Update · October 2021

White paper

XSL LABS

A tamper-proof and decentralized digital identity

XSL LABS

XSL Labs undertakes to deploy a means of identification that makes digital identity verifiable and decentralized. Through an ecosystem of alternative services and interoperability, the Secure Decentralized Identity solution will seamlessly integrate with all the solutions of both today's and tomorrow's Internet.

TABLE OF CONTENTS

TABLE OF CONTENTS

01

Introduction

1. INTRODUCTION

For the past ten years, our relationship to the Internet has been transformed to the point where almost all of our identity and life data, such as personal records or information about our tastes, habits or social environment, is available and stored in centralized databases. Additionally, institutions and companies store the customers' data in their centralized systems, but their vulnerabilities allow cybercriminals to steal the data and then sell it on the dark Web or use it to blackmail these institutions and companies.

Figures confirm this spectacular increase over the past decade and suggest an even greater one in the future. Cybersecurity Ventures predicts that the global costs of cybercrime will increase by 15% per year during the next five years, reaching 10, 500 billion dollars per year by 2025, up from 3,000 billion dollars in 2015. This represents the largest transfer of economic wealth in history, threatens incentives for innovation and investment, is exponentially more important than the financial damage inflicted by natural disasters annually, and will be more profitable than the global trade of all major illegal drugs combined. If the entire wealth stolen by cybercrime in a year was counted as a country's GDP, it would be the fourth richest country in the world[1], ahead of Japan.

These figures show the importance of this cost to the global economy. Indeed, data theft not only harms institutions themselves, but also causes considerable losses both in terms of money and time. Globally, in 2020, a single data theft inflicts on average a 3.86 million dollars loss. The report also shows a correlation between the cost of a data theft and the time it takes to detect and contain the threat. The cost of a data theft is estimated to an average of 150 dollars per customer[2].

For this reason, Georges Tresignies and Ludovic Ryckelynck developed their thoughts on technological solutions that could help solve such problem for the global economy, institutions, companies and users. They gathered a team under the name XSL Labs, whose ambition was to develop a solution based on the blockchain's decentralized technologies and the recent work of the W3C on decentralized identity (DID[3]). XSL Labs has grown rapidly. Today, the development team is led by Frédéric Martin and Imad El Aouny, cybersecurity experts specialized in blockchain solutions, smart contracts and decentralized identifiers (DID).

Since March 2020, XSL Labs has been developing a decentralized identifier called Secure Digital Identity (SDI) and ONE, a decentralized application (dApp[4]) that enables the SDI management. Ultimately, by decentralizing data storage, the company aims to fight the growing cost of data theft for institutions and businesses while giving SDI users back full sovereignty over their data. Thus, a rich and diverse ecosystem of dApps will be developed around the use of the SDI and the entire system will be powered by its utility token, the SYL.

XSL Labs intends to revolutionize the fight against data theft on today's Internet as well as on the upcoming Web 3.0[5].

1 Cybercrime Magazine

2 According to the IBM report

3 Decentralized Identifiers (DIDs) W3C

4 Decentralized applications (dApps) are applications built on decentralized networks.

5 Web 3.0 is the third generation of Internet services for websites and applications. The goal is to use machine learning to deliver a data-driven semantic Web, with the ultimate goal of creating more intelligent, connected and open websites.

02
External technologies used

2. EXTERNAL TECHNOLOGIES

The purpose of this section is to present the external technologies that the SYL ecosystem will rely on.

Section 2.1 presents both the network on which XSL Labs has developed and the one on which they will develop the technological solution presented in this White Paper, namely the Binance Smart Chain and Flare Network.

The section 2.2 presents Smart Contracts technology.

The section 3 presents the technology developed by XSL Labs, the SYL ecosystem.

2.1 NETWORKS & BLOCKCHAINS

2.1.1 BINANCE SMART CHAIN

After studying every possible technological options to provide the best service to its users, XSL Labs implemented its ecosystem on the Binance Smart Chain (BSC) network.

The Binance Smart Chain is a blockchain using a proof-of-stake[6] consensus algorithm. More precisely, it uses an algorithm called Proof of Staked Authority (or PoSA[7]) that allows participants to stack their BNBs to become validators. If they provide a valid block, they receive the fees for the transactions included in that block.

The network allows transactions to be carried out with fees 100 times lower and at least 10 times faster than the Ethereum network. Beyond this performance, the BSC is able to produce a new block every 3 seconds. Its compatibility with Ethereum tools and in especially its virtual machine (EVM[8]) also allows the network to be extended to all dApps on Ethereum network and their migration to BSC.

All of these advantages have led XSL Labs to initially favor Binance Smart Chain for the SYL token smart contract and the first SDI smart contract.

6 Proof of Stake is a block validation method meant to achieve distributed consensus.

7 "Binance Smart Chain uses a consensus model called Proof of Staked Authority (PoSA). It's a hybrid between Proof of Authority (PoA) and Delegated Proof of Stake (DPoS). This consensus model can support a short block time and low fees, and it only requires 21 validators to run. Validators take turns to produce blocks. They essentially power the BSC network by processing transactions and signing blocks. In return for their service, they earn a reward in BNB tokens. Meanwhile, they also require daily re-election by staking governance to be able to continue to be part of the validator set. What are the requirements to be a validator? A validator needs to spin up a hardware node with the required specs, run a full BSC node, and stake a minimum of 10,000 BNB. But that's not all. These requirements are only enough to become an elected candidate. In order to actually start producing blocks, a validator candidate needs to become an elected validator. Elected validators are the top 21 validator candidates with the highest amount of voting power. They change every 24 hours through an ongoing election process, and you can check them out on the top validator list on Binance.org." (Source : https://academy.binance.com/fr/articles/a-quick-guide-to-bnb-staking-on-binance-smart-chain-bsc)

8 The Ethereum Virtual Machine (EVM) is a sub-layer system of the Ethereum platform, it is the one that allows the calculations related to the implementation and execution of smart contracts on the blockchain.

2.1.2 FLARE NETWORK

XSL Labs will eventually deploy smart contracts (see section 2.2 : Smart Contracts) on the Flare network for several reasons.

The Flare blockchain is a new blockchain that also uses EVM and thus allows the creation of smart contracts (in Solidity[9] language). This network is intended to be different from Ethereum because it uses the Avalanche[10] consensus protocol. This allows to have a network as secure as networks using PoW[11] and PoS[12], without requiring the use of high-end, expensive and power-hungry machines like PoW networks, nor asking users to lock their tokens on smart contracts.

Flare Network aims to have a network that supports smart contracts, like Ethereum, but with transaction costs as low as XRPL[13]. That is why Flare uses Federated Byzantine Agreement (FBA), while also using the Ethereum Virtual Machine (EVM).

Smart contract developers who have been working on Ethereum in Solidity will not need to learn a new programming language to create smart contracts on Flare Network, ensuring a smooth transition. It also provides Flare with the assurance that a vast majority of blockchain developers already have the knowledge and resources to create smart contracts on its network.

Thus, Flare will be the second network on which a smart contract for the SDI will be deployed. Depending on technological advances and partnerships, other blockchains may be supported.

9 Solidity is an object-oriented programming language used by computer developers to write smart contracts.

10 "Consensus is the task of getting a group of computers to come to an agreement on a decision. Computers can reach a consensus by following a set of steps called a consensus protocol. Avalanche is a new consensus protocol that is scalable, robust, and decentralized. It has low latency and high throughput. It is energy efficient and does not require special computer hardware. It performs well in adversarial conditions and is resilient to "51% attacks"." (Source : https://docs.avax.network/learn/platform-overview/avalanche-consensus)

11 "Proof of Work (commonly abbreviated to PoW) is a mechanism for preventing double-spends. Most major cryptocurrencies use this as their consensus algorithm. That's just what we call a method for securing the cryptocurrency's ledger. Proof of Work was the first consensus algorithm to surface, and, to date, remains the dominant one. It was introduced by Satoshi Nakamoto in the 2008 Bitcoin white paper, but the technology itself was conceived long before then. Adam Back's HashCash is an early example of a Proof of Work algorithm in the pre-cryptocurrency days. By requiring senders to perform a small amount of computing before sending an email, receivers could mitigate spam. This computation would cost virtually nothing to a legitimate sender, but quickly add up for someone sending emails en masse." (Source : https://academy.binance.com/fr/articles/proof-of-work-explained)

12 "The Proof of Stake consensus algorithm is the most common alternative to Proof of Work. PoS systems were designed to solve some of the inefficiencies and emerging problems that commonly arise on PoW-based blockchains. It specifically addresses the costs associated with PoW mining (power consumption and hardware). Basically, a Proof of Stake blockchain is secured in a deterministic way. There is no mining in these systems and the validation of new blocks is dependent on the number of coins being staked. The more staking coins a person holds, the higher the chances of being picked as a block validator (also known as minter or forger). While PoW systems rely on external investments (power consumption and hardware), a Proof of Stake blockchain is secured through an internal investment (the cryptocurrency itself). Additionally, PoS systems make attacking a blockchain more costly, since a successful attack would require an ownership of at least 51% of the total existing coins. Failed attacks would result in huge financial losses. Despite the upsides and convincing arguments in favor of PoS, such systems are still in the early stages and have yet to be tested on larger scales." (Source : https://academy.binance.com/fr/articles/delegated-proof-of-stake-explained)

13 "Based on the work of Fugger and inspired by the creation of Bitcoin, Ripple deployed the Ripple Consensus Ledger (RCL) in 2012 - along with its native cryptocurrency XRP. The RCL was later renamed to XRP Ledger (XRPL). [...] The network reaches consensus through the use of its own customized consensus algorithm – formerly known as the Ripple Protocol Consensus Algorithm (RPCA)." (Source : https://academy.binance.com/fr/articles/what-is-ripple)

1. The Federated Byzantine Agreement[14] (FBA) divides the network into several parts (slices). A node can be part of one or several slices, and can be programmed to trust a particular slice. This node then does not need the entire network to validate the block, which greatly increases the speed of transaction validation and reduces the resources used by the network.

2. As a reminder, in the Byzantine Agreement (BA), nodes validate a block once the majority of all nodes in the network have verified its validity and the transactions inside it. This consensus is robust but resource-intensive when there are already several thousand nodes on the network.

14 "A Federated Byzantine Agreement (FBA) is a form of Byzantine fault tolerance where each byzantine general is responsible for their own blockchain. A Federated Byzantine Agreement (FBA) is used for its high throughput, network scalability, and low transaction costs. Notable cryptocurrencies using the Federated Byzantine Agreement (FBA) include Ripple. FBA consensus mechanism was pioneered by Ripple. Federated Byzantine Agreements (FBA) require nodes to be known and verified ahead of time before users request any performance from the FBA. The nodes also choose who they trust, and eventually quorums of nodes emerge from decisions made by the individuals nodes making up the FBA network. A quorum is the minimum number of nodes required for a solution to be correct, and after a quorum forms the block is validated and included on the blockchain. The FBA uses 'quorum slices', which are subsets of quorums that can convince specific nodes operating on the network to agree with them." (Source: https://golden.com/wiki/Federated_Byzantine_Agreement_(FBA))

2.2 SMART CONTRACTS

Smart contracts are intimately linked to the blockchain. Indeed, one of the characteristics of the blockchain is its immutability, i.e. the permanence of the information recorded on it. It cannot be modified or erased. It is possible to use smart contracts with the certainty that they cannot be broken.

