Mise à jour · 2022

White paper

XSL LABS

L'identité numérique infalsifiable et décentralisée

XSL LABS

XSL Labs s’engage à déployer un moyen d'identification qui permettra à l’identité numérique d’être vérifiable et décentralisée. Au travers d’un écosystème proposant des services alternatifs et grâce à son interopérabilité, le Secure Digital Identity s’intègrera parfaitement à toutes les solutions d’un Web 3.0 toujours plus connecté.

TABLE DES MATIÈRES

TABLE DES MATIÈRES

01

Introduction

1. INTRODUCTION

Depuis une dizaine d'années désormais, notre rapport à Internet s'est transformé au point que la quasi-totalité des données de notre identité et de notre vie, qu'elles soient des données d'état civil ou des informations sur nos goûts, nos habitudes ou notre environnement social sont disponibles et stockées dans des bases de données centralisées. De plus, les institutions et les entreprises stockent également les données de leurs clients dans leurs systèmes centralisés mais les failles présentes dans ceux-ci permettent aux cybercriminels de dérober les données de tous ceux qui s'y trouvent puis de les revendre sur le Dark Web ou de faire chanter les institutions et les entreprises pour qu'elles puissent les récupérer.

Des chiffres confirment cette spectaculaire augmentation au cours de la décennie passée et laissent présager d'une augmentation encore bien plus grande à venir. L'étude Cybersecurity Ventures prévoit que les coûts mondiaux de la cybercriminalité augmenteront de 15 % par an au cours des quatres prochaines années, pour atteindre 10 500 milliards de dollars par an d'ici 2025, contre 3 000 milliards de dollars en 2015. Cela représente le plus grand transfert de richesse économique de l'histoire. En plus de menacer l'innovation et l'investissement, ces coûts sont exponentiellement plus important que les dommages financiers infligés par les catastrophes naturelles en un an et sera plus rentable que le commerce mondial de toutes les principales drogues illégales combinées. Si toute la richesse dérobée par la cybercriminalité en un an était comptabilisée comme le PIB d'un pays, celui-ci serait le 4ème pays le plus riche du monde[1], devant le Japon.

Au-delà de ces chiffres qui montrent l'importance de ce coût pour l'économie mondiale, le vol de données engendré par la cybercriminalité affecte en premier lieu les entreprises elles-mêmes qui subissent également des pertes considérables aussi bien en argent qu'en temps. Au niveau mondial en 2020, un vol de données inflige aux entreprises des pertes à hauteur de 3,86 millions de dollars en moyenne. L'étude montre également un lien entre le coût d'un vol de données et le temps de détection et de réponse aux intrusions. Pour la détection, les entreprises mettent en moyenne 280 jours à identifier et confiner la menace. Le coût d'un vol de données par client est estimé quant à lui à 150 dollars en moyenne[2].

Forts de ce constat, Georges Tresignies et Ludovic Ryckelynck ont développé leur réflexion autour des solutions technologiques qui pouvaient permettre de lutter contre ce fléau pour l'économie mondiale, les institutions, les entreprises et les utilisateurs. Ils ont alors constitué sous le nom de XSL Labs une équipe qui s'est donnée pour ambition d'élaborer cette solution en se basant notamment sur les technologies décentralisées de la blockchain et les récents travaux menées par le consortium W3C sur les identités décentralisées (DID[3]). Aujourd'hui, l'équipe de développeurs de XSL Labs est dirigée par Frédéric Martin et Imad El Aouny, experts en cybersécurité spécialisés dans les solutions blockchain, les contrats intelligents et les identifiants décentralisés (DID).

XSL Labs développe depuis mars 2020 un identifiant décentralisé appelé Secure Digital Identity (SDI) ainsi que ONE, l'application décentralisée (dApp[4]) qui permet la gestion de ce SDI. L'objectif final de la société est de lutter contre le coût croissant du vol de données pour les institutions et les entreprises en décentralisant le stockage des données d'identité des utilisateurs du SDI et en rendant à ceux-ci une souveraineté totale sur leurs données. Il s'agit également d'alimenter un écosystème riche et varié de dApps autour de l'utilisation du SDI. L'ensemble du système sera irrigué et fonctionnera grâce au token utilitaire de l'écosystème, le SYL.

XSL Labs entend ainsi révolutionner la lutte contre le vol de données sur l'Internet actuel ainsi que sur le Web 3.0[5] à venir.

1 Cybercrime Magazine

2 Rapport IBM 2020 : coût d'une violation de la confidentialité des données

3 Decentralized Identifiers (DIDs) W3C

4 Une application décentralisée (dApp) est un programme informatique qui s'exécute sur un système décentralisé ou distribué.

5 Le Web 3.0 est la troisième génération des services Internet pour les sites Web et les applications. L'objectif est de s'appuyer sur le machine learning, pour proposer un Web sémantique piloté par les données, dans le but ultime de créer des sites plus intelligents, connectés et ouverts.

02

Technologies externes utilisées

2. TECHNOLOGIES EXTERNES UTILISÉES

Cette section a pour vocation de présenter les technologies externes sur lesquelles s'appuiera l'écosystème SYL.

La section 2.1 présente les réseaux sur lesquels XSL Labs a développé et continuera de développer à l'avenir la solution technologique présentée dans ce White Paper, à savoir la Binance Smart Chain.

La section 2.2 présente la technologie des contrats intelligents (smart contracts).

La section 3 présente la technologie développée par XSL Labs : l'écosystème SYL.

2.1 RÉSEAUX ET BLOCKCHAINS

2.1.1 BINANCE SMART CHAIN

XSL Labs a déployé son écosystème sur le réseau Binance Smart Chain (BSC) après avoir étudié toutes les options technologiques actuelles capables de fournir le meilleur service possible à ses utilisateurs.

La Binance Smart Chain émet un nouveau bloc toutes les 3 secondes grâce à un algorithme de consensus de type preuve d'enjeu[6]. Plus exactement, elle utilise un algorithme appelé Proof of Staked Authority (PoSA[7]) qui permet aux participants de stacker leurs BNB pour devenir validateurs. S'ils proposent un bloc valide, ils reçoivent les frais des transactions incluses dans ce bloc.

Le réseau permet de réaliser des transactions avec des frais 100 fois inférieurs et de façon au moins 10 fois plus rapide que le réseau Ethereum. Sa compatibilité avec les outils Ethereum et notamment sa machine virtuelle (EVM[8]) permettent également l'étoffement du réseau à toutes les dApps du réseau Ethereum et la migration de toutes celles-ci sur la BSC.

L'ensemble de ces avantages a conduit XSL Labs à privilégier dans un premier temps la Binance Smart Chain pour le contrat intelligent du token SYL et le premier contrat intelligent du SDI.

