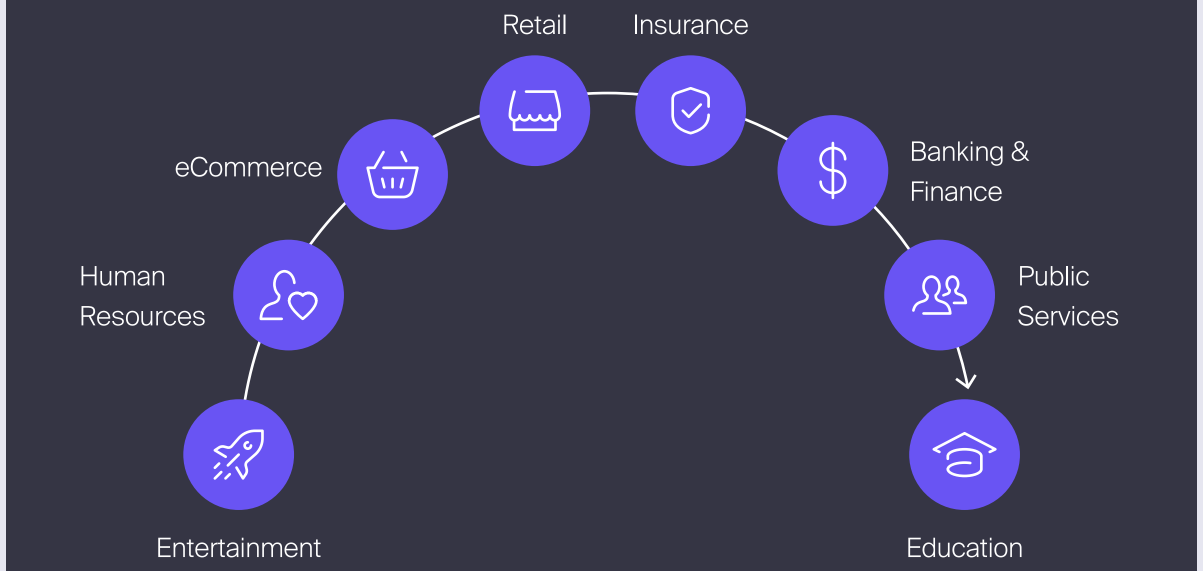
3. **Security:** With SSI, companies can implement more secure authentication methods, thereby minimizing risks through decentralized storage and reducing sensitive data.

4. **Privacy and Compliance:** SSI facilitates consent management and automates compliance with data protection regulations.

5 . **Process Automation:** SSI allows access to reliable and structured data, enhancing better process automation.

Self-sovereign identity

SSI is related to a non-exhaustive series of sectors that continues to grow as technology develops.



Entertainment

Human Resources

eCommerce

Retail

Insurance

Banking & Finance

Public Services

Education

Banking and Finance: Transformed Risk Management and Compliance

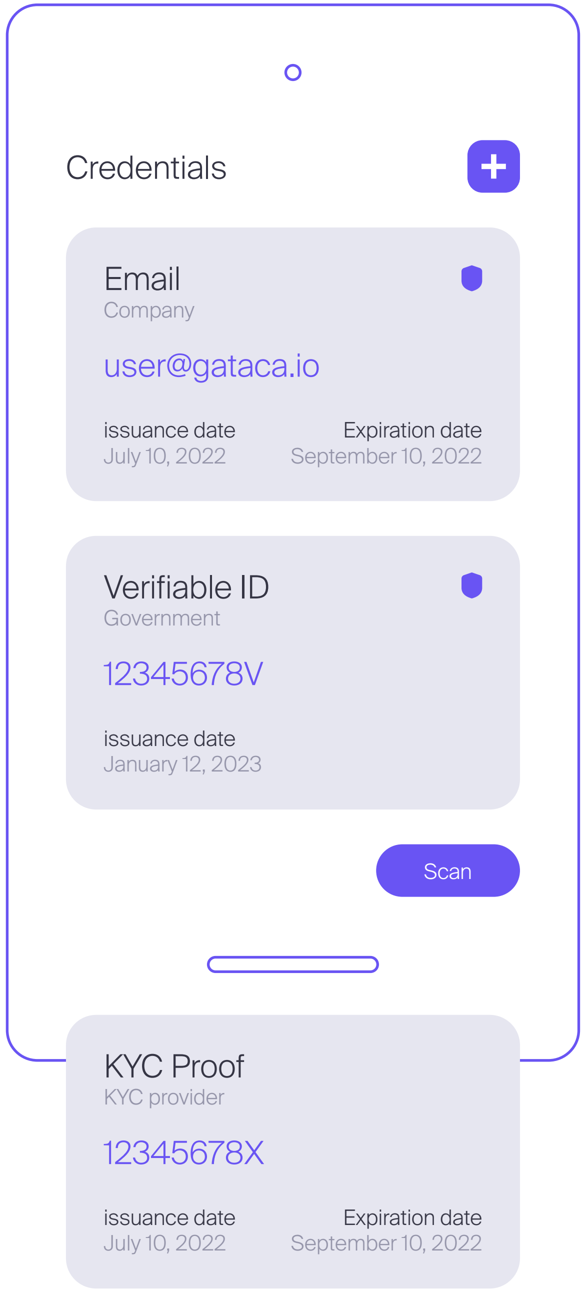
In the banking sector, self-sovereign digital identity is **revolutionizing risk management and regulatory compliance.** One of the main challenges in banking is identity verification, which is necessary in both centralized (CeFi) and decentralized finance (DeFi), where customer verification procedures (KYC) are often inefficient and unsatisfactory.