A smart contract helps to create SDIs. The SDI subject[15] creates a public/private set of keys, keeps the private key and then transfers the public key to the smart contract. Since the smart contract makes available this public key, references and information that the user chooses to share on a case by case basis, exchanges with third parties become possible. In addition to the creation and update of the SDI, this smart contract also acts as a directory so the SDI subject can manage its attributes.

It is a place where non-sensitive information is gathered, allowing the user to assemble their SDI Document (SDO[16]).

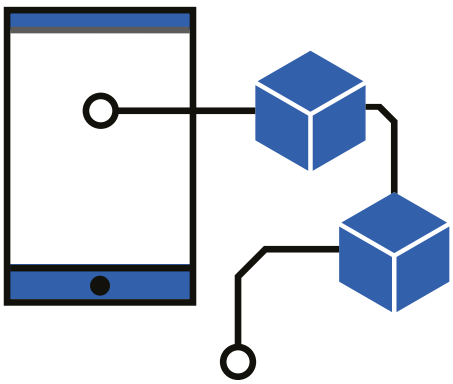
Finally, the smart contract can allow the delegation of the SDI control (for example, the implementation of a parental control).

Thus, this smart contract is an essential tool of the ecosystem, with multiple functions.

It can be consulted on our GitHub[17] .

Synthesis

XSL Labs has implemented its ecosystem on Binance Smart Chain, which is currently the network offering the best possible service, combining scalability, low network costs, reliability and cross-chain compatibility. Eventually, the advantages offered by Flare network will lead XSL Labs to transfer the SYL ecosystem to it. XSL Labs will use smart contract technology as part of its SDI development.



GitHub

XSL LABS

15 *Subject identified by an SDI.*

16 *See section 3.1.2 SDI technology.*

17 *To consult XSL Labs' Github : https://github.com/XSL-Labs*

03

SYL ecosystem

3. SYL ECOSYSTEM

3.1 SECURE DIGITAL IDENTITY (SDI)

3.1.1 INTRODUCTION

3.1.1.1 SDI and Self-sovereign identity (SSI)

The Secure Digital Identity (SDI) developed by XSL Labs is a Decentralized Identifier (DID) based on the 10 principles of Self-Sovereign Identity[18] defined by Christopher Allen. The aim of Self-Sovereign Identity, like the SDI, is to guarantee the users identity protection against cybercriminals and their independence from private or state entities that might be tempted to take advantage of their information or use it against them. The concept of Self-Sovereign Identity seeks to revolutionize interactions between Internet users, whether they are individuals or entities, by making interactions more secure and trustworthy.

1. Existence
The identity of individuals cannot be reduced to their digital identity; digital identity only makes accessible and public certain aspects of the full identity of individuals.

2. Control
The users must have control over their identity and the way their data is used. They are the absolute authority in this matter, and can decide to share it, to update it, to hide it.

3. Access
The users must have access to all of their data as well as the ability to modify them, without the intervention of any intermediary.

4. Transparency
The systems allowing the implementation of self-sovereign identity must be transparent both technically and in their-management. Algorithms must be open-source, free, and-must be available for review to understand their functioning.

5. Persistence
Identities must last as long as their authors wish, at least until they become obsolete due to technological evolution. Users must also be able to exercise their right to be forgotten.

6. Portability
The identity should not be held by a single third party, even if it is a trusted authority. A portable identity ensures that the user retains control of it, which promotes persistence.

7. Interoperability
The identity must be usable as widely as possible throughout the world, across different systems, without the author losing control of it

8. Consent
The user must give his consent to the use of his identity. Any sharing of data with anyone is subject to their express consent.

9. Minimalisation
The disclosure of data must be kept to an absolute minimum. Technical processes such as zero knowledge support this principle, and everything must be done to protect the user's privacy as much as possible.

10. Protection
User rights must be protected. If the needs of identity systems conflict with the rights of the user, the latter take precedence. Systems must also use independent algorithms, be able to withstand censorship, computer attacks, and be decentralized.

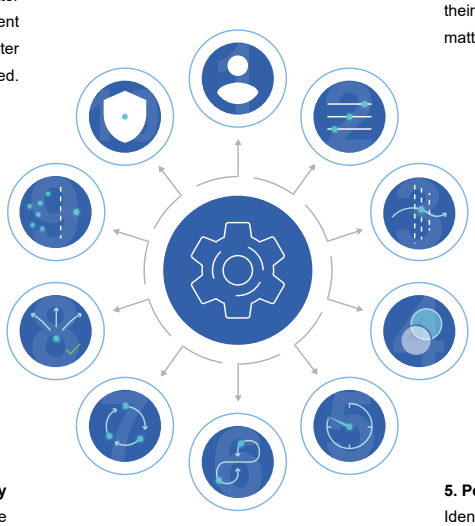


Figure : The 10 principles of SSI

The SDI technology, which relies on these principles, is a central component of XSL Labs' solution against data theft.

18 http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

3.1.1.2 How does SDI fight data theft ?

Data storage centralisation is one of the issues XSL Labs intends to address.

When cybercriminals hack into a centralized database, they have access to every users' data which they can steal and then sell or use for wrongful purposes.

This is the first problem that the SDI solves. According to the W3C[19], a decentralized identifier, or DID, is unique and persistent identifier that does not require a centralized registration authority "[because it makes] use of distributed ledger technology (DLT[20]) or some other form of decentralized network". The blockchain and decentralized servers that form the SDI technology basis enable decentralized storage of SDI users personal data. It is impossible to link identity data to a specific SDI user. Only the SDI subject can use the data, because it is the only person that has the required private key to present them.

This way, a cybercriminal who intends to steal the personal data of SDI users will have to hack each user's device one by one. This renders such practices ineffective and significantly less profitable, thus discouraging them.

The second problem that the SDI solves is the spread of personal data. With the SDI, identification and access to a website or a service may no longer require the sharing of personal data. The service could simply have access to the sequence of characters that constitute the SDI (See section 3.1.2 : SDI Technology) without ever being able to associate it with other information.

Also, sharing personal data with a service allows the user to choose which data is transmitted, so it is no longer necessary to share irrelevant data with them. Since services only have very limited access to the data, it cannot use it for commercial or political purposes.

It is also possible to access a service without disclosing any data at all. In such case, a verified document can be issued, based on certain data and attesting that the conditions for accessing the service have been met. This process is called Zero-Knowledge Proof.

19 The W3C (also World Wide Web Consortium) is the main international standards organization for the World Wide Web.
20 Distributed Ledger Technology.

Example : In order to register to a service that requires an age verification, the SDI confirms to the service that the requirement is met, without providing the date of birth.

Therefore, the SDI defines a new era in terms of user data security on the Internet.

In the long run, it will also significantly reduce the power of large companies such as Facebook or Google, whose solutions facilitate, at the cost of massive profiling, the connection to a large number of third-party services. In fact, such power gives them an excessive amount of control over their users' Internet activities, privacy and data. Moreover, their business model relies on their exploitation for profit or political purposes. Today, the right to privacy is not respected and everyone's digital life is partly controlled by GAFAM[21].

The SDI technology constitutes a very important example of decentralized counter-power to the Web giants. The SDI allows to keep the practicality of a unique identifier while guaranteeing data security and user's sovereignty over it.

The adoption of DIDs is bound to grow considerably in the years to come. XSL Labs' SDI can be used in the same way as any other existing DIDs. Eventually and when decentralized identifiers are widely used, it may no longer be possible to request access to a DID user's data without owning one, effectively eliminating the risk of identity fraud and data theft.

A complete overview of the SDI technology and its ecosystem is detailed in the following sections.

GAFAM : Google, Apple, Facebook, Amazon and Microsoft

Synthesis

Secure Digital Identity (SDI) is a decentralized identifier that relies on the principles of Self-Sovereign Identity. Its purpose is to guarantee the independence and sovereignty of users in the management of their data by using decentralized technologies, independent from centralized authorities and the power of governments or GAFAM. It helps fight both theft and spread of data by preventing their storage on centralized databases and by using Zero-Knowledge Proof (ZKP) methods.

21 An acronym for the Web giants.


SDI TECHNOLOGY

3.1.2 SDI TECHNOLOGY

Before being able to associate personal data verified by third parties with one's identity, an SDI must be created. This SDI is an identifier that refers to a single user and respects the following principles :

- It cannot be assigned (or reassigned) to anyone else
- It can operate without a central authority
- It is linked to one or more cryptographic keys to verify that its owner has exclusive control over it
- It allows the retrieval of a public document, the SDI Document, which references other elements such as one or more public keys or services

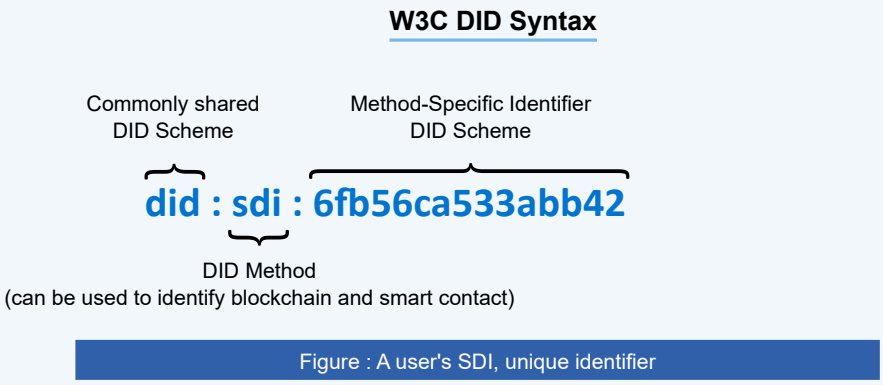


Figure : A user's SDI, unique identifier

3.1.2.1 SDI Document (SDO)

The SDI is an identifier associated with an “SDI Document” (called also SDO) available on a public blockchain.

3.1.2.2 An SDI Document refers to an SDI

The SDI Document is the essential public profile of the user. It is not intended to contain much information, and since it is available on a public blockchain, it should not contain identity information such as name and date of birth.

Section 3.1.2.4 describes the mechanisms through which new types of information can be added to the SDI Document. Ongoing standardization work will define the possible contents of such document, its syntax and structure.

3.1.2.3 History and innovation about the technology

In 2017, with the first public experiments on decentralized identities, the Decentralized Identity Foundation[22] (DIF) began listing the resolution methods for DIDs to form a "Universal Resolver[23]" that allows each service provider wishing to interact with a DID presented by a user to retrieve the associated Document DID.

This correspondence table is referenced in the first document of the W3C working group on DIDs[24].

The release of this DID document, finalized in 2019, was a major step forward as the World Wide Web Consortium (W3C) is the leading standards body for Internet technologies (such as with the creation of HTML, DOM, PNG, XML standards).

XSL Labs will soon join the Decentralized Identity Foundation (DIF) to have its own DID method listed in the official DID resolution table.

3.1.2.4 SDI Document content

As noted in the introduction to section 3.1.2, the SDI is always associated with an SDI Document. This document does not directly contain personal information, it essentially contains :

- sub-identifiers to localize information in the SDO (SDI Document)
- public keys
- information about services and public keys
- information about the SDO's creator and creation date/update
- signature

Definition

Public keys (and indirectly public crypto addresses) are mathematically linked to private keys which must remain in their owner's wallet, under its exclusive control. Private keys are used to sign data (documents, transactions and proofs) and public keys are used to verify the validity of these signatures.