6 La preuve d'enjeu (Proof of Stake) est une méthode de validation de nouveaux blocs par consensus distribué.

7 "La Binance Smart Chain utilise une méthode de consensus appelée Proof of Staked Authority (PoSA). Il s'agit d'une méthode de consensus hybride regroupant la Proof of Authority (PoA) et la Delegated Proof of Stake (DPoS). Ce modèle de consensus permet de générer rapidement des blocs [à] des frais faibles, tout en n'ayant besoin que de 21 validateurs pour fonctionner.
Les validateurs produisent des blocs à tour de rôle. Ils se chargent de faire tourner le réseau BSC en traitant toutes les transactions et en signant les blocs. En échange de leurs services, ils reçoivent des tokens BNB à titre de récompense. Dans le même temps, ils doivent aussi être réélus chaque jour via le vote des utilisateurs stakant leurs BNB pour continuer à faire partie du groupe des 21 validateurs. Un validateur doit faire tourner un nœud hardware répondant aux spécificités techniques définies, faire fonctionner un nœud BSC complet, et staker un minimum de 10 000 BNB. Ces prérequis permettent seulement de devenir candidat au rôle de validateur. Pour commencer à réellement valider des blocs, un candidat validateur doit devenir validateur élu. Les validateurs élus sont les 21 meilleurs candidats validateurs, soit ceux ayant la plus grande part des votes. Ils changent toutes les 24 heures via un processus d'élection continu, qui peut être observé au moyen de la liste des meilleurs validateurs de Binance.org". (Source : https://academy.binance.com/fr/articles/a-quick-guide-to-bnb-staking-on-binance-smart-chain-bsc)

8 L'Ethereum Virtual Machine (EVM) est un système sous-couche de la plateforme Ethereum, c'est elle qui permet les calculs liés à la mise en place et l'exécution de contrats intelligents sur la blockchain.

2.1.2 AUTRES CHAINES

[Mise à jour 2022] XSL Labs évalue le support d'autres blockchains pour le déploiement de contrats intelligents (voir section 2.2 : Contrats Intelligents) ou le support de certains DIDs.

- Flare Network: Flare[10] est un nouveau projet qui supporte aussi l'EVM (et par conséquent les contrats intelligents écrits en Solidity[9]). Cet ecosystème n'est pas encore mature et n'a pas encore réussi à attirer une véritable communauté de développeurs. Nous reviendrons sur l'évaluation de cette technologie plus tard l'année prochaine.

- Polygon: Polygon[11] (MATIC) est une solution de second niveau basée sur Ethereum (compatible EVM) avec une large communauté de développeurs et d'utilisateurs. Le sous-projet PolygonID[12] supporte nativement des preuves ZKP pour l'identité décentralisée. Nous poursuivons l'évaluation de cette opportunité.

- Bitcoin: Même si Bitcoin ne supporte évidemment pas la machine virtuelle EVM et les contrats en Solidity, Bitcoin peut toujours supporter la création de DID publics d'émetteurs/d'entreprises ou de DID privés d'utilisateurs à travers la méthode BTCR[13] DID que nous évaluons pour certains cas d'utilisation.

9 Solidity est le langage privilégié par les développeurs de contrats intelligents pour l'EVM.

10 Site web officiel : https://flare.network

11 Site web officiel : https://www.polygon.com

12 Site web officiel : https://polygon.technology/polygon-id

13 Documentation officielle : https://w3c-ccg.github.io/didm-btcr/

2.2 CONTRATS INTELLIGENTS

Les contrats intelligents (smart contracts) sont intimement liés à la blockchain. En effet, l'une des caractéristiques de la blockchain consiste en son immuabilité, c'est-à-dire la permanence des informations qui y sont inscrites. Elles ne peuvent pas être modifiées ni effacées. On peut ainsi déployer des contrats intelligents en étant certain qu'ils ne pourront pas être rompus.

C'est un contrat intelligent qui permet à XSL Labs la création des SDI. Le sujet SDI[15] crée une paire de clés publique/privée. Il conserve la clé privée puis transfère la clé publique au contrat intelligent. C'est grâce à celui-ci que des échanges avec des tiers deviennent possibles, puisqu'il permet de mettre à disposition cette clé publique, des références et informations que l'utilisateur choisit de partager au cas par cas. Ce contrat intelligent, outre la création de SDI et la mise à jour de celui-ci, agit aussi comme annuaire permettant au sujet SDI de gérer ses attributs. Le contrat intelligent est utilisé comme un lieu de rassemblement des informations non sensibles, permettant à l'utilisateur d'assembler son document SDI (SDO[16]).

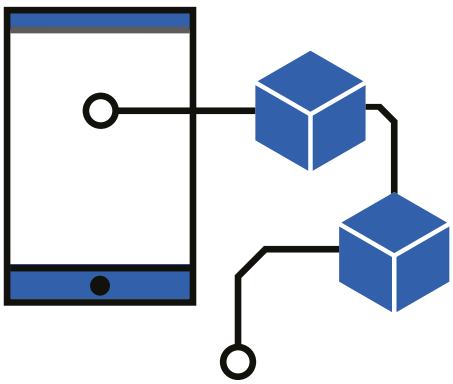
Enfin, le contrat intelligent peut permettre le cas échéant la délégation du contrôle du SDI (ce qui permet notamment la mise en place d'un contrôle parental).

Ce contrat intelligent est ainsi un véritable moteur de l'écosystème, aux fonctions multiples.

Il est consultable sur notre GitHub[17].

Synthèse

XSL Labs a déployé son écosystème sur le réseau Binance Smart Chain qui est le réseau offrant à l'heure actuelle le meilleur service possible, alliant scalabilité, frais de réseau peu élevés, solidité et compatibilité cross-chain.



GitHub

XSL LABS

15 Sujet identifié par un SDI.

16 Voir section 3.1.2 Technologie du SDI.

17 Pour consulter le github de XSL Labs : https://github.com/XSL-Labs

03

L'écosystème SYL

3. L'ÉCOSYSTÈME SYL

3.1 SECURE DIGITAL IDENTITY (SDI)

3.1.1 PRÉSENTATION

3.1.1.1 SDI et Self-sovereign identity (SSI)

Le Secure Digital Identity (SDI) que propose XSL Labs est un Identifiant Décentralisé (DID) qui repose sur les 10 principes de la Self-Sovereign Identity[18] développés par Christopher Allen. Le but de la SSI comme celui du SDI est de garantir à l'utilisateur la protection de son identité contre les cybercriminels et son indépendance vis-à-vis des entités privées ou étatiques qui seraient tentées de tirer profit de ses informations ou de lui nuire grâce à elles. Le concept d'identité auto-souveraine propose ainsi de révolutionner les interactions entre les utilisateurs d'Internet, qu'ils soient des individus ou des entités en rendant nos interactions plus sûres et plus dignes de confiance.