SSI provides an effective and privacy-respecting solution by creating an identity layer that acts as a bridge between traditional processes, which require large amounts of data, and the anonymous approach of decentralized finance. Unlike traditional KYC, which is used once for each entity, SSI allows verified information to be securely and audibly reused, thereby improving efficiency and reducing the risk of fraud. In this regard, SSI enables users to have complete control over their verifiable credentials. This means that the **customer only shares strictly necessary information, ensuring greater privacy without compromising the accuracy of the data.**

Additionally, SSI introduces a **reusable approach to KYC**, preventing users from having to repeat the process at each institution or financial service, thus optimizing the onboarding experience and strengthening regulatory compliance in a more agile and auditable manner.

In terms of regulatory compliance, SSI also facilitates adherence to regulations such as anti-money laundering (AML) laws and KYC processes by automating and simplifying identity verification through verifiable credentials issued by trusted entities. This technology not only prevents fraud but also allows banking institutions to reduce credit risk by enabling instant fund validation and accurate risk assessment. By providing traceable and auditable personal information, SSI ensures that institutions can meet regulatory requirements without compromising customer privacy.

Moreover, SSI improves operational **efficiency in the management of financial assets** by facilitating the ownership, exchange, and trading of assets in a more secure and transparent manner. The ability to decentralize identity verification and financial transactions helps reduce operational costs and the risks associated with handling large volumes of personal data. Together, SSI can transform the way banks manage risk and compliance, **providing greater security, privacy, and trust for both financial institutions and their customers.**