22 For more information : https://identity.foundation

23 Available here : https://github.com/decentralized-identity/universal-resolver/

24 For more information : https://w3c.github.io/did-core/

In the following example, the SDI and the SDI Document are linked to an individual. However, the SDI can also be associated with a legal person, an object or an organization.

Here is an example of an SDI Document (in standard JSON/JSON-LD format) :

```
{
  "@context": "https://www.w3.org/ns/did/v1",
  "id": "did:sdi:aea42randn1awa3xzhjkbvc33",
  "controller": "did:sdi:aea42randn1awa3xzhjkbvc33",
  "authentication":
  [{
    "id": "did:sdi:aea42randn1awa3xzhjkbvc33#authkey",
    "type": "EcdsaSecp256k1KeyFID2021",
    "controller": "did:sdi:aea42randn1awa3xzhjkbvc33",
    "publicKeyBase58":
    "mM3wnZ3wXmC2AVvLNakc6zjZpfm3uJCwDMv6gVAnHqPV"
  }],
  "service":
  [{
    "id":"did:sdi:aea42randn1awa3xzhjkbvc33#webvc",
    "type": "VerifiableCredentialService",
    "serviceEndpoint": "https://example.com/vcheck"
  }],
  "created": "2021-01-01T14:22:21Z",
    "proof":
    {
      "type": "LinkedDataSignature2020",
      "created": "2021-01-01T14:21:14Z",
      "creator": "did:sdi:aea42randn1awa3xzhjkbvc33",
      "signatureValue": "NRB43Y42Q21...1tndsf45sw=="
    }
}
```

Figure : An SDI Document (SDO) referring to the SDI "did:sdi:aea42randn1awa3xzhjkbvc33"

As a reminder, this document is the resolution of the SDI "did:sdi:aea42randn1awa3xzhjkbvc33".

In order to find this document, several segments must be solved.

"did" indicates a decentralized identity protocol, just as "http" indicates a server/client communication protocol for browsing the World Wide Web.

"sdi" corresponds to the used DID method[25].

Once the method is found (example : the smart contract 0xb9c15…98e246504 on Binance Smart Chain), the identifier is used to find the SDI document. Here, the smart contract is requested with the identifier "aea42randn1awa3xzhjkbvc33" (this is a random identifier assigned when the SDI is created). Whether directly through a main smart contract or through individual smart contracts, the documentation of the DID method allows to obtain the SDI Document, which is called the SDI resolution.

The rudimentary content of the SDI Document in the figure above can be much more diverse and detailed. This example is an overview of this type of document in order to explain its different parts.

25 *Available here : DID Methods*

“@context”: “https://www.w3.org/ns/did/v1”

This line indicates that this is a document related to a decentralized identifier.

“id”: “did:sdi:aea42randn1awa3xzhjkbvc33”

The first "id" shows the SDI address that is resolved by the SDI Document. It is associated with this SDI Document.

“controller”: “did:sdi:aea42randn1awa3xzhjkbvc33”

This first “controller” specifies who controls this DID and therefore who can make changes to it. This example represents the simplest case, where the identity of the controller is the same as the identity which is described in the SDI Document.

This is not the only possibility. Many other cases are possible and can be useful in the following situations (non-exhaustive list) :

- A person uses several different wallets to control the same identity
- A person uses a single wallet to control several identities
- An adult manages certain parts of a child’s decentralized identity
- A person delegates certain rights over all or part of their identity to a trusted third party

```
“authentication”:
[{
    “id”: “did:sdi:aea42randn1awa3xzhjkbvc33#authkey”,
    “type”: “EcdsaSecp256k1KeyFID2021”,
    “controller”: “did:sdi:aea42randn1awa3xzhjkbvc33”,
    “publicKeyBase58”:
    “mM3wnZ3wXmC2AVvLNakc6zjZpfm3uJCwDMv6gVAnHqPV”
}]
```

This segment describes the default authentication method of the SDIs owner. An authentication public key is inserted.

“id” which ends with #authkey allows direct reference to this segment. Here, the SDI is “did:sdi:aea42randn1awa3xzhjkbvc33” but it is possible to directly show the key which serves as authentication.

An anchor allows to proceed and point directly to a specific segment. In this case : “did:sdi:aea42randn1awa3xzhjkbvc33#authkey”.

“type” gives the public key digital signature algorithm used for authentication. In this example, it is the DSA[26] using elliptic-curve cryptography[27].

“**controller**” refers to the SDI responsible for this segment. Once again, it is the simplest case since the reference is identical to the owner of the identity.

“**publicKeyBase58**” is followed by the value of the public key base 58 encoded.

26 Digital Algorithmic Signature : a standardized digital signature algorithm.
27 A set of cryptographic processes particularly suited to public key cryptography.

This segment can be used by an external web service to authenticate a new user using his SDI.

```
“service”:
[{
    “id”:”did:sdi:aea42randn1awa3xzhjkbvc33#webvc”,
    “type”: “VerifiableCredentialService”,
    “serviceEndpoint”: “https://example.com/vcheck”
}]
```

Verifiable Credentials are described in section 3.1.3. These Credentials are verifiable data available in the user wallet, it is sometimes useful, or even necessary to have them verified by a centralized online service. This configuration makes it easier to share a Verifiable Credential with an entity that is not part of the ecosystem.

In practice, this entity can verify a Verifiable Credential linked to this SDI by going to the indicated address (in this example, “https://example.com/vcheck”), then copy-pasting it or by directly checking the Verifiable Credential in the SDI Document.

```
“created”: “2021-01-01T14:22:21Z”,
  “proof”:
  {
    “type”: “LinkedDataSignature2020”,
    “created”: “2021-01-01T14:21:14Z”,
    “creator”: “did:sdi:admin42randn1awa3xzhjkbvc33”,
    “signatureValue”: “NRB43Y42Q21…1tndsf45sw==”
  }
```

At the end of the SDI Document, a digital signature can be found to authenticate the person who created it. The first timestamp refers to the document’s date of creation in the smart contract and is followed by details of the signature which serves as proof, often containing a slightly earlier date.

Again, the simplest case is shown in this example, where the creator is the owner of the identity. But this is not necessarily the most frequent case. Indeed, the creation of an SDI Document on a blockchain often requires the payment of data creation fees and the user is not necessarily the one who performs this transaction.

Example : when an SDI Document is created on a smart contract on Binance Smart Chain, a user that downloads a wallet to create and manage his decentralized identity, does not necessarily possess BNB (Binance coin) to pay the necessary gas fees when creating this SDI Document. The identity owner can therefore be in a situation where he knows how to provide all the details to create the content of his SDI Document, but needs an intermediary to help him put this document on the smart contract of the blockchain. This intermediary will pay the fees associated with the creation of the SDI Document on behalf of the user.

The author of the SDI Document can therefore be different from the user. However, even in this case :

The author's SDI can be used to find and verify the identity of the intermediary to ensure that it is indeed a trustworthy intermediary. Thus SDI can point to the SDI Document of a referenced administrator.

This does not necessarily mean that the author can modify the information in the SDI document, especially without the consent of the identity owner. The latter may indicate that they alone remain authorized to make future modifications to their SDI document or to share control with a third party.

3.1.2.5 Use case

A web service wishes to authenticate SDI owners through a dedicated web page. This is a common case of authentication on a website initially displayed in a desktop browser.

The server login page displays a QR Code that contains the web service address and a unique random character string (also called a "challenge").

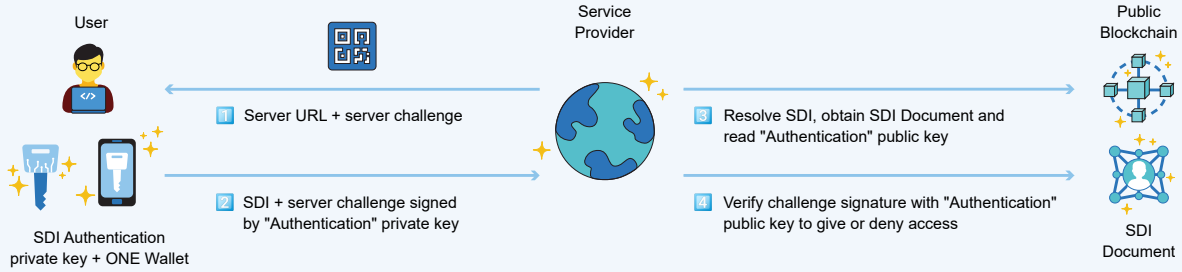


Figure : SDI owner authentication on a web server

The wallet user scans the QR Code found on the web page. The wallet asks the user if they agree to use a key linked to their SDI to authenticate on this server and then, after confirmation, uses the private authentication key to sign the challenge contained in the QR Code. The wallet then sends the signed challenge and the SDI (identifier) back to the server.

The web service receives the SDI (acting as “username”) and automatically follows the steps described above to obtain the associated SDI Document. The service reads the segment on authentication and finds the public key linked to the SDI that can be used for authentication by default. The server must now ensure that the SDI owner has the private key corresponding to this public key. Then, the server checks the validity of the signature it has just received. If the signature is valid, the server confirms the authentication and provides access to the service.

Using an SDI to do an authentication is a simple use case that is important to understand before moving on to the description of Verifiable Credentials.

Note

Within an SDI document, it is possible to assign several authentication keys to different web services and contexts, and also other keys to other uses such as message encryption and contract signature.

3.1.3 VERIFIABLE CREDENTIALS

In order to obtain verifiable personal information, it is necessary that a trusted issuer is previously identified and contacted. Trust in the Verifiable Credentials issuer must be established through verifiable information about their own identity and issuer qualification.

Following the example of Public Key Management Infrastructures (PKI), a chain of trust must be traced guaranteeing the reliability of the identity of all the actors in the chain, it then indirectly guarantees the reliability of the transmitted information.

In a case of a Verifiable Credential (VC) such as a family name, this information can be validated by an issuer qualified as a KYC service provider. This requires prior verification of the reliability of the issuer's identity through its own SDI.

At the top of the chain of trust, the first link is the highest verified identity, the root authority. In the context of queryable SDI, it generally consists of the smart contract administrator's SDI.

As a reminder, it is possible to interact with other DIDs and blockchains as long as the wallet or the tool that seeks to verify a VC can trace the chain of trust of the DIDs between different blockchains (interoperability principle).

It is also possible to not make it mandatory for the root authority to have an SDI, but instead to have at least one identity linked to a certificate issued either by a certification authority (as is the case for SSL/TLS[28]), or by government agencies.

Being able to choose between different root authorities makes it possible to increase the decentralization of the architecture. Nevertheless, it will be necessary for XSL Labs to work on supporting these different authorities so that the user can easily judge the reliability of the authorities' identities.

28 Protocols for securing exchanges over information networks.TLS is the successor to SSL.

The following case describes a simple chain of trust.