1. Existence
L'identité des individus ne peut pas être résumée à leur identité numérique ; l'identité numérique rend uniquement accessibles et publics certains aspects de l'identité pleine des individus.

2. Contrôle
L'utilisateur doit avoir le contrôle sur son identité, et la façon dont ses données sont utilisées. Il est l'autorité absolue en la matière, et peut décider de la partager, de la mettre à jour, de la cacher.

3. Accès
L'utilisateur doit avoir accès à l'ensemble de ses propres données ainsi qu'à toute modification de ces données, sans devoir faire intervenir un quelconque intermédiaire.

4. Transparence
Les systèmes permettant la mise en place de l'identité auto-souveraine doivent être ouvert tant techniquement que dans leur gestion. Les algorithmes doivent être open-source, gratuits, et doivent pouvoir être examinés pour comprendre leur fonctionnement.

5. Persistence
Les identités doivent subsister tant que leurs auteurs le souhaitent, du moins jusqu'à ce qu'elles deviennent obsolètes de par l'évolution technologique. En parallèle, les utilisateurs doivent pouvoir actionner leur droit à l'oubli.

6. Portabilité
L'identité ne doit pas être détenue par un tiers unique, même s'il s'agit d'une autorité de confiance. Une identité portable assure que son auteur en garde le contrôle, ce qui favorise sa persistance.

7. Interoperabilité
L'identité doit être utilisable le plus largement possible, à travers le monde entier, à travers des systèmes différents, sans que son auteur en perde le contrôle.

8. Consentement
L'utilisateur doit donner son accord à l'utilisation de son identité. Tout partage de donnée, envers qui que ce soit, est soumis à son consentement exprès.

9. Minimalisation
La divulgation de données doit se limiter au strict minimum. Des procédés techniques de type zero-knowledge soutiennent ce principe, et tout doit être mis en œuvre pour protéger au maximum la vie privée de l'utilisateur.

10. Protection
Les droits de l'utilisateur doivent être protégés. Si les besoins des systèmes d'identité entrent en conflit avec les droits de l'utilisateur, ces derniers priment. Les systèmes doivent en outre utiliser des algorithmes indépendants, pouvoir résister à la censure, aux attaques informatiques, et être décentralisés.

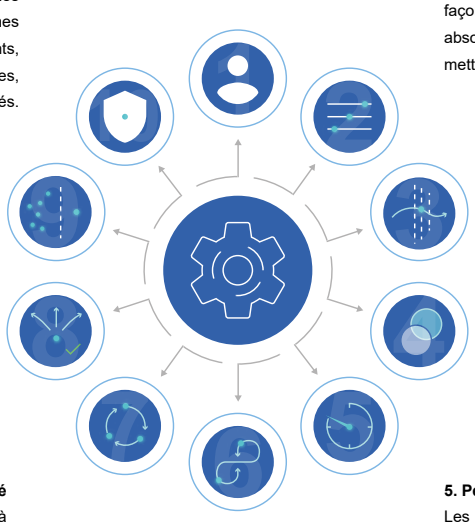


Illustration : Les 10 principes de la SSI

La technologie du SDI qui repose sur ces principes est à la base de toute la solution que souhaite apporter XSL Labs afin de lutter contre le vol de données.

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

3.1.1.2 Comment le SDI va-t-il lutter contre le vol de données ?

La centralisation du stockage des données constitue l'un des problèmes auquel compte remédier la solution de XSL Labs.

En effet, lorsque des cybercriminels parviennent à pénétrer dans une base de données centralisée, ils disposent de l'ensemble des données utilisateur à la fois, ce qui leur permet de s'approprier toutes les données stockées par de nombreux utilisateurs d'un service.

C'est le premier problème que le SDI résout. Selon le W3C[19], un identifiant décentralisé, ou DID, est "un identifiant unique au niveau mondial qui ne nécessite pas d'autorité d'enregistrement centralisée parce qu'il est enregistré sur la technologie des registres distribués (DLT[20]) ou une autre forme de réseau décentralisé". La blockchain et les serveurs décentralisés qui constituent la base de la technologie du SDI permettent une décentralisation du stockage des données d'identité des utilisateurs de SDI. Il est impossible de relier des données d'identité et un utilisateur de SDI en particulier. La seule personne capable d'utiliser ces données d'identité est le sujet SDI, parce qu'il est le seul à posséder la clé privée indispensable pour pouvoir les présenter.

De cette façon, le cybercriminel qui souhaiterait obtenir les données personnelles des utilisateurs du SDI devra pirater un à un les appareils de chaque utilisateur. Une telle complexité décourage ces pratiques rendues inefficaces et bien moins rentables.

Le deuxième problème que résout le SDI est celui de la dispersion des données personnelles. Grâce au SDI, l'identification et l'accès à un site ou un service pourraient ne plus requérir un accès à des données personnelles. Le service pourrait simplement avoir accès à la suite de caractères qui constitue le SDI (voir section 3.1.2 : Technologie du SDI) sans jamais pouvoir l'associer avec d'autres informations.

Aussi, le partage de données personnelles avec un service permet de choisir quelles données sont transmises, il n'est plus nécessaire de partager des données superflues dans le cadre du service. Celui-ci ne bénéficiant que d'un accès très restreint aux données ne peut exploiter celles-ci à des fins commerciales ou politiques.

Il est également possible d'accéder à un service sans aucune divulgation de données. Il s'agit alors d'émettre un document vérifié établi grâce à certaines données et qui atteste que les conditions d'accès au service sont remplies. Ce procédé est parfois nommé "preuve à divulgation nulle de connaissance" et plus communément Zero-Knowledge Proof.

19 Le W3C, ou World Wide Web Consortium, est l'organisme majeur de standardisation des technologies du World Wide Web.
20 Distributed Ledger Technology

Exemple : Dans le cadre de l'inscription à un service soumis à une vérification de majorité, le SDI permet de confirmer au service que l'âge requis est atteint, sans transmettre d'éléments précis tels qu'une date de naissance.

Le SDI définit donc une nouvelle ère en termes de sécurité des données des utilisateurs sur Internet.

Il permettra également à terme de considérablement réduire le pouvoir de grandes entreprises telles que Facebook ou Google, dont les solutions facilitent, au prix de profilage massif, la connexion à un grand nombre de services tiers. Le pouvoir de telles entreprises technologiques leur donne en effet un contrôle démesuré sur les activités sur Internet, sur les données et sur la vie privée des utilisateurs. De plus, leur modèle économique repose sur leur exploitation à des fins lucratives ou politiques. Aujourd'hui, le droit à la vie privée n'est pas respecté et la vie numérique de chacun est contrôlée en partie par les GAFAM[21].