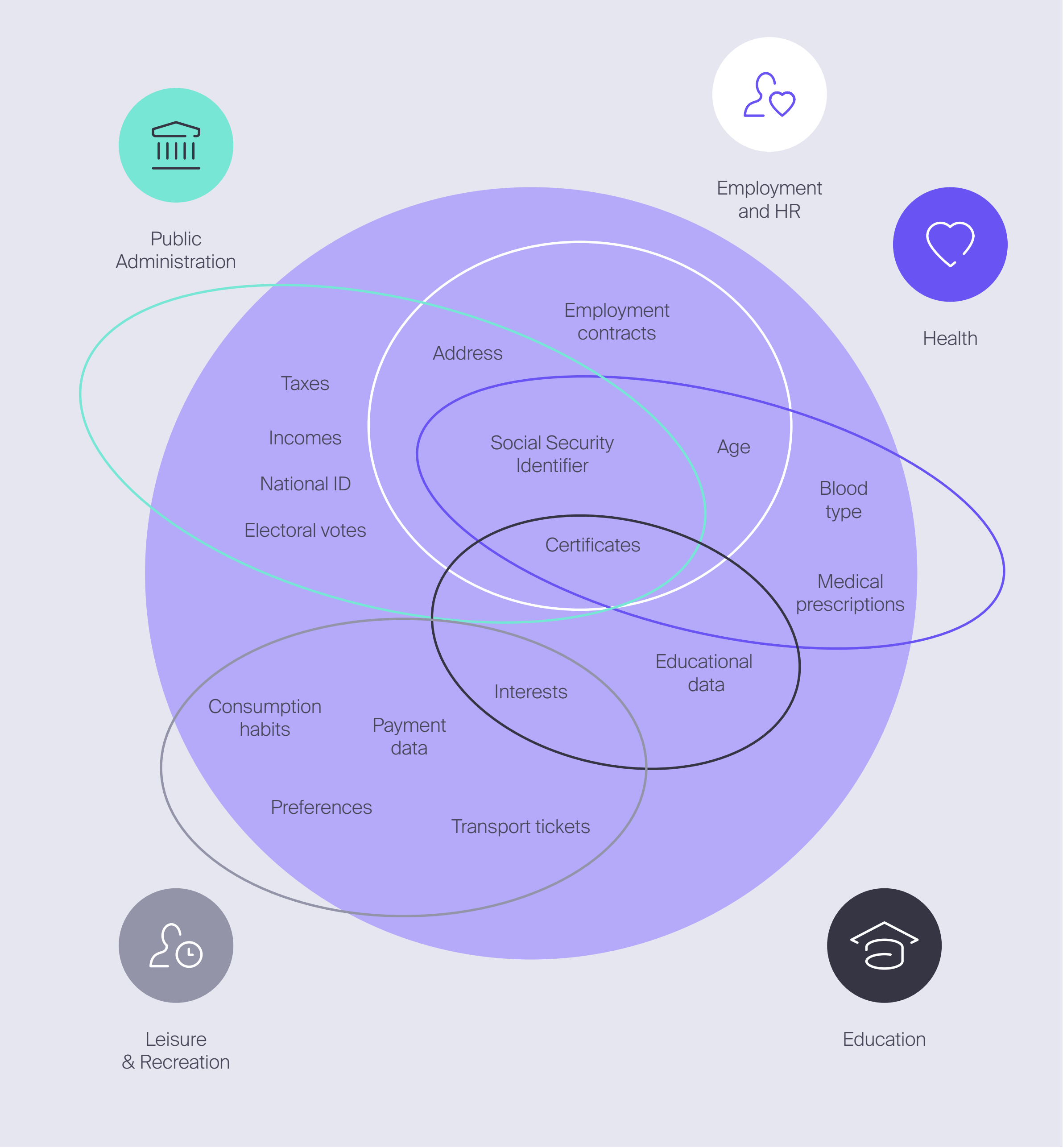


Credentials

Email
Company
user@gataca.io
issuance date July 10, 2022
Expiration date September 10, 2022

Verifiable ID
Government
12345678V
issuance date January 12, 2023

KYC Proof
KYC provider
12345678X
issuance date July 10, 2022
Expiration date September 10, 2022



Education and HR: A New Ecosystem of Credentials and Hiring

The cross-cutting utility of SSI extends to sectors beyond finance or e-commerce. In fact, SSI is also **transforming the education and human resources ecosystem**, particularly in the management of credentials and hiring processes. In the educational sphere, SSI allows students to have full control over their academic records. This means that **diplomas, certificates, and educational achievements can be securely stored in a digital wallet and shared quickly and efficiently with any institution or employer.** This simplified management not only enhances the student experience but also ensures the authenticity and privacy of documents, reducing the risk of forgery or loss of sensitive information.

When applying for a spot at a university or registering for an exam, the citizen simply shares the relevant credentials from their wallet with the corresponding educational institution. This university, using SSI technology, can immediately verify the authenticity of diplomas, certificates, and other documents, thereby reducing bureaucratic processes.

In this sense, this ecosystem of verifiable credentials also has a significant impact on the job market and human resources departments. **Companies can directly and securely access academic records and certifications through SSI platforms**, eliminating the need for external verifications and reducing the time required to confirm the validity of candidates' degrees and skills. This is especially valuable in industries where certifications and continuous training are crucial, as employers can gain a clearer and more accurate view of a candidate's competencies.

In summary, the combination of SSI with the education and human resources sectors is creating **a new ecosystem of credentials and hiring**. Students and professionals have more control over their achievements and experiences, while educational institutions and employers benefit from more efficient and reliable processes for verifying these credentials.

eCommerce and Customer Experience: Beyond Traditional UX

E-commerce is undergoing a radical transformation thanks to self-sovereign digital identity, advancing traditional user experience (UX) practices. In this new landscape, SSI technology offers consumers and businesses **greater transparency and trust in transactions, particularly in supply chain management.**

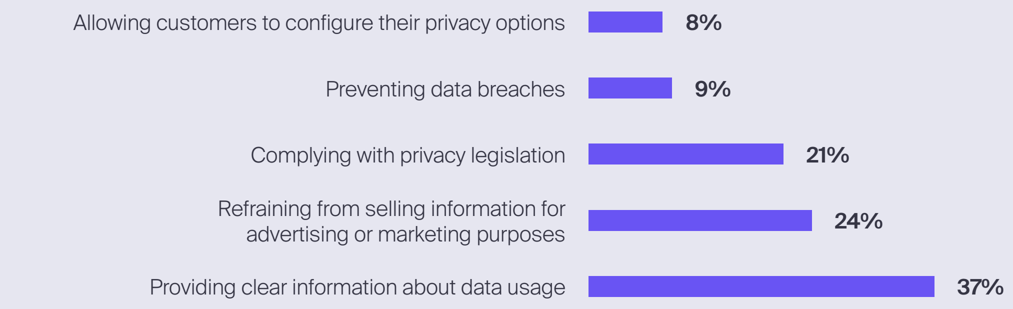
Firstly, regarding UX, **SSI gives users control over their personal and payment information.** By using SSI, buyers can selectively share only the strictly necessary data to complete a transaction, significantly improving privacy and security.

In the realm of purchasing and supply chain management, one of the main benefits of SSI is the ability to **track assets and products from their origin to the point of sale, integrating sensor networks and the Internet of Things (IoT).** This not only enhances traceability but also reinforces consumer trust, as they can be assured of the authenticity of the products they purchase.