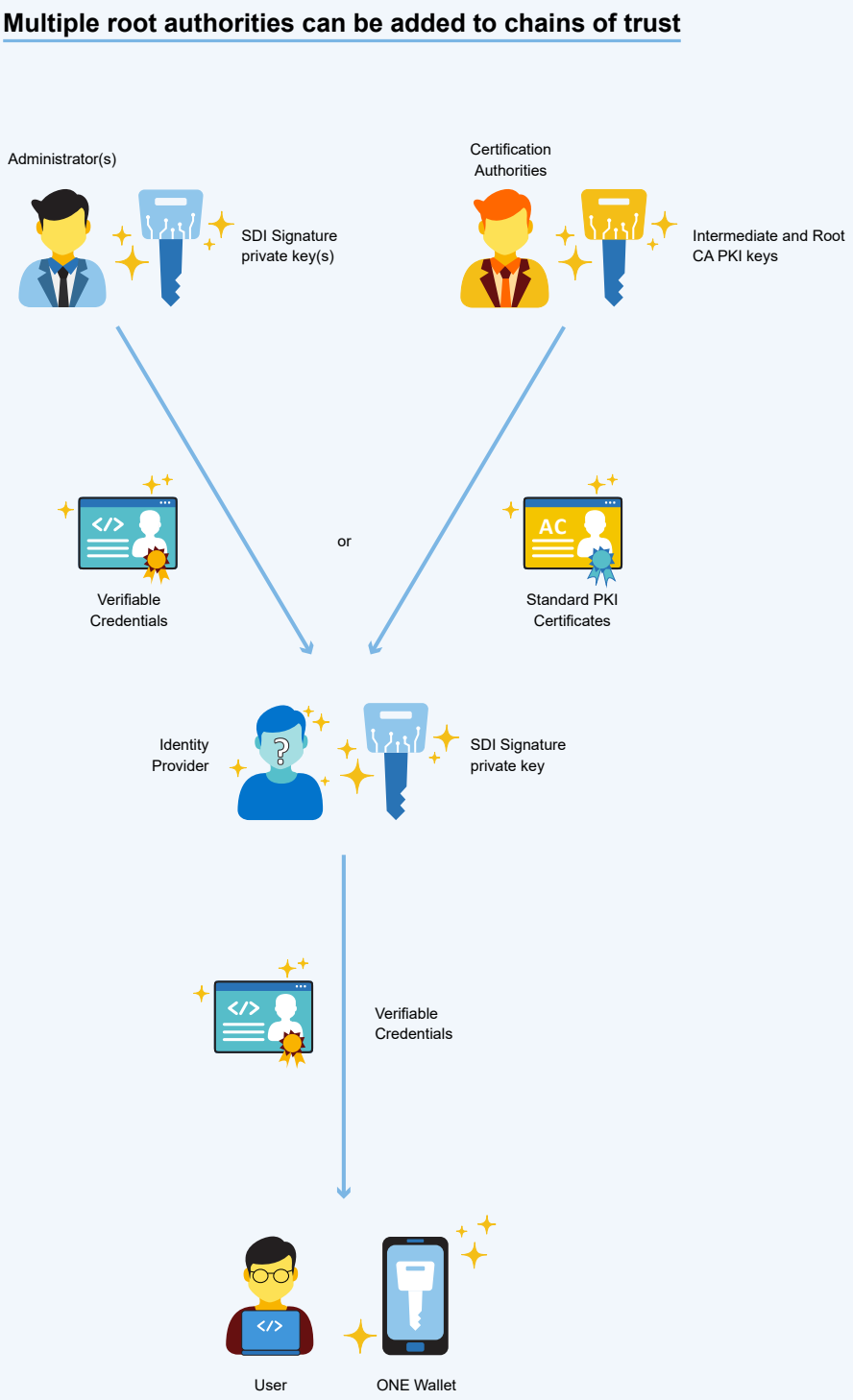


Figure : Verifying a VC also implies going up the chain of trust to check the identities involved

In order for the user to obtain a Verifiable Credential, it is necessary to request it from an identity provider (Verifiable Credential issuer) whose legitimacy has been previously verified.

As mentioned earlier, it is necessary to verify the VC issuer's legitimacy.
The diagram below details the steps of this verification procedure :

How to check if an "Identity Provider" is legit?

1. Check provider of SDI Document
2. Check provider of the public profile
3. Check provider of the Verifiable Credential's public trace
4. Check public Verifiable Credential (role)
5. Check if SDI Document's issuer is admin
6. Check Verifiable Credentia public signature

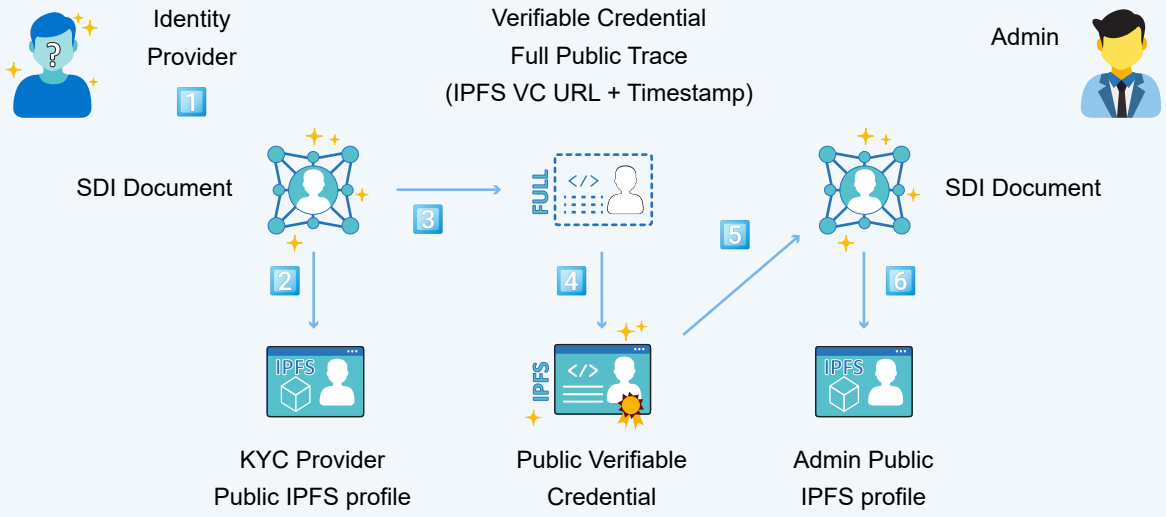
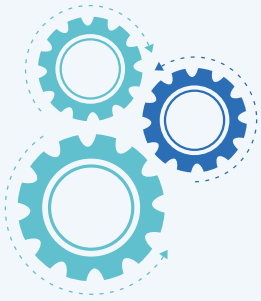


Figure : How to verify that an Identity Provider is trustworthy

The user can be directed to a VC issuer or decide on his own to go to a recognized provider. The notion of verifiable information that can be presented several times with the same reliability will lead to changes in user behavior and pathways.

It should be noted that the owner (user) that owns a verified identity can also issue a Verifiable Credential for another user.



3.1.3.1 SDI Document of a VC issuer

The figure below describes a simple use case of identity providers (public issuers of Verifiable Credentials with a clearly identified role, separated from standard users).

```
{
    “@context”:  “https://www.w3.org/ns/did/v1” ,
    “id”:  “did:sdi:0x4B20993Bc481177ec7E8f571ceCaE8A9e22C02db” ,
    “controller”:  “did:sdi:0x4B20993Bc481177ec7E8f571ceCaE8A9e22C02db” ,
    “authentication”:  [{
           “did:sdi:0x4B20993Bc481177ec7E8f571ceCaE8A9e22C02db#keyAuth-1” ,
           “type”:  “EcdsaSecp256r1Signature2019” ,
           “controller”:  “did:sdi:0x4B20993Bc481177ec7E8f571ceCaE8A9e22C02db” ,
           “publicKeyBase58”:
        “027560af3387d375e3342a6968179ef3c6d04f5d33b2b611cf326d4708badd7770”

    }] ,
    “assertionMethod” : [{
           “did:sdi:0x4B20993Bc481177ec7E8f571ceCaE8A9e22C02db#VC-Signature” ,
           “type”:  “EcdsaSecp256klSignature2019” ,
           “controller”:  “did:sdi:0x4B20993Bc481177ec7E8f571ceCaE8A9e22C02db” ,
           “ethereumAddress”:  “0x4B20993Bc481177ec7E8f571ceCaE8A9e22C02db”
    }] ,
    “service” : [{
           “id”: “did:sdi:0x4B20993Bc481177ec7E8f571ceCaE8A9e22C02db#Public_Profile” ,
           “type”:  “Public Profile” ,
           “serviceEndpoint” :
               “https://ipfs.infura.io/ipfs/QmNTMEmwUTG5mFhdRrsiAADPed1i4HccbhCcbdALAyyxLE”
    }]
}
```

Figure : SDI Document of a public issuer of Verifiable Credential

A notable difference is the availability of a public profile on IPFS:

```
{“type”: “Profile”,
“id”: “IPFS”,
“name”: “XSL Labs”,
“image”:
“https://ipfs.infura.io/ipfs/
QmXV2ZEMMom4Z9ciFzgNnpJ33oPipb3rzbWe4J5GBfFDSb”,
“url”: “https://www.xsl-labs.io/en/”,
“email”: “contact@xsl-labs.io”}
```

As a reminder, IPFS is a public decentralized storage space where files are referenced by their hash. Thus, the XML content of the above file comes from the IPFS file that can be easily found with an IPFS software, like the image referenced in this file. Web browsers are progressively integrating the ability to read these files on the network. For the moment, it is still preferable to use web gateway services.

Files stored on IPFS cannot be deleted voluntarily so it must be assumed that they can remain available for a long time and for everyone. It is therefore necessary to indicate only neutral and non-nominative information (example: website + generic contact email).

To verify the VC issuer's legitimacy, the user can (with the automatic help of its software portfolio) request the smart contract that manages its SDI. Then, the user obtains a list of Verifiable Credentials' traces that the issuer has previously received itself. Thus, the verifying software client can find the trace of a Verifiable Credential provided by the administrator to qualify its role as an identity provider (and VC provider) in the form of an IPFS reference (IPFS url) and a reliable timestamp information linked to the blockchain used. The IPFS reference retrieves the public content of the Verifiable Credential provided by the admin to this VC issuer. The client wallet can then verify the signature of this VC by the admin and conclude the legitimacy of the issuer.

3.1.3.2 Request and receive a Verifiable Credential

Once trust has been established with the VC issuer, it is possible to request Verifiable Credentials.

Below are the steps required to obtain a Verifiable Credential :

- The user completes the KYC procedure and uses his private key to sign a request for a VC.
- The issuer verifies the signature of this request (by consulting the user’s SDI Document).
- The issuer uses its own private key to sign a Verifiable Credential that corresponds to the information verified in the official documents.

This operation can be performed via a web interface or API if the issuer’s key is protected on a Hardware Security Module[29]. It can also be performed on a local machine with enhanced security provided by XSL Labs, which could include a mini software wallet in the form of a smart card reserved for identity providers. The primary goal of this all-in-one solution is to secure and simplify the life of VC issuers.

- The issuer creates an "on-chain" public trace of this Verifiable Credential by associating the hash[30] of this VC with a timestamp information.
- The issuer sends the Verifiable Credential to the user who requested it.

29 HSMs are physical devices that are supposed to be tamper-proof and use cryptographic functions. They can be PCI cards, rackmount external boxes, USB devices, and more.

30 A hash is a sequence of alphanumeric characters resulting from the application of a mathematical function to a set of data. It is a one-way operation.