La technologie du SDI constitue un exemple très important de contre-pouvoir décentralisé face aux géants du web. Le SDI permet de conserver l'aspect pratique d'un identifiant unique tout en garantissant la sécurité des données et la souveraineté de l'utilisateur sur celles-ci.

L'adoption des DID est vouée à croître fortement au cours des années à venir. Le SDI de XSL Labs peut être utilisé de la même manière que tous les autres DID existants. À terme et lorsque les identifiants décentralisés seront utilisés par un nombre suffisant de personnes, il ne sera peut-être plus possible de demander l'accès aux données d'un utilisateur de DID sans posséder soi-même un DID, ce qui réduira de facto à néant les risques de fraude et de vol de données.

Une présentation complète de la technologie SDI et de son écosystème sont détaillés dans les sections suivantes.

GAFAM : Google, Apple, Facebook, Amazon et Microsoft

Synthèse

Le Secure Digital Identity (SDI) est un identifiant décentralisé qui s'appuie sur les principes de la Self-Sovereign Identity. Son objet est de garantir l'indépendance et la souveraineté des utilisateurs dans la gestion de leurs données en utilisant des technologies décentralisées, indépendantes d'autorités centralisées et du pouvoir des États ou des GAFAM. Il permet de lutter à la fois contre le vol et la dispersion des données en évitant le stockage de ces dernières sur des bases de données centralisées et en utilisant des méthodes Zero-Knowledge Proof (ZKP).

21 Il s'agit d'un acronyme désignant les géants du Web.

TECHNOLOGIE DU SDI

3.1.2 TECHNOLOGIE DU SDI

Avant de pouvoir associer à son identité des informations personnelles vérifiées par des entités tierces, il est nécessaire de créer un SDI, identifiant qui référence un seul utilisateur et respecte les principes suivants :

- le SDI ne peut pas être assigné (ou réassigné) à une autre personne
- le SDI peut fonctionner sans autorité centrale
- le SDI est relié à une ou plusieurs clés cryptographiques permettant de vérifier que son propriétaire a sur lui un contrôle exclusif
- le SDI permet de retrouver un document public, le document SDI, qui référence d'autres éléments tels qu'une ou plusieurs clés publiques, des services et autres

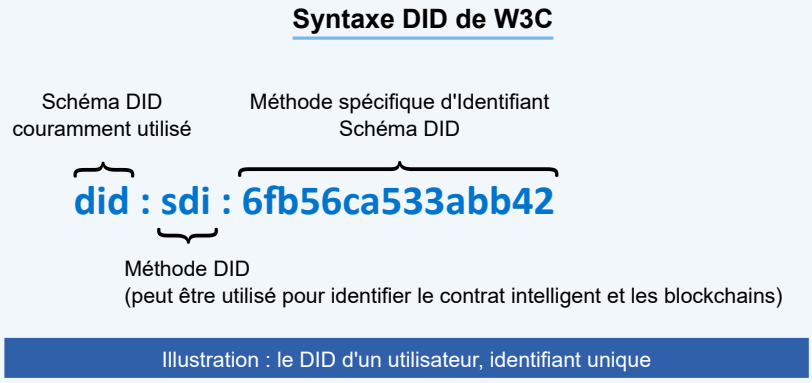


Illustration : le DID d'un utilisateur, identifiant unique

3.1.2.1 Document SDI (SDO)

Le SDI est un identifiant permettant d'obtenir un document SDI (également appelé un SDO) présent sur une blockchain publique.

3.1.2.2 Le document SDI fait référence à un SDI

Ce document SDI constitue le profil public essentiel de l'utilisateur. Il n'a pas vocation à contenir beaucoup d'informations, et puisqu'il est public et disponible sur une blockchain publique, il ne doit pas contenir d'informations d'identité, telles que nom, date de naissance ou autres.

La section 3.1.2.4 décrit les mécanismes permettant d'ajouter de nouveaux types d'informations au document SDI. Les travaux de standardisation en cours définiront les contenus possibles pour un tel document, sa syntaxe et son organisation.

3.1.2.3 Historique de la technologie et innovations récentes

En 2017, avec les premières expérimentations publiques sur les identités décentralisés, la Decentralized Identity Foundation[22] (DIF) a commencé à lister les méthodes de résolution des DID pour constituer un “Universal Resolver[23]” qui permet à chaque fournisseur de service souhaitant interagir avec un DID présenté par un utilisateur de retrouver le DID Document qui lui est associé.

Ce tableau de correspondance est référencé dans le premier document du groupe de travail du W3C sur les DID[24].

La sortie de ce document sur les DID, finalisé en 2019, a constitué une avancée majeure puisque le World Wide Web Consortium (W3C) est le principal organisme de standardisation des technologies d’Internet (on lui doit déjà entre autres les standards HTML, DOM, PNG, XML).

XSL Labs rejoindra prochainement la Decentralized Identity Foundation (DIF) afin de faire lister sa propre méthode DID dans le tableau officiel de résolution des DID.

3.1.2.4 Contenu du document SDI

Comme indiqué dans la section 3.1.2, un identifiant SDI est toujours associé à un document SDI. Ce document ne contient pas directement d’informations personnelles, il contient principalement les éléments suivants :

- des sous identifiants utilisés comme marqueurs dans le document SDI
- des clés publiques
- des informations associées à ces clés publiques à propos des services et des usages concernés
- des informations sur le créateur du document SDI avec des dates de création/de mise à jour
- une signature

Définition

Les clés publiques (et indirectement les adresses “crypto” publiques) sont liées de façon mathématique à des clés privées qui doivent demeurer dans le wallet de leur propriétaire, sous son contrôle exclusif. Les clés privées servent à signer des données (documents, transactions, preuves ou autres); les clés publiques permettent de vérifier la validité de ces signatures.

22 *Pour plus d'informations : https://identity.foundation*
23 *Pour suivre l'état et l'avancée des travaux relatifs à celui-ci : https://github.com/decentralized-identity/universal-resolver/*
24 *Pour plus d'informations : https://w3c.github.io/did-core/*

Dans l'exemple suivant, le SDI et le document SDI sont liés à un individu. Toutefois, le SDI peut également être associé à une personne morale, à un objet ou à une organisation.

Voici un exemple de document SDI (au format standard JSON/JSON-LD) :


```
{
  "@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=="
    }
}
```


Illustration : le document SDI correspondant au SDI "did:sdi:aea42randn1awa3xzhjkbvc33"

Pour rappel, ce document est la résolution du SDI **"**did:sdi:aea42randn1awa3xzhjkbvc33".