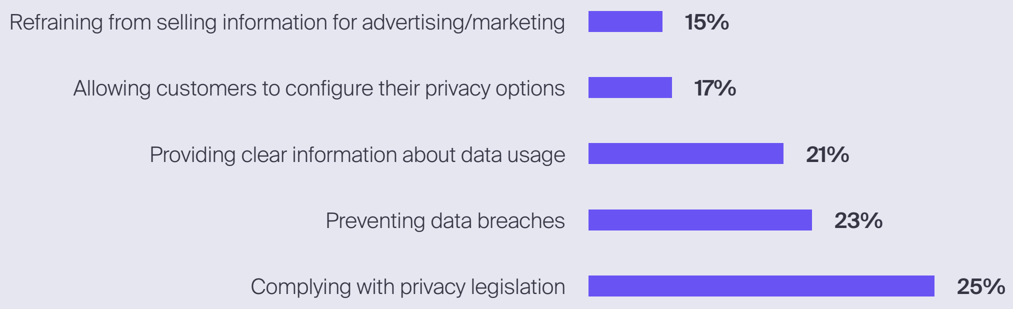
In this sense, SSI plays a crucial role by enabling companies **to verify the authenticity of products and the reliability of their suppliers**. This verification is particularly useful in sectors such as luxury goods, food, or technology, where product authenticity is a primary value. This factor also ensures that suppliers comply with regulations, contracts, and standards, generating greater transparency throughout the supply process.

> In light of consumer distrust regarding the handling of their data, and parallel to the rise of privacy regulations, SSI positions itself as a key solution in the field of commerce.

Global Consumer Opinion on How Companies Can Build Trust Regarding Data Privacy in 2023



Global Companies' Perspective on How to Build Consumer Trust Regarding Data Privacy in 2023

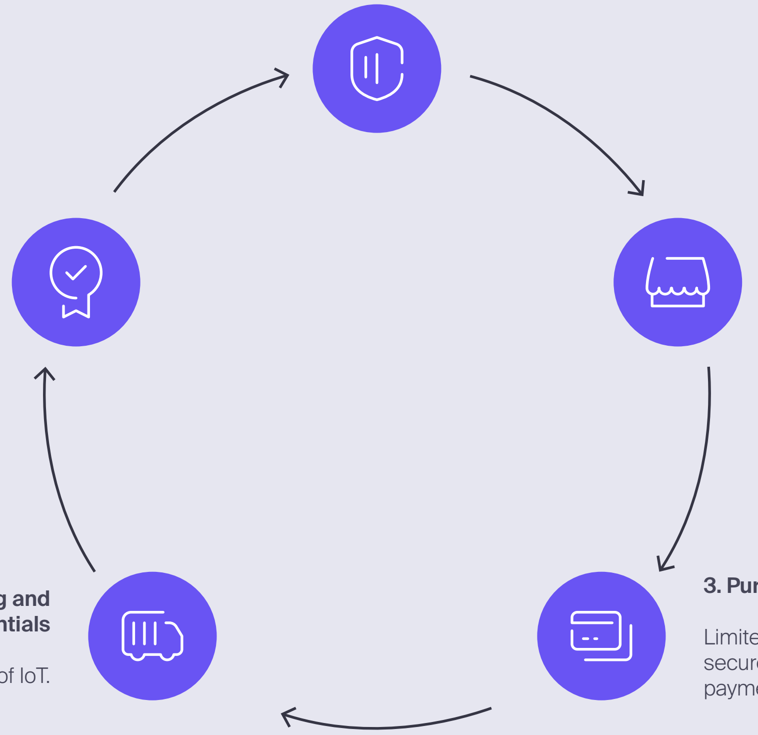


The impact of SSI is not limited to the supply chain. Companies can also use this technology to **verify documents related to shipping, company details, or even the credentials of carriers and logistics operators.** This approach ensures that all parties involved in commerce, from production to final delivery, are aligned and comply with the highest standards of quality and reliability.

By reducing trust gaps between parties and increasing visibility at each stage of the process, **SSI revolutionizes the experience for both consumers and businesses**, enhancing security and efficiency in transactions.

Ultimately, transparency, authenticity, and security are key elements that transform the relationship between brands and consumers. This new paradigm not only guarantees a **smoother and more reliable shopping experience** but also **strengthens the overall commercial ecosystem**, allowing companies to offer authentic, high-quality products backed by a reliable digital verification system.

SSI provides greater transparency, traceability, and trust in product authenticity, while also ensuring data protection throughout the supply chain



1. Authentication and Verification

Of the customer and supplier.

2. Verification of Product and Supplier Authenticity

Throughout the supply chain with the participation of IoT.

3. Purchase Process

Limited credential exchange securely and transparently for payment.

4. Verification of Shipping and Logistics Credentials

Essential participation of IoT.

5. Delivery and Confirmation

Complete authenticity tracking.

Frictionless Digital Onboarding

Digital onboarding is one of the processes most impacted by SSI, **facilitating the user onboarding process to platforms and services in an agile and secure manner.** Unlike traditional methods that require repeated entry of personal, financial, or employment information at multiple stages, the use of SSI allows users to share only the strictly necessary data from a digital wallet. This approach eliminates the need for forms, reducing the time and effort required to complete the onboarding process while ensuring the authenticity of the information. This significantly improves the user experience by reducing friction and barriers to entry.

From a strategic perspective, companies across multiple sectors can utilize SSI to **optimize all aspects of onboarding, whether for new customers, employees, or suppliers.** For example, instead of requiring new users to create multiple passwords and verify their identity with documents at different stages, SSI enables **single, decentralized authentication.** Users simply share their verifiable credentials—be it their identity, contact details, or payment methods—securely and efficiently. This minimizes the points of vulnerability that are often present in traditional data entry processes.