How to obtain a Verifiable Credential from an issuer

(ex : Verifiable Credential of a nationality from an Identity Provider)

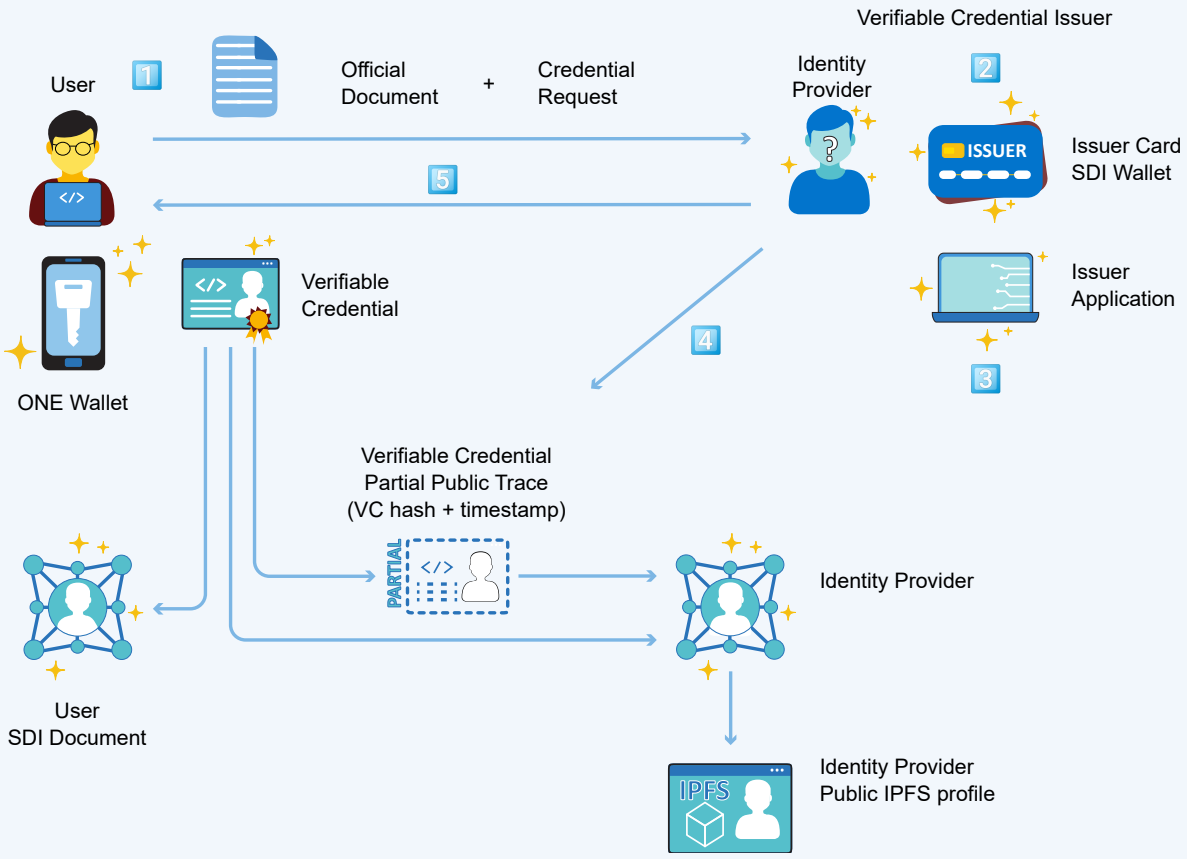


Figure : Steps to request and receive a Verifiable Credential

3.1.3.3 Verifiable Credential : creation, content and verification

A Verifiable Credential can be transmitted from its issuer to its receiver by email, face-to-face using a QR code, by file transfer, social network, API[31]. The identity wallet of the requester (first receiver) will interpret its content and perform the first total verification of this VC before importing it.

31 Application Programming Interface (API) : a set of functions and procedures allowing data communication between applications.

VERIFIABLE CREDENTIAL

Figure : Example of a Verifiable Credential given by a university to one of its members

The Verifiable Credential contains the following information:

- A header to indicate the nature of the file
- Metadata. In the figure above, they contain the issuer's SDI as well as a creation date. But they may contain other information such as expiration date, associated image, revocation mechanism
- Data involved in the initial request
- SDI of the receiver/owner
- Information previously verified by the issuer (in this case, the university's membership)
- Proof in the form of a signature with the issuer's private key dataset

The Verifiable Credential is sent to its owner, who can check it and present it on request.

Each new receiver will also be able to verify the VC themselves.

The verification consists of going back to the Verifiable Credential and checking :

- The owner's SDI
- The issuer's SDI
- The Verifiable Credential's signature

How to verify a Verifiable Credential

(ex : Member Credential from University)

1. User provides Verifiable Credential
2. Verifier checks user SDI Document
3. Verifier checks Issuer/Identity Provider SDI Document
4. Verifier checks if Issuer/Identity Provider is legit
5. Verifier checks Verifiable Credential's public trace (timestamp)

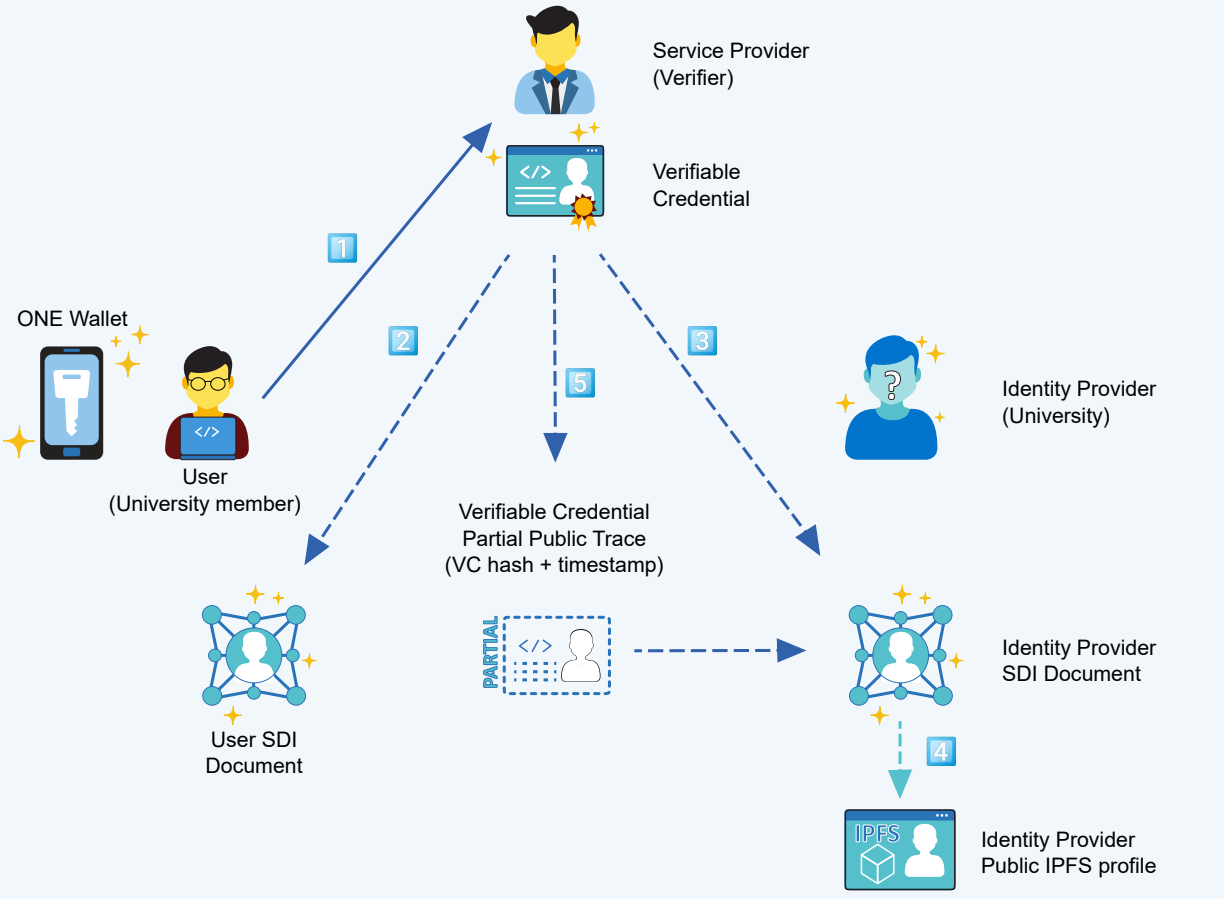


Figure : Steps to verify a Verifiable Credential

3.1.3.4 Verifiable Presentation : request, content and verification

The presentation of the Verifiable Credential is generally done through another file format, the "Verifiable Presentation". This file takes the Verifiable Credential and associates it with a signature linked to a challenge sent by the VC requester, to avoid any form of reuse.

How to request and obtain a Verifiable Credential from a VC owner

1. Requester provides a random challenge, a domain (which can be a website domain or any identifier giving context) with details about which credential is requested and a reason for the request.

2. Owner of the VC reads the domain, details and reason and is asked to sign the collected information: credential + domain/ context + requester's challenge. This content, once signed, becomes a Verifiable Presentation.

3. Requester checks VC owner SDI Document from blockchain, checks if signature is valid and checks if Verifiable Credential is genuine.

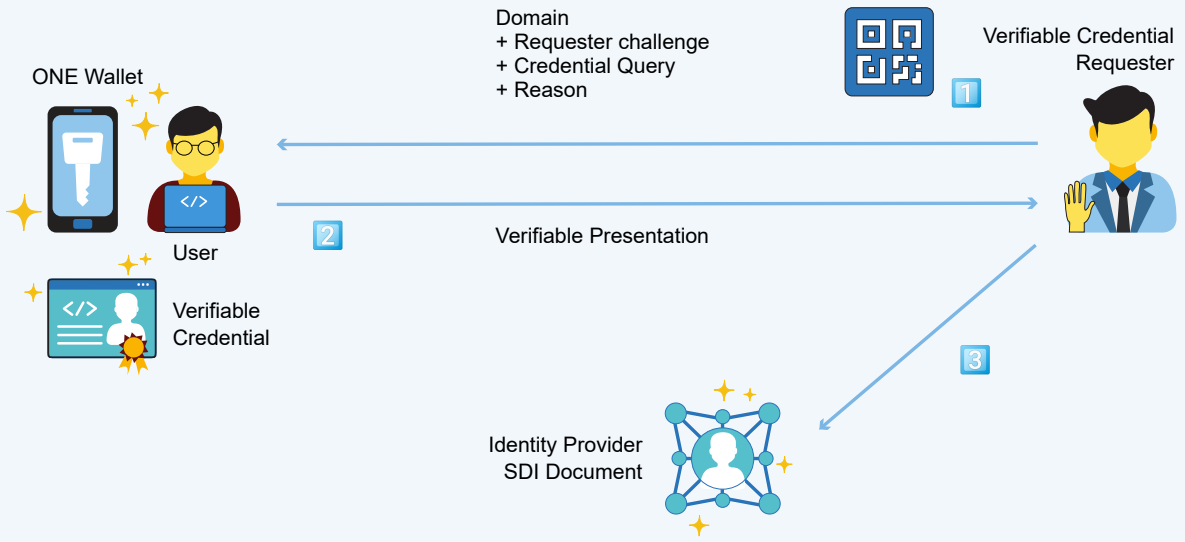


Figure : Request and acquisition of a Verifiable Presentation (signed Verifiable Credential)

Each Verifiable Presentation is unique and specific to the context of a given request and event. The request can be presented in the form of a QR code directly readable on the application ONE (see section 3.2).