Pour trouver ce document, il faut résoudre les différents segments.

"did" indique un protocole d'identité décentralisée, tout comme "http" indique un protocole de communication serveur/client pour naviguer sur le World Wide Web.

"sdi" correspond à la méthode DID[25] utilisée.

Une fois la méthode trouvée (exemple : il s'agit du contrat intelligent 0xb9c15…98e246504 sur la Binance Smart Chain), l'identifiant permet de trouver le document SDI, ici on interroge donc le contrat intelligent avec l'identifiant "aea42randn1awa3xzhjkbvc33" (il s'agit d'un identifiant aléatoire attribué à la création du SDI). Que ce soit directement via un contrat intelligent principal ou bien à travers des contrats intelligents individuels, la documentation de la méthode DID permet d'obtenir le document SDI, la "résolution" du SDI.

Le contenu rudimentaire du document SDI dans la figure ci-dessus peut être bien plus divers et détaillé. Il permet cependant d'établir une vision d'ensemble de ce type de documents afin d'en expliquer les différentes parties.

25 La liste des DID Methods.

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

Cette ligne indique qu’il s’agit d’un document lié à un identifiant décentralisé.

“id”: “did:sdi:aea42randn1awa3xzhjkbvc33”

Ce premier “id” indique l’adresse du SDI que le document SDI résout (qui lui est associé).

“controller”: “did:sdi:aea42randn1awa3xzhjkbvc33”

Cette première indication de “controller” spécifie qui contrôle ce SDI et peut y effectuer des modifications. Il s’agit ici du cas le plus courant, l’identité du contrôleur est la même que l’identité qui est décrite dans le document SDI.

De prime abord, cela peut sembler être la seule possibilité. Cependant, bien d’autres cas de figure sont envisageables qui ont une utilité dans les situations suivantes (liste non-exhaustive) :

- Une personne utilise plusieurs wallets différents pour contrôler une même identité
- Une personne utilise un seul wallet pour contrôler plusieurs identités
- Une personne adulte gère certaines parties de l’identité décentralisée d’un enfant
- Une personne délègue à un tiers de confiance certains droits sur tout ou partie de son identité

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

Ce segment décrit la méthode d’authentification standard du propriétaire du SDI, une clé publique d’authentification y est insérée.

Le nouvel **“id”** qui se termine par #authkey permet de renvoyer directement à ce segment. Ici, le SDI est “did:sdi:aea42randn1awa3xzhjkbvc33” mais il est possible d’indiquer directement la clé qui sert d’authentification. Pour procéder, et atteindre un segment précis, il suffit d’ajouter une ancre, comme ici dans le cas présenté : “did:sdi:aea42randn1awa3xzhjkbvc33#authkey”.

Le “**type**” renvoie à l’algorithme de signature numérique à clé publique utilisée pour l’authentification, ici la variante de DSA[26] utilisant la cryptographie sur courbes elliptiques[27].

Le “**controller**” fait référence au SDI responsable de ce segment. Ici encore il s’agit du cas le plus simple puisque que la référence est identique au propriétaire de l’identité.

“**publicKeyBase58**” est suivi de la valeur de la clé publique encodée en base 58.

26 Digital Algorithmic Signature : il s’agit d’un algorithme de signature numérique standardisé.
27 Ensemble de procédés cryptographiques particulièrement adaptés à la cryptographie à clé publique.

Ce segment pourra être utilisé par un service web externe pour authentifier un nouvel utilisateur se présentant avec son SDI.

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

Le concept de Verifiable Credentials est décrit dans la section 3.1.3. Ces références sont des données généralement vérifiables, disponibles à l'intérieur des wallets des utilisateurs mais qu'il est parfois utile voire nécessaire de spécifier à un service en ligne centralisé capable d'effectuer ce type de vérification.

Une telle configuration permet de partager plus simplement un Verifiable Credential avec une entité qui ne fait pas partie de l'écosystème. Concrètement, cette entité peut vérifier un Verifiable Credential lié à ce SDI en se rendant à l'adresse indiquée, ici “https://example.com/vcheck” et en effectuant un simple copier-coller ou en passant les informations du Verifiable Credentials en paramètres.

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

A la fin du document SDI se trouve une signature numérique qui permet d'authentifier son créateur. La première date fait référence à la date effective de création du document dans le contrat intelligent puis donne des détails sur la signature qui sert de preuve, contenant souvent une date légèrement antérieure.

Là encore, c'est le cas le plus simple qui est affiché, le créateur est le propriétaire de l'identité mais ce n'est pas forcément le cas le plus fréquent. En effet, la création d'un document SDI sur une blockchain nécessite souvent le paiement de frais de création de données et l'utilisateur n'est pas forcément celui qui effectue cette transaction.

Exemple : si un document SDI doit être créé sur un contrat intelligent sur la Binance Smart Chain, un utilisateur qui télécharge un wallet pour créer et gérer son identité décentralisée n'est pas nécessairement immédiatement en possession de BNB pour payer les frais de “gaz” nécessaires à la création de ce document SDI. Le propriétaire de l'identité peut donc se trouver dans une situation où il sait fournir tous les détails pour créer le contenu de son document SDI mais passe par un intermédiaire pour le mettre “en ligne” sur le contrat intelligent de la blockchain. Cet intermédiaire procédera au paiement de la transaction associée à la création du document SDI pour le compte du véritable utilisateur/propriétaire.

Le créateur du SDI Document peut donc être différent du propriétaire. Cependant, même dans ce cas :

Le SDI du créateur permet de retrouver et de vérifier l'identité de cet intermédiaire pour assurer qu'il est bien un intermédiaire de confiance (ce SDI peut ainsi pointer sur le document SDI d'un administrateur référencé).

Cela ne signifie pas obligatoirement que ce créateur à la capacité de modifier les informations du document SDI, particulièrement sans le consentement du propriétaire de l'identité. Celui-ci peut indiquer qu'il reste seul autorisé à effectuer de futures modifications sur son document SDI ou à partager son contrôle avec un tiers.

3.1.2.5 Exemple d'utilisation

Un service web souhaite authentifier les possesseurs de SDI via une page web dédiée. Il s'agit ici d'un cas commun d'authentification sur un site web initialement affiché dans le navigateur d'un ordinateur de bureau.

La page de login du serveur affiche un QR Code qui contient l'adresse du service web et une chaîne de caractères aléatoires unique (également appelée un "challenge").