A key aspect of frictionless onboarding is the ability to **maintain a balance between simplicity and privacy.** Once again, with SSI, users have full control over what information they share and with whom, fostering greater trust and reducing the fear of potential data breaches. For companies, this not only enhances customer or employee satisfaction but also **minimizes the risk of human error or fraud, as the credentials used in the onboarding process are verified and backed by a robust security infrastructure.**

Ultimately, SSI can also simplify more complex processes, such as setting up payments or verifying identity for employee hiring. For instance, by integrating SSI into a payment system, users can securely connect their bank accounts or credit cards without needing to enter their information repeatedly. This accelerates transactions and makes the process more efficient, offering a **seamless user experience from the very beginning.**

1. **The insurance sector** could also benefit from SSI, thanks to more secure and efficient management of customer information, as well as the development of hyper-personalized products and the creation of accurate and dynamic risk profiles.

2. In the **healthcare sector**, potential uses include the issuance of prescriptions, appointment scheduling, management of medical records, filing claims with insurance companies, and the exchange of medical records, facilitating communication between patients and healthcare professionals.

3. In the **real estate sector**, the issuance of key documents for tenants, buyers, and sellers as VCs could reduce tedious processes, decreasing the chances of identity fraud.

05

Take Action Now: Integrating SSI into Your Digital Strategy

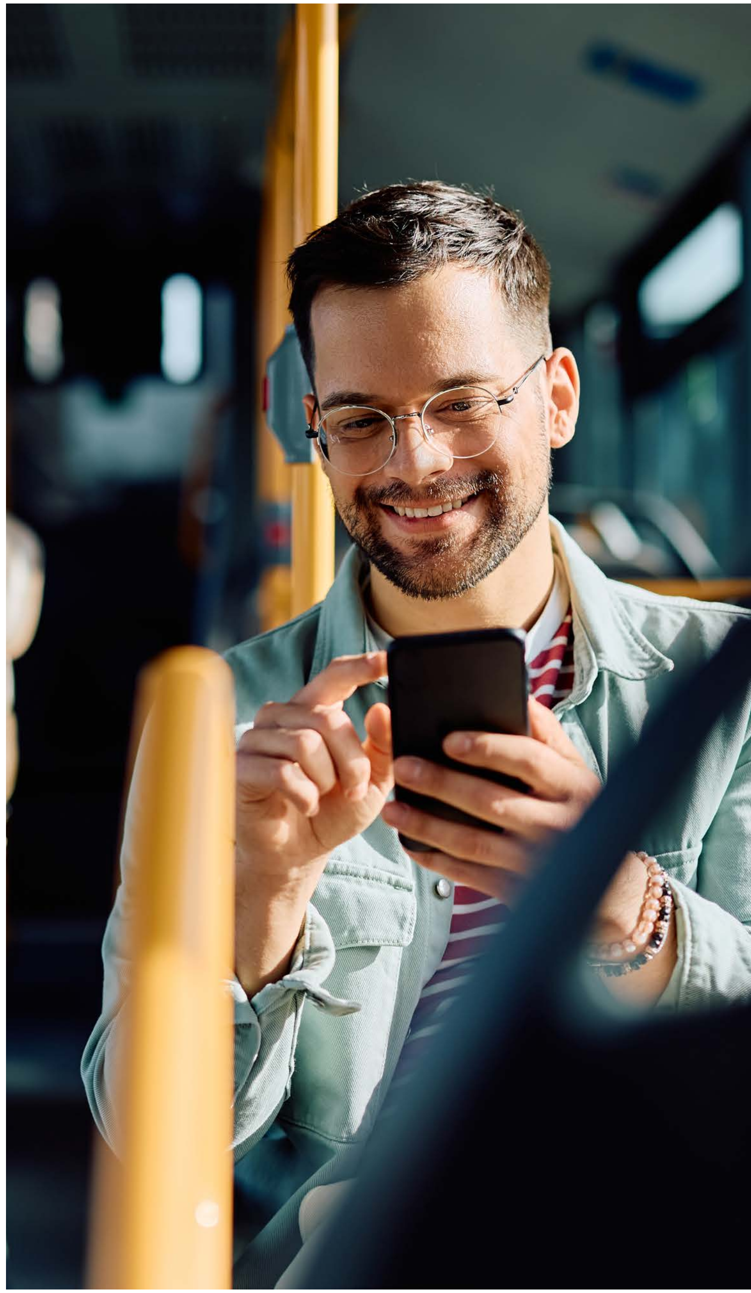
Public-Private Collaboration: The Key to Successful Adoption

Public-private collaboration is crucial for the successful adoption of self-sovereign digital identity, and legislation plays a key role as a driver of this adoption. Indeed, governments, by implementing regulations that **govern** and support the use of SSI, **provide a solid legal and technological foundation upon which companies can develop innovative and secure solutions**, creating the necessary framework for the corporate world to leverage this infrastructure for their operations.