VERIFIABLE PRESENTATION

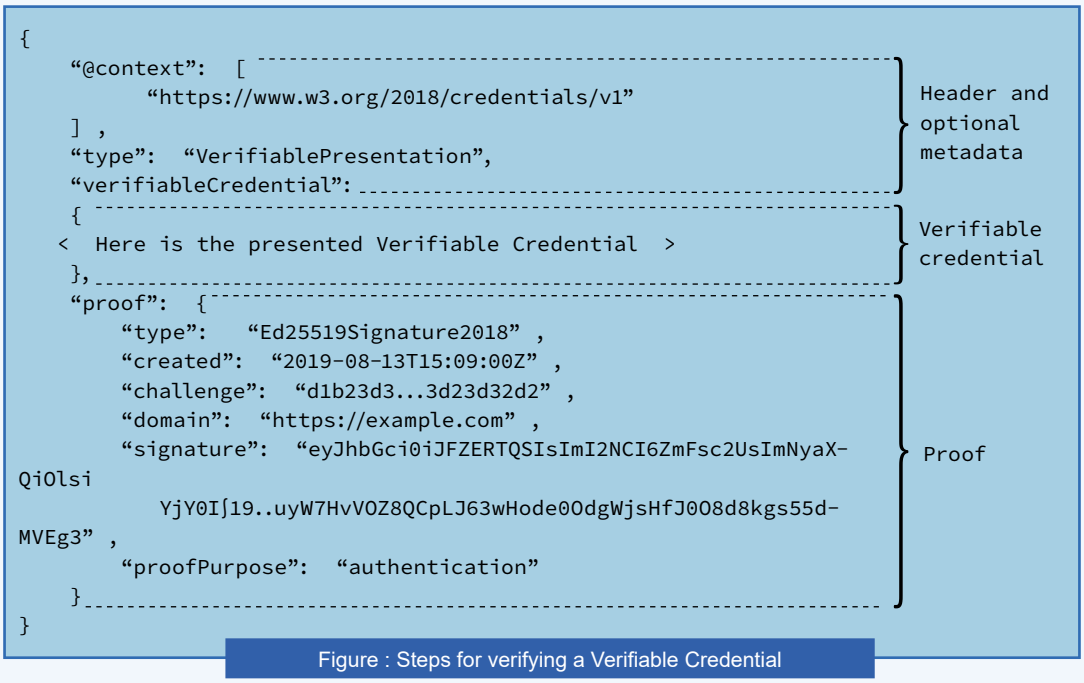


Figure : Steps for verifying a Verifiable Credential

Therefore, the Verifiable Credential and wallet owner is informed about the context before signing it, in order to create the Verifiable Presentation.

The Verifiable Presentation can be sent back to the requester via an address specified in the request details (or in “domain”) or visually with a QR code if the request was made face to face.

The requester or anyone else intercepting the Verifiable Presentation cannot reuse it in any other context.

The requester, who receives the Verifiable Presentation, can therefore verify that he is dealing with the right owner of the Verifiable Credential. The requester needs to verify the Verifiable Presentation's signature through the owner's SDI Document (before verifying the Verifiable Credential).

3.1.4 SDI LIFESPAN

The right to be forgotten is essential when it comes to digital identity data. The SDI user can consult the history of their portfolio use at any time to better exercise their right to be forgotten. It is possible for a user to publicly revoke an SDI (report it as deactivated). If the user manually destroys his private key, no one will be able to modify or access the contents of their identity wallet.

3.1.5 UNVERIFIED SDI

The SDI features a quick creation function. Any user can use this functionality. It can be activated at a service terminal, a payment point or even a control point.

This function will initiate the creation of an imperfect digital identity which its holder can then complete. The temporary digital identity can be reduced to a minimum of a single piece of information so its owner can take possession of it. In such case, an e-mail address may be sufficient.

An unverified SDI consists of :

- An identity element such as contact information (e-mail address or phone number)
- A function allowing the newly created identity to move to a higher level of verification, involving the use of KYC

The creation of an unverified SDI may be associated with a future incentive benefit offered to the customer or user. The final acquisition of this advantage or of the specific right that was granted will require the completion of the SDI, via a connection through the decentralized application ONE, or to a service of the official site that will be made available to users.

3.1.6 SDI INTEROPERABILITY

Interoperability and standards compliance (services and resolution methods) are important goals for the SDI. They are ensured through compliance with W3C (World Wide Web Consortium) standards and the work of the DIF (Decentralized Identity Foundation).

Synthesis

The SDI is a unique character string identifying a user or another resource. It is linked to a public SDI Document and available on a blockchain that contains functional information such as sub-identifiers, public keys. It also contains information about the creator of the document, its creation date, updates and a signature. It does not contain any kind of identity information.

Each SDI subject (a person or resource associated with an SDI) owns an identity wallet where its Verifiable Credentials are stored. These credentials are issued by third parties at the beginning of the chain of trust (institutions, companies, organizations or verified users) that contain information related to the identity of the SDI subject, as well as a signature that proves that it has not been modified and a timestamp certifying the issuance time. When the SDI subject wishes to prove an information to a third party, it issues a Verifiable Presentation which may contain information, about one or more Verifiable Credentials or the sole proof of validity of the information without distributing any other data (Zero-Knowledge Proof).

The SDI can be verified with a KYC (Know Your Customer) or can stay unverified for a quicker use. It will also be interoperable with all other decentralized identifiers (DID) and blockchains.

3.2 ONE

3.2.1 INTRODUCTION

3.2.1.1 Context

The following sections aim to define the outlines of the ecosystem built around the wallet ONE. This project is part of the work on decentralized identities which aims to use blockchain to prove the authenticity of personal data and provide a better framework for accessing this data.

3.2.1.2 Multi-identity wallet

Today, our digital life is made up of a multitude of personal data that are not easily verifiable and abusively requested each time a user account is created. Web services that request them don’t usually have any particular interest in getting this data. Until now, each Internet user had neither the tools to manage the dissemination of their identity data nor the means to contribute to track or fight against the collection of data.

Moreover, proving one's identity and attributes is a real challenge in a world that is moving ever more towards the digital age.

Digital identity management includes the management of :

1. User registration and attribute validation phase
2. User identification and authentication on the basis of his verified data
3. Verifiable Credentials reception, storage and presentation
4. Access to services and transactions on the basis of these Verifiable Credentials

Thus, the user is informed of the companies' identity and is demonstrating part of his information in order to access the services they offer. The consent to the presentation of information may be accompanied by a context or a usage agreement (temporary proof, storage duration, potential sharing).

Online service providers generally take on the role of identity provider. If not, they delegate this activity to third parties, mostly Web giants and social media.

Through various regulations, governments are trying to :

- Regulate the use of personal data to limit their misuse (GDPR[32]), often for customer profiling purposes
- Strengthen authentication security levels on the most sensitive online services (PSD2, eIDAS, TSP)

In terms of security, the best practices pushed by these regulators are based on the same cryptographic bases that are well known to crypto-assets enthusiasts: hash functions, data encryption, strong authentication, data and transaction signatures.

Generic cybersecurity and crypto-asset security are already being combined with, for example, the use of FIDO (strong authentication protocol developed by the Web giants and endorsed by regulators) on certain hardware wallets such as Ledger, Trezor and Bitbox or, the support of message encryption in the Metamask software wallet[33].

Conversely, some crypto wallets can now perform message signatures outside the usual framework of crypto-asset transactions and transfers.

Traditional centralized cybersecurity actors such as certification authorities can also benefit from this convergence.

3.2.1.3 One and XSL Labs ecosystem

ONE is a decentralized application that acts as the control tower of the SDI user's identity.

The decentralization of this app allows it to be independent of any third party authority by freeing itself from all intermediaries that could potentially exert control over users. This dApp, short for decentralized application, allows interoperability of all services that use SDI solution and it represents the gateway to the SYL ecosystem.
Each presentation of personal data made by the wallet owner is added to a local searchable history (including nature of data, recipient, context, date and time).

The dApp ONE also features a wallet to manage the user's SYL tokens and their issuance.

32 General Data Protection Regulation (EU) 2016/679.

33 Portfolio management extension, allowing easy access to decentralized applications from a web browser.

3.2.2 ONE : CHARACTERISTICS AND PILLARS

PRIMARY FEATURES OF ONE

- Creation of a user space
- Sending and receiving SYL tokens
- Receiving, storing and using Verifiable Credentials
- Complete history of the account's interactions
- Services related to the use of cryptographic keys listed in its SDI (strong authentication, electronic signature, data encryption)

THE 4 PILLARS OF ONE

- Protection of personal data

ONE uses the SDI solution in all services that will enable users to connect to it, in order to protect user data. It will also provide a direct access to SDI settings and a history of all interactions resulting from the user's activity.

- Scalability and adaptability

Through various decentralized applications available on the ecosystem, ONE can adapt to the needs of each user.

- ID wallet

The ID wallet will be used to receive and store Verifiable Credentials issued by trusted third parties and to issue Verifiable Presentations.

- SYL wallet

The SYL wallet integrated directly into ONE will make it possible to receive or send SYLs and to be able to access various services of the ecosystem independently.

3.2.3 KNOW YOUR CUSTOMER SERVICE

3.2.3.1 KYC & AML for financial institutions

One of the great strengths of ONE is the storage of Verifiable Credentials linked to KYC, Know Your Customer, which makes it possible to comply with AML, Anti-Money Laundering regulations.

This advantage of XSL Labs' solution aims to considerably reduce the costs in time and money for companies subject to these legal requirements.

The financial sector, represented by payment institutions, banks, traditional financing platforms and also new crypto providers, are subject to numerous rules (KYC and AML).

The fight against fraud, money laundering and terrorist financing is reflected in the need to repeatedly ask their users for a certain amount of information and proof of identity (when opening an account for example).

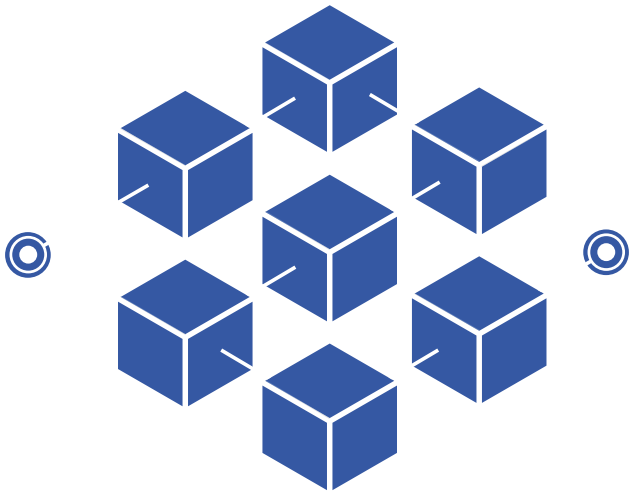
Each bank spends around 60 million dollars a year on KYC processes.

XSL Labs could save financial institutions a large part of this amount with the SDI and ONE application.

3.2.3.2 KYC Cost

The cost of KYC that requires access to a third party service may either be covered by the service providers or by the customer depending on the business plan of each service.