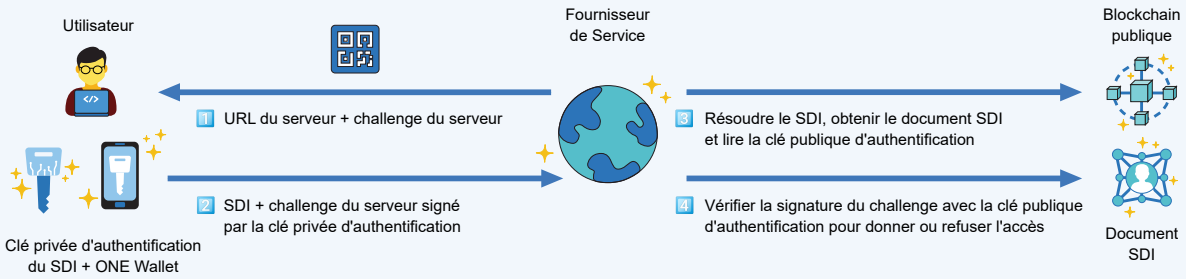


Illustration : Authentifier le propriétaire d'un SDI sur un serveur web

L'utilisateur du wallet scanne le QR Code présent sur la page. Le wallet demande à l'utilisateur s'il accepte d'utiliser une clé liée à son SDI pour s'authentifier sur ce serveur puis, après confirmation, utilise la clé privée d'authentification pour signer le challenge contenu dans le QR Code. Le wallet renvoie ensuite au serveur le challenge signé et son SDI (identifiant).

Le service web reçoit le SDI (faisant office de nom d'utilisateur) et suit automatiquement les étapes décrites plus haut pour obtenir le document SDI associé. Le service lit le segment relatif à l'authentification et trouve la clé publique liée au SDI utilisable pour l'authentification par défaut.

Le serveur doit maintenant s'assurer que le propriétaire du SDI possède bien la clé privée correspondant à cette clé publique. Il lui suffit pour cela de vérifier la validité de la signature qu'il vient de recevoir. Si la signature est valide, le serveur confirme l'authentification et fournit l'accès souhaité.

L'utilisation d'un SDI pour effectuer une authentification est un cas d'utilisation simple qu'il est important d'avoir compris avant de passer à la description des Verifiable Credentials.

Note

Il est possible, dans un document SDI, d'affecter plusieurs clés d'authentification à des services web et contextes différents, mais également d'affecter d'autres clés à d'autres usages comme par exemple, le chiffrement de messages et la signature de contrats.

3.1.3 VERIFIABLE CREDENTIALS

Pour qu'un propriétaire de wallet d'identité puisse obtenir différentes informations vérifiables à son sujet, il est nécessaire qu'un émetteur de confiance ait été préalablement identifié et contacté. La confiance en cet émetteur de Verifiable Credentials doit être établie grâce à des informations vérifiables sur sa propre identité et sa qualification d'émetteur.

A l'instar des Infrastructures de Gestion des Clés Publiques (IGCP), une chaîne de confiance doit garantir la fiabilité de l'identité de tous les acteurs de la chaîne, elle garantit alors indirectement la fiabilité de l'information transmise.

Exemple : information vérifiable (VC) de type "nom de famille". Cette information peut être validée par un émetteur qualifié de "fournisseur de service de KYC". Ceci nécessite préalablement la vérification de la fiabilité de l'identité de l'émetteur à travers son propre SDI.

En haut de cette chaîne de confiance se trouve le premier maillon de la chaîne. Il s'agit de l'identité vérifiée la plus haute : l'autorité racine. Dans le cadre du SDI interrogeable sur la blockchain, il s'agit généralement du SDI de l'administrateur du contrat intelligent.

Pour rappel, il est possible d'interagir avec d'autres DID et blockchains pourvu que le portefeuille ou l'outil qui cherche à vérifier un VC sache remonter la chaîne de confiance des SDI entre différentes blockchains (principe d'interopérabilité).

Il est aussi possible de ne pas rendre obligatoire le fait que l'autorité racine possède un SDI, il lui faut alors détenir au moins une identité liée à un certificat délivré par une autorité de certification d'identités publiques et d'organismes étatiques. (comme c'est le cas pour des certificats SSL/TLS[28])

La possibilité de choisir entre différentes autorités racines permet d'augmenter la décentralisation de l'architecture. Il sera néanmoins nécessaire pour XSL Labs de travailler à l'accompagnement de ces différentes "autorités" afin que l'utilisateur puisse juger facilement de la fiabilité des identités de ces autorités.

28 *Protocoles de sécurisation des échanges sur réseaux informations. Le TLS est le successeur de SSL.*

Le cas suivant évoque une chaîne de confiance simple.