Therefore, **legislation not only acts as a facilitator but also creates incentives for the mandatory adoption of certain systems**, such as government digital identities. By standardizing these systems at the national or supranational level, as in the case of the EU, companies have a trust framework upon which to build, minimizing fragmentation and maximizing interoperability. This is essential, as one of the biggest challenges for SSI adoption is the lack of an interoperable and regulated ecosystem where both public and private entities can interact under the same technological and legal standards.

An example of this synergy is the eIDAS Regulation in Europe, which has laid the groundwork for a more harmonized digital identity ecosystem. With the revision of eIDAS 2.0, a **"European digital identity wallet"** is proposed, allowing citizens to manage their identity sovereignly across multiple contexts, **from government services to private transactions.** Companies will be able to utilize this infrastructure to reduce costs in identity verification processes and improve user experience, relying on identities verified by the state.

In the case of **Singapore**, thanks to Singpass, an originally governmental initiative that is now robustly implemented, citizens already have access to **over 2,700 services from more than 800 public agencies and businesses**, demonstrating the potential of public-private collaborations. Citizens can both sign documentation and verify transactions. Additionally, **SGFinDex** has recently been integrated, a platform designed to facilitate financial planning that allows users to connect their accounts with financial entities and public agencies and securely manage all their finances in one place.



Investing in SSI Infrastructures: Building the Foundations for Change

To effectively implement SSI, companies must invest in a **technological infrastructure that combines blockchain/DLT, advanced cryptography, management of verifiable credentials, and secure digital wallets.** This approach enables the creation of an ecosystem where users control their identity securely, in a decentralized and private manner, minimizing reliance on intermediaries and enhancing the security and privacy of data.

1. **Blockchain and DLT** technology provide a mechanism to ensure integrity, transparency, and decentralization in the storage of identity data. Although the identity itself is not stored on the blockchain, verifiable records can be stored to ensure the immutability of identity-related transactions.

- **Ethereum** can be used for smart contracts and to create decentralized trust networks.
- **Hyperledger Indy** is specifically designed for the management of decentralized identities.
- **Corda, Quorum, or Polkadot** can be utilized for identity solutions.

Investment in **development or integration with a public or private blockchain**, node infrastructure, and management of smart contracts.

2. **Asymmetric cryptography (PKI - Public Key Infrastructure),** since decentralized identities rely on the possession of pairs of cryptographic keys (public and private) to digitally sign credentials and verify authenticity without intermediaries.

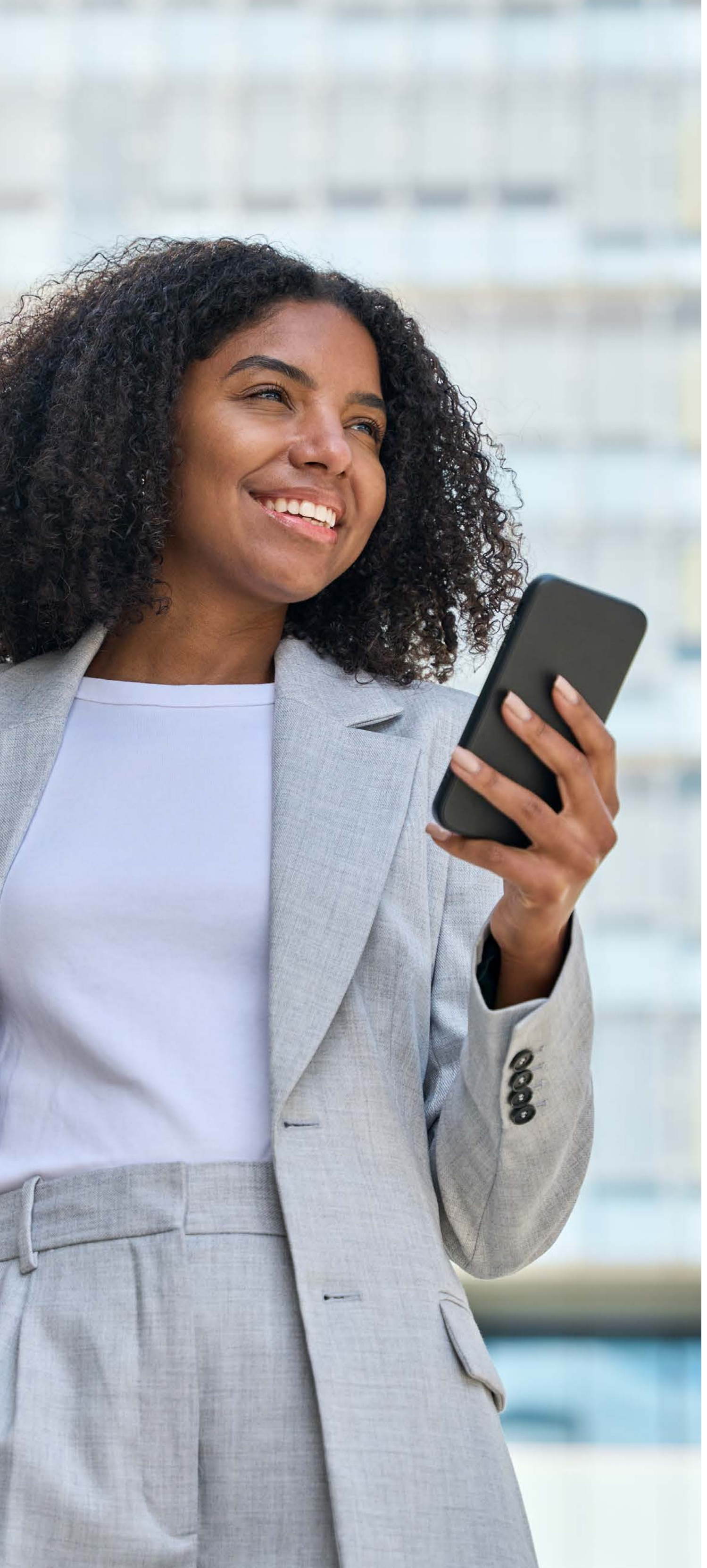
- **Key Management Systems (KMS)** such as AWS KMS or Google Cloud KMS for storing private keys.
- **Digital signature protocols:** Tools like Elliptic Curve Digital Signature Algorithm (ECDSA) or RSA.