KYC is not a necessity by nature, but it may be a prerequisite for service provision, in which case the cost of KYC could be included in the purchase of a service. Once KYC is performed, it will be valid for all services requiring the same level of verification.



TECHNICAL DOCUMENT ONE

3.2.4 ONE TECHNOLOGY

Nowdays, the attributes of online accounts are often hosted by the service that created them. Therefore, the online Service Provider (SP) also acts as an Identity Provider (IDP) with its own authentication portal (Single Sign On).

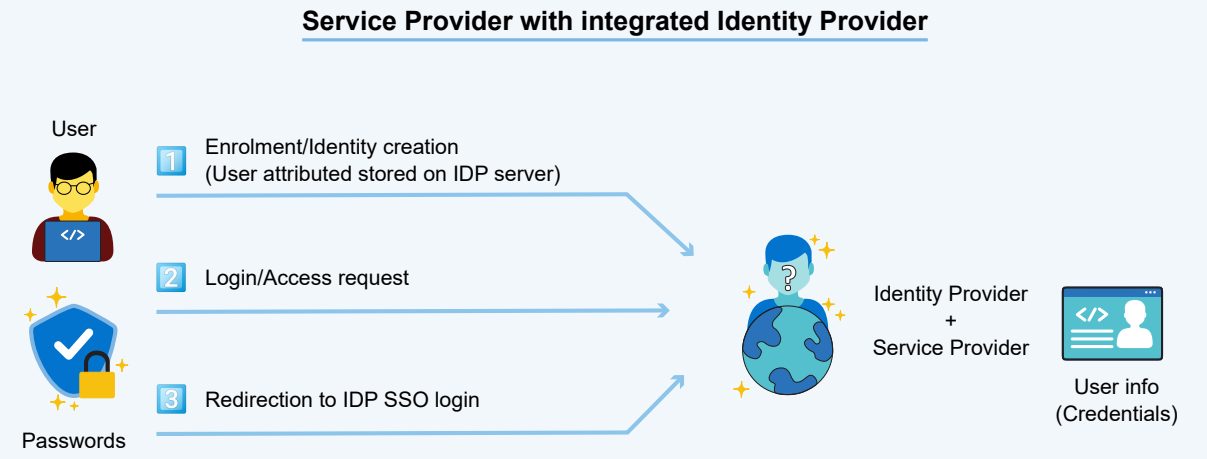


Figure : The Service Provider (SP) creates the user's account and its attributes

The roles of identity provider and service provider can be dissociated. This is the principle of account openings and information sharing through authentication on social networks gateways.

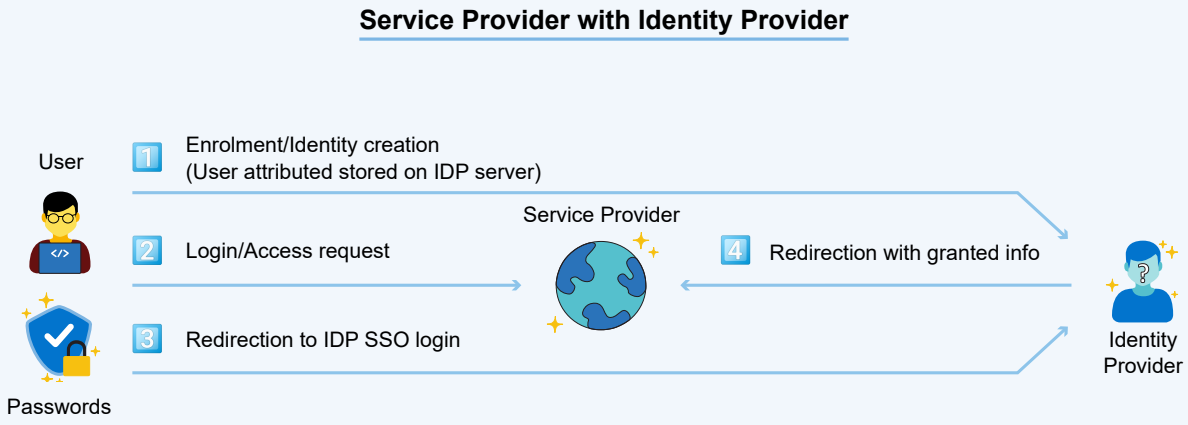


Figure : The Service Provider (SP) uses the attributes of an account that is created with an external Identity Provider (IDP)

3.2.4.1 Transition to decentralized architectures

In a decentralized architecture, digital assets are assigned in reference to a public address that depends on a private key kept by the user, in their wallet. The user only performs transaction signatures that are verified.

Wallet (locally generated keys) for crypto assets (blockchain)

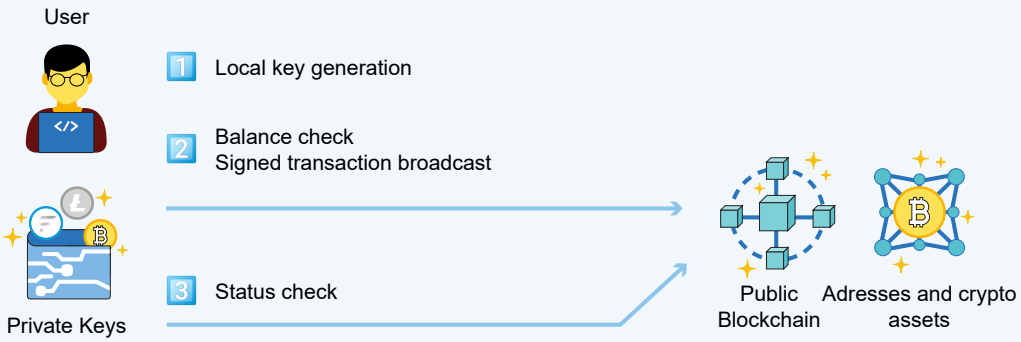


Figure : No personal information is kept outside the local wallet of the SYL holder

It is also possible to receive and control Verifiable Credentials with the wallet ONE.

Wallet ONE : SDI and crypto asset management

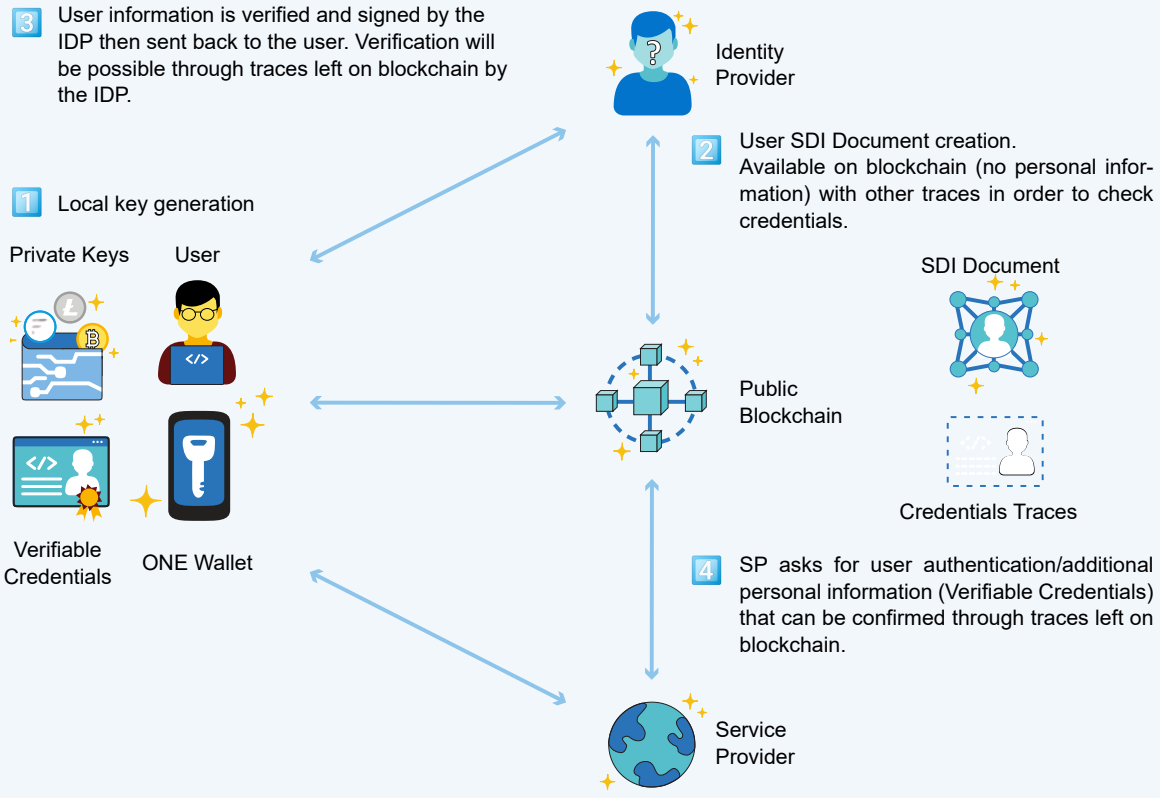


Figure : Wallet ONE is used to receive and control Verifiable Credentials

The wallet that controls the private key linked to the user's SDI must be able to manage the Verifiable Credentials it receives and must also :

- Demonstrate cryptographically to the Identity Provider (IDP) that it has control over its SDI
- Test the validity and verifiability of the Verifiable Credentials provided by the IDP
- Obtain files referenced in the Verifiable Credentials on centralized and decentralized storage spaces

- Store Verifiable Credentials
- Distribute Verifiable Credentials on the right communication channels
- Use other cryptographic keys specified for other uses (encryption, generic signature, signature for authentication)
- Manage some DIDs from other channels for the purpose of interoperability and scalability

This Wallet can benefit from significant progress made by Hierarchical Deterministic Wallets[34]. It also offers a simplified backup and restores procedures.

ONE HD Wallet (Key derivations from Seed)

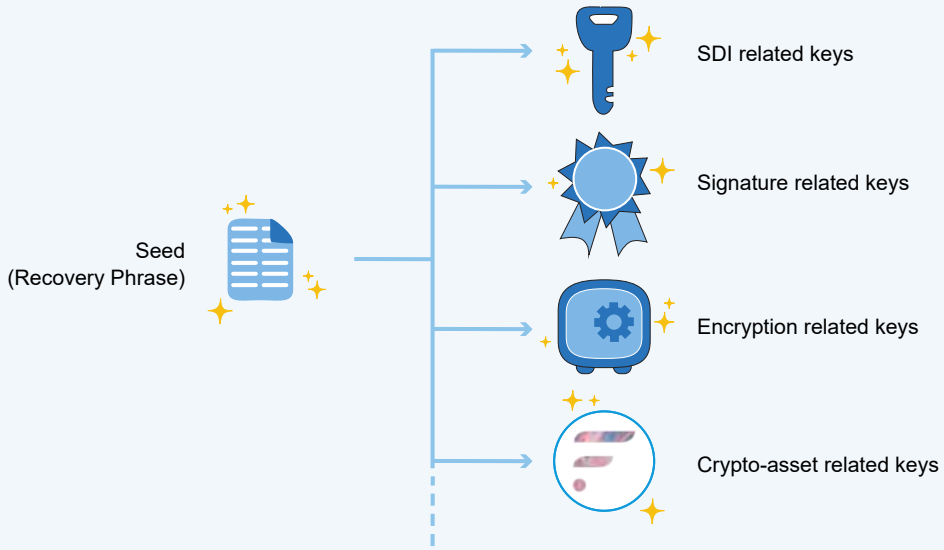


Figure : HD Wallet ONE manages all the private keys essential to all cryptographic uses

3.2.4.2 Web interfaces

Several optional web services can simplify the use of DIDs and Verifiable Credentials:

- A directory to list services for users, whether they are issuers, subjects or verifiers of Verifiable Credentials
- A verifier of Verifiable Credentials allowing the creation of challenges (QR codes scan) and the reception and verification of Verifiable Presentations
- A host for public Verifiable Credentials when necessary
- A wallet web version for users who need to manage a common identity that can be automated

Synthesis

ONE is the control tower of the SDI. This decentralized app enables the interoperability of the services in the SYL ecosystem. It will act as an identity wallet (DID wallet) by storing the user's Verifiable Credentials and allowing the delivery of Verifiable Presentations as well as the management of the utility token.
The ability to perform KYC through ONE will greatly facilitate the management of legal requirements for companies subject to them, while greatly reducing costs.