De multiples autorités racines sont intégrales aux chaines de confiance

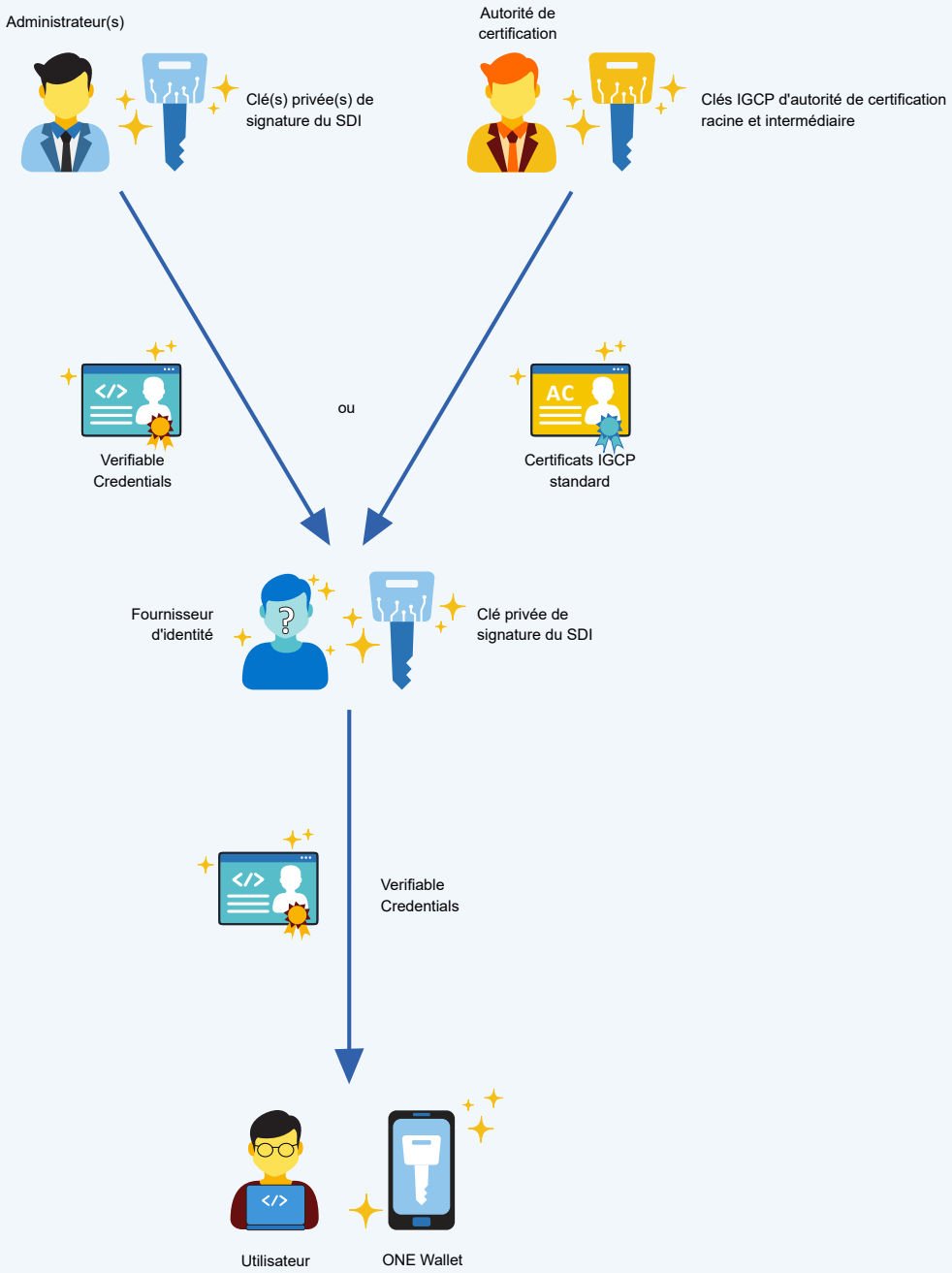


Illustration : Vérifier un VC implique aussi de remonter la chaîne de confiance pour contrôler les identités en question

Afin que l'utilisateur obtienne un Verifiable Credential, il doit le demander à un fournisseur d'identité (émetteur de Verifiable Credential) dont la légitimité a été préalablement démontrée.

Le schéma ci-dessous détaille les étapes de cette procédure de vérification :

Comment vérifier la légitimité d'un Fournisseur d'identité?

1. Vérifier le fournisseur du document SDI
2. Vérifier le fournisseur du profil public
3. Vérifier le fournisseur de la trace publique des Verifiable Credentials
4. Vérifier le Verifiable Credential public (rôle)
5. Vérifier si l'émetteur du document SDI est légitime (ici cas simple : l'admin)
6. Vérifier la signature publique du Verifiable Credential

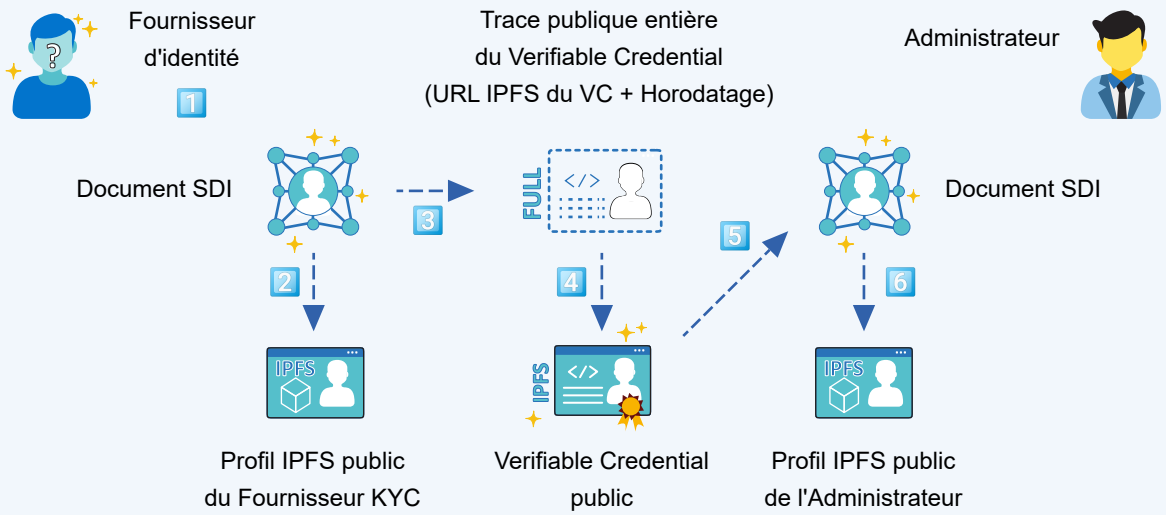
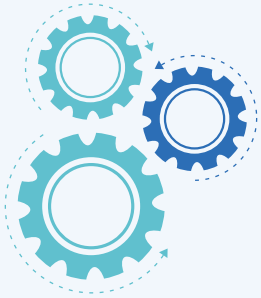


Illustration : Comment vérifier qu'un fournisseur d'identité est digne de confiance

L'utilisateur peut être dirigé vers un émetteur de VC ou décider de lui-même d'aller vers un prestataire reconnu. La notion même d'informations vérifiables présentables plusieurs fois avec la même fiabilité entraînera certainement des modifications de comportement et de parcours utilisateurs.

Il est à noter aussi que l'utilisateur propriétaire possédant une identité vérifiée pourrait lui aussi à son tour émettre un Verifiable Credential pour un autre utilisateur.



3.1.3.1 Document SDI d'un émetteur de VC

Ci-dessous est décrit un cas d'usage simple des fournisseurs d'identité (émetteurs publics de Verifiable Credentials au rôle bien identifié, séparés des utilisateurs standards).

```
{
    “@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”
    }]
}
```

Illustration : Document SDI d'un émetteur public de Verifiable Credentials

Différence notable, un profil public est mis à disponibilité sur 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”}
```

Pour rappel, IPFS est un espace de stockage décentralisé public où les fichiers sont référencés par leur hash. Ainsi le contenu XML du fichier ci-dessus provient d'un fichier IPFS que l'on peut retrouver facilement avec un client logiciel IPFS, comme l'image référencée dans ce fichier. Les navigateurs web intègrent progressivement la capacité de lecture de ces fichiers sur ce réseau. A l'heure actuelle, il est toutefois encore préférable d'utiliser des services de passerelle web pour procéder.

Les fichiers stockés sur IPFS ne peuvent pas être supprimés volontairement, il faut donc partir du principe qu'ils peuvent rester disponibles longtemps pour tous. De ce fait, il est nécessaire de n'indiquer que des informations neutres et non-nominatives (exemple : site web + mail de contact générique).

Pour vérifier la légitimité d'un émetteur de VC, l'utilisateur peut ensuite (avec l'aide automatique de son portefeuille logiciel) interroger le contrat intelligent qui gère son SDI. Il obtient alors une liste de traces de Verifiable Credentials que l'émetteur a précédemment lui-même reçu. Ainsi, le client logiciel vérificateur peut trouver la trace d'un Verifiable Credential fourni par l'administrateur pour qualifier son rôle de fournisseur d'identité (et de fournisseur de VC) sous la forme d'une référence IPFS ("IPFS url") et d'une information d'horodatage fiable liée à la blockchain utilisée.

La référence IPFS permet de retrouver le contenu public du Verifiable Credential fourni par l'administrateur à cet émetteur de VC. Le portefeuille client peut alors vérifier la signature de ce VC par l'admin et conclure à la légitimité de l'émetteur.

3.1.3.2 Demande et réception d'un Verifiable Credential

Une fois la confiance établie vis-à-vis de l'émetteur de Verifiable Credentials, il est possible d'en effectuer la demande.

Ci-dessous, les étapes nécessaires à la requête puis à l'obtention d'un Verifiable Credential :

- L'utilisateur suit la procédure de KYC et utilise sa clé privée de SDI pour signer une requête de demande de VC
- L'émetteur vérifie la signature de cette requête (en consultant le document SDI de l'utilisateur)
- L'émetteur utilise sa propre clé privée pour signer un Verifiable Credential correspondant à l'information vérifiée dans les documents officiels

Cette opération peut être effectuée via une interface web ou une API si la clé de l'émetteur est protégée sur un Hardware Security Module[29]. Elle peut aussi être réalisée sur une machine locale à la sécurité renforcée fournie par XSL Labs et qui pourrait notamment comprendre un mini-portefeuille logiciel sous la forme d'une carte à puce réservée aux fournisseurs d'identité. Ces solutions tout-en-un devront être développées dans des buts de praticité et sécurité vis-à-vis des émetteurs de VC.

- L'émetteur crée une trace publique "on-chain" de ce Verifiable Credential en associant le hash[30] de ce VC avec une information d'horodatage (fiable/liée à la blockchain)
- L'émetteur envoie le Verifiable Credential à l'utilisateur qui lui en fait la demande

29 Les HSM sont des appareils physiques a priori inviolables qui recourent à des fonctions cryptographiques. Leur forme varie, il peut s'agir d'une carte PCI, d'un boîtier externe rackable, d'un périphérique USB ou autres.

30 Un hash consiste en une suite de caractères alphanumériques résultant de l'application d'une fonction mathématique à un ensemble de données. Il s'agit d'une opération à sens unique.

Comment obtenir un Verifiable Credential d'un émetteur

(ex : Verifiable Credential de nationalité provenant d'un fournisseur d'identité)

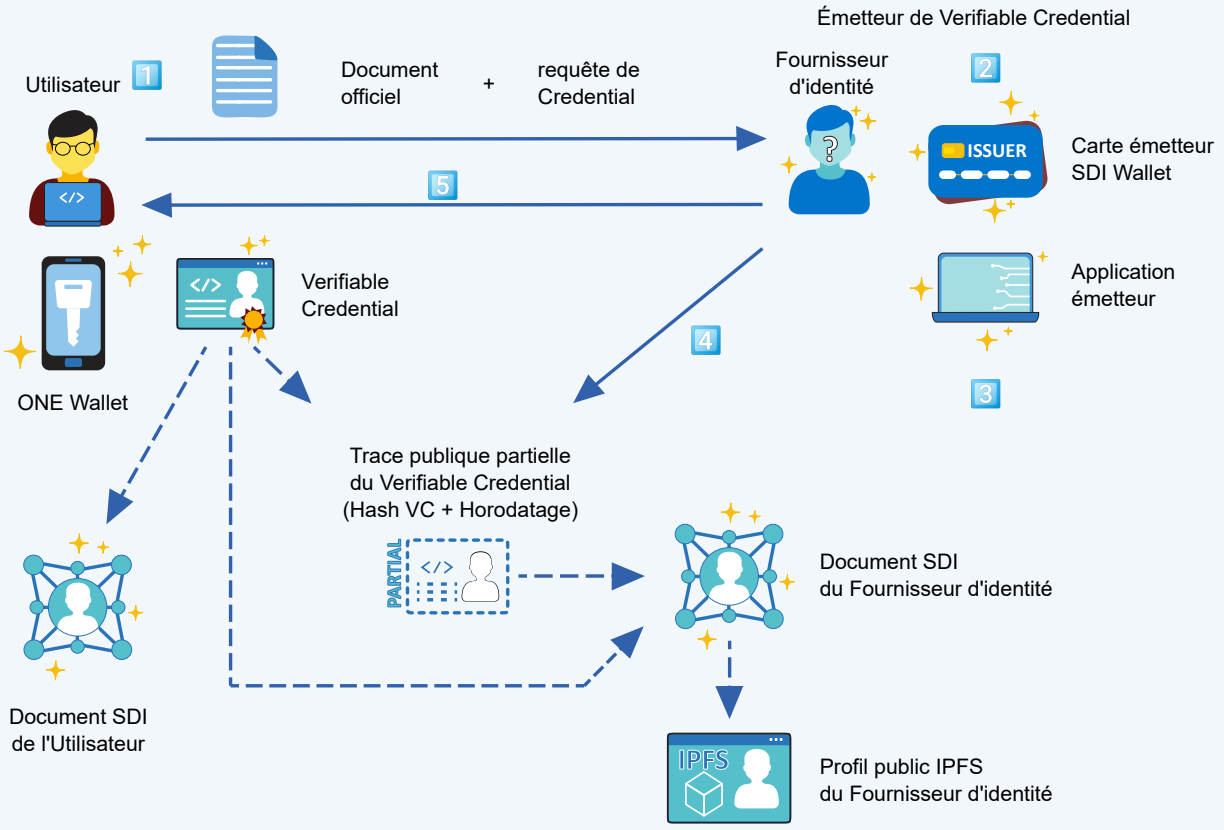


Illustration : Les étapes de la demande et de la réception d'un Verifiable Credential

3.1.3.3 Verifiable Credential : création, contenu et vérification

Le Verifiable Credential peut être transmis de son auteur à son destinataire par mail, QR code, face à face, transfert de fichier, réseau social, API[31] et autres. Le portefeuille d'identité du demandeur (destinataire initial) interprète alors son contenu et effectue la première vérification complète de ce Credential avant de l'importer.

31 Interface de programmation, un ensemble de fonctions et procédures permettant la communication de données entre des applications.

VERIFIABLE CREDENTIAL

Illustration