Investment in the **integration of infrastructure for the generation, storage, and retrieval of secure key**s for users.

3. **Decentralized Identifiers (DIDs),** , global and unique identifiers that allow for the creation of identities without the need to rely on a centralized authority. Each user has a DID associated with their identity.

- **W3C Decentralized Identifiers (DID) standard:** Standards for the creation and management of decentralized identifiers.
- **Frameworks like Sovrin or uPort:** These platforms implement the DID standard and provide infrastructures for managing SSI identities.

Investment in developing the **capability to manage and resolve DIDs**, as well as interoperability with other solutions based on the standard.



4. **Verifiable Credentials (VC),** ,the foundation of SSI, allow companies to issue, verify, and revoke identity credentials that individuals control and share securely between users and verifiers.

- The **W3C Verifiable Credentials standard**, which defines how credentials are issued, stored, and verified in an SSI system.
- Frameworks that implement the verifiable credentials standard, such as **Hyperledger Aries and AnonCreds.**

Investment in implementing solutions that allow for the **secure issuance, verification, and managemen**t of credentials.

5. **Digital wallets** to securely store cryptographic keys, DIDs, and verifiable credentials, allowing individuals to manage their identity sovereignly.

- SSI Wallets such as **uPort, Sovrin Wallet, or Evernym.**
- Development of white-label wallets.

Investment in the **development or integration of digital wallets** compatible with SSI infrastructure, and support for mobile and desktop devices.

6. **Secure Storage and Off-Chain Data** to keep sensitive identity data and credentials off-chain to protect privacy.

- Decentralized systems for the secure off-chain storage of data, such as **IPFS (InterPlanetary File System) or Storj.**
- Encrypted databases like **SQLCipher** or **MongoDB with encryption** to manage identity data.

Investment in **decentralized storage or encrypted storage solutions to keep data secure and private.**

Consumer Education: A Must in the Digital Age

Traditional identity management systems often fix identity in rigid categories, making it difficult for individuals to adapt their identity to changing circumstances. In contrast, **SSI invites a dynamic understanding of identity that can evolve over time**, allowing individuals to update their identity attributes as needed.

This flexibility, informed by the principles of autonomy, control, and access, places an obligation on the user or consumer to educate themselves regarding its use. However, **46% of internet users globally are unaware of the existence or content of regulations** that protect their data privacy. Despite this lack of awareness, by 2024, the proportion of the global population covered by modern privacy regulations is expected to reach 79%, compared to just 10% in 2020.

Furthermore, the percentage of internet users who had already adopted some measure to protect their data privacy in June 2023 was 42% among the 18-24 and 25-34 age groups, while the average across all age groups was 33%. This demonstrates a need to tailor education strategies according to age group.

At the same time, **the number of data requests** from users to tech giants, including Apple, Google, Meta, and Microsoft, is increasing. American users are the most active in this regard, making **over 1.2 million queries between 2013 and 2021.** They were followed by Indian users, with more than 460,000 requests, Germans (~366,000 requests), Brits (~275,000), and French (~271,000).

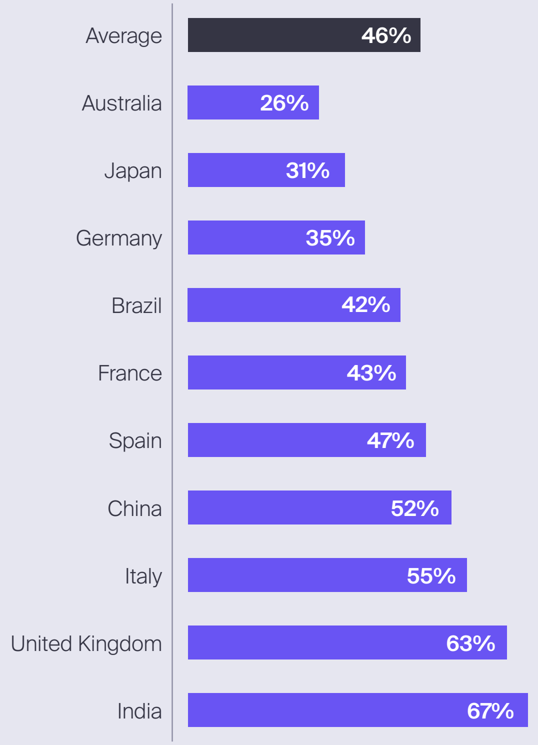
In this context, it is vital for the widespread implementation of SSI that **consumers or users become increasingly aware of the protection framework** provided by institutions at the regulatory level and by companies for their daily use. Their education will lead to greater trust in SSI identification systems, and their awareness as owners of their data will be essential for the development and improvement of these systems.

81% of Americans are **concerned about companies using their data.**

56% say they never read **privacy policies** before accepting them.

~35% of Europeans are concerned about companies using their **data.**

Global Internet Users' Awareness of Privacy Legislation in Their Country in June 2023

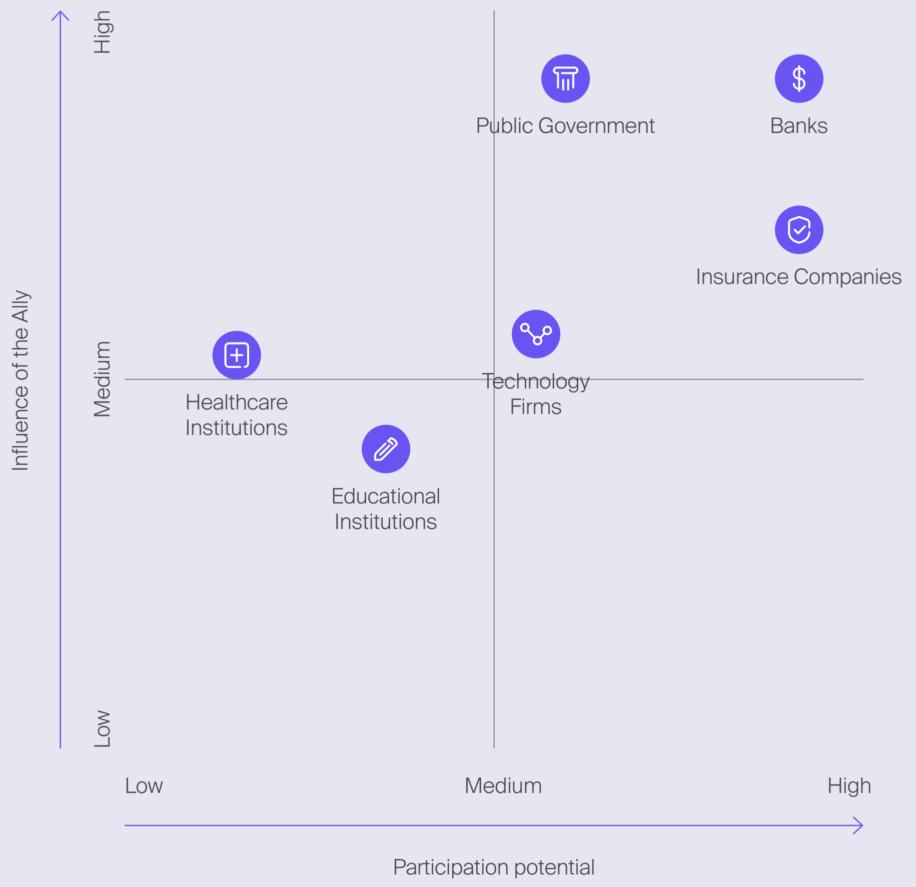


Strategic Alliances: Co-creating the Future of the Ecosystem

Strategic alliances, along with cross-sector cooperation among different industries, strengthen the SSI ecosystem, enhancing user experience and ensuring greater control over their identities. In particular, **strategic partnerships with banks** and insurance companies play a fundamental role in credential verification and the development of the SSI ecosystem. These institutions already hold large volumes of data about their users, making them key issuers and verifiers of identities.

Banks, for example, can issue verifiable credentials (VCs) based on the information they already manage about their clients, such as financial and personal data. This not only gives them a central role in the SSI ecosystem but also streamlines verification processes and increases security and privacy by eliminating the need to rely on third parties to authenticate information. Additionally, insurance companies can play a crucial role in validating critical data related to insurance and claims, enhancing trust and efficiency throughout the ecosystem.

Another key alliance in this environment is the collaboration with technology companies and **blockchain platforms**, essential for providing the technical infrastructure that allows self-sovereign identities to operate securely and at scale. These alliances include the development of encryption technologies, blockchain to ensure data immutability, as well as the creation of digital wallets that enable users to manage their credentials. In addition to alliances with banks, insurance companies, and technology firms, there are other important strategic partnerships that strengthen this system. Among these, **governments** are key actors in the issuance of official credentials, such as identifications, driver's licenses, and academic degrees. Collaboration with governments reinforces the legitimacy of the SSI system and helps establish global standards for its implementation. Furthermore, universities and educational institutions can also issue VCs, such as diplomas and certificates, and healthcare institutions issue medical credentials, such as medical records or vaccination certificates.



softtek.com

Softtek®