34 *"HD Wallet" enables the generation of many private keys from a single initial secret called seed.*

SYL DOCUMENT

4. SYL

4.1 CHARACTERISTICS

4.1.1 NETWORKS

Currently, the SYL is a BEP-20 token operating on Binance Smart Chain network.

4.1.2 ISSUANCE AND ESCROW

7 billion SYL, divisible to the 6th decimal place, have been put into circulation. The maximum amount of SYL in circulation will never exceed 10 billion.

3 billion SYL were placed in an escrow account by XSL Labs in April 2021.

This progressive release escrow account was created in order to release these 3 billion SYL through a smart contract that respects fixed rules. A maximum of 60,000,000 SYL per month can be released and this process can be repeated until the total 10 billion SYL are in circulation.

For the sake of total transparency, the escrow account as well as its immutable operating rules are available for consultation by the public.

4.2 LEGAL OPINION & TOKEN CLASSIFICATION

For now, three Legal Opinions have been formulated, in Japan, Singapore and Saint Vincent and the Grenadines, all three recognize the SYL as a utility token.

4.3 AUDIT

SYL Smart Contract was audited by the firm Beosin, and its report is available on xsl-labs.org

4.4 SYL PURPOSE

4.4.1 ISSUING VERIFIABLE CREDENTIALS

The SYL token is involved in the payment of certain services, such as the issuance of certain Verifiable Credentials and the payment of certain apps.

In order to reward the use of SDIs and Verifiable Credentials, an amount in SYL can be distributed to the users at the time of the creation of the first SDIs, to the issuers of the first Verifiable Credentials, and even to some verifiers.

Indeed, as explained above, once the SDI of each user is created, they need to obtain Verifiable Credentials that are provided by trusted issuers. These credentials certify certain information about the user's identity. It can be a KYC (Know Your Customer), a diploma or certificate issued by an employer.

Users will also be able to exchange Verifiable Credentials by becoming issuers themselves, thus creating a peer-to-peer network of trust.

4.4.2 APP LIBRARY

When third-party applications use the XSL Labs ecosystem, a library can be set up with the possibility of purchasing these applications or services with SYL.

4.4.3 PAYMENT GATEWAY

A payment gateway will be implemented in ONE to simplify and standardize exchanges within the application.

The standardization of the payment method among all users allows for the acquisition of Verifiable Credentials regardless of the users and issuers' local currencies.

This method simplifies the acquisition of Verifiable Credentials for the user. It allows the user to pay trusted issuers of commercial Verifiable Credentials or other fee-based services through a single wallet while maintaining traceability of transactions.

4.4.4 CORTEX

SYL will be particularly useful in the launch of the Cortex project, which aims to revolutionize advertising targeting by strongly implying the consent of their owner and the preservation of personal data. Advertisers will be able to target users who have consented to be targeted, without them sharing their personal data. A portion of the advertising revenue will also be shared directly with users via an incentive-based SYL reward.

In addition to the obtained Verifiable Credentials, the user will also be able to add additional personal information.

Cortex litepaper will be released in 2022.

Synthesis

SYL is the utility token of the SYL ecosystem. It is a BEP-20 token running on Binance Smart Chain. It will be used to issue Verifiable Credentials, to access services inside the SYL ecosystem, and as a payment gateway to simplify and standardize exchanges within an ecosystem that many countries will be able to use, in various currencies.

5. USE CASES

The following sections describe possible use cases for the SDI without being exhaustive.

5.1 VISION SDI

XSL Labs has partnered with Swiss Biometrix[35] to develop a terminal called ThermoVSN that will integrate the SDI technology in a new network called Vision SDI in order to secure their users' biometric data.

The SDI guarantees the anonymity and the security of personal and biometric data, thus ensuring full compliance with GDPR standards regarding the processing and storage of these data.

5.2 VIDEO GAMES

The use of SDI in the video game industry will profoundly change the video game ecosystem. XSL Labs will launch a first phase of experimentation with the use of its decentralized identifier. Multiplayer video games face a lot of problems related to the use of cheating software[36].

Using such third-party programs is prohibited, and most often results in bans for players who use them. There is a problem, however, because while banning a cheater's account makes that account permanently inaccessible, there is no guarantee that a cheater will not return to the game with another account. Thus, any punishment can be circumvented, and the persistent cheater can freely come back to ruin the experience of other players. The SDI will be able to be combined with a unique anonymous ID to alleviate this problem while incorporating various features that will pave the way for a new user experience.

The unique identification of each user will be possible after a KYC procedure and will make both player sanctions and rewards effective.

Also, Verifiable Credentials containing a history of players will allow recruiters or other players to have knowledge of each player's positive and negative history.

Verifiable Credentials can also be used to certify players' experience in different games, thus facilitating recruitment to teams and guilds.

Based on these Verifiable Credentials, it will also be possible to organize teams according to the level of the players or to grant connection authorizations according to their age, experience or level.

35 For your information: https://swissbiometrix.com/

36 It includes functions such as "aimbot", "triggerbot", "wallhack" and "ESP" functions. They are common functions in first-person shooter (FPS) video games. Such programs analyze data that the player receives so he can trace his opponents (wallhack, ESP), facilitate aiming (aimbot), or even make it automatic (triggerbot), leaving no chance for a regular player.

5.3 ANTI-FRAUD TICKETING

In order to fight against frauds and resale on the black market, it will be possible for ticketing sites to request an SDI from customers to ensure that the person who made the purchase is indeed the same person that is attending the concert.

5.4 DATING APPS

The SDI can play a key role in order to strengthen security on dating sites and applications. Issuing a KYC in the form of a Verifiable Credential on the SDI user's ID Wallet will give the assurance that the person registered on the dating site or application is who they claim to be.

Synthesis

The SDI is destined to be used by many third-party applications and services, in particular the Cortex project, which aims to revolutionize the way personal data is shared, biometric access control and the video game industry. Other use cases will evolve over time, promoting the adoption of the ecosystem.

6. MEDIAS

The following list, which is non-exhaustive, contains links about media introducing XSL Labs projects.

2021.03.10 - Article written in French from CoinTribune
https://www.cointribune.com/blockchain/ecosysteme/xsl-labs-syl-va-utiliser-la-smart-chain-de-binance-bnb

2021.03.08 - Article from U.Today
https://u.today/how-xsl-labs-builds-go-to-ecosystem-for-decentralized-identity-management?amp

2021.02.26 - Article from CoinTelegraph (different languages available)
https://cointelegraphcn.com/news/the-internet-of-trust-why-secure-digital-identities-are-crucial-to-web-30

2021.02.17 - Article from Tron Weekly
https://www.tronweekly.com/here-how-xsl-labs-revolutionize-digitalidentity

2021.02.15 - Article from AMB Crypto
https://ambcrypto.com/decentralised-identity-project-in-the-works-at-xsl-labs/

2021.02.11 - Article from Coin Speaker
https://www.coinspeaker.com/xsl-labs-data-identity-security/

2021.01.15 - Article from Le Point, in French, announcing our partnership with Swiss Biometrix
https://partenaires.lepoint.fr/block-chain/partenariat-thermo-vsn-xsl-labs-lutilisation-de-la-blockchain-dans-les-bornes-dacces-biometriques

2021.01.30 - Article written in French from CoinTribune
https://www.cointribune.com/tribunes/adopte-un-projet-crypto/xsl-labs-mieux-comprendre-le-projet-qui-reinvente-le-concept-didentite-decentralisee/

ROAD MAP

7. ROAD MAP

JULY 2021

- Public alpha testnet of SDI smart contract on BSC
- Private alpha of ONE wallet app
- Private alpha of KYC VC issuer
- Private alpha of enrolment web services and authentication via VC KYC

SEPTEMBER 2021

- Private alpha and demonstrator of e-sport services (gaming e-reputation)
- Private alpha of the online verifier (VP with challenge)
- Verifier's private alpha and online hosting (VP without challenge)

NOVEMBER 2021

- Private alpha of services for biometric access control (Facial recognition demonstrator)
- Private alpha of separate VP verification app
- Public beta testnet of SDI smart contract
- ONE's private beta
- Private beta of the online verifier (VP with challenge)
- Private beta and online hosting (VP without challenge)
- Private Beta of VC KYC issuer
- Open source codes for e-sport tools
- Opening of enrolment web services code and authentication via VC KYC

JANUARY 2022

- SDI smart contract on BSC and Flare Network (mainnets)
- Alpha version of Web + HSM service centralizing management tools on issuer's side
- Rewards alpha service for using Verifiable Credentials
- SDK Beta for integration into third party applications
- Audits and stress tests

FEBRUARY 2022

• Version 1.0 of KYC VC Issuer with rewards (KYC SYL Airdrop)
• Rewards beta service for using Verifiable Credentials
• Public version 1.0 of ONE
• Public version 1.0 of online verifier (VP with challenge)
• Public version 1.0 and online hosting (VP without challenge)

SECOND TRIMESTER 2022

• Commercial public services of Verifiable Credentials issuers including KYC
• Beta version of Web + HSM service centralizing management tools on issuer's side
• Public SDK for integration into third-party applications
• Opening of authentication integration source codes for CMS/SSO

THIRD TRIMESTER 2022

• Version 1.0 of Web service + HSM service centralizing management tools on issuer's side

More coming

8. CONCLUSION

Data theft is one of the major challenges our society is facing. Its cost to companies and consequently to the global economy is enormous, and it significantly hinders entire sectors of economic activity.

XSL Labs' solutions make it possible to effectively tackle these problems. Based on the 10 principles of Self-Sovereign Identity, XSL Labs' decentralised identifier, the SDI, enables users to maintain control over their identity and their data.

Solutions built around XSL Labs' decentralized architecture will help reduce the need to store personal data on centralized servers, while reinforcing the reliability of the presented information and the authentication of its owners.

The decentralized app ONE, which enables the control of the SDI, will also simplify KYC (Know Your Customer) and AML (Anti-Money Laundering) procedures.

Cortex advertising services will benefit advertisers and users, allowing them to target Internet users in a more ethical manner that respects their privacy and personal data, while rewarding them in SYL.

With these new tools, XSL Labs is committed to build an open and collaborative Internet of Trust for the future.

XSL LABS

Contact

First Floor, First St. Vincent Bank Ltd Building, P. O
Box 1574, James Street, Kingstown,
St. Vincent & the Grenadines
Entity Registration Number : 678 LLC 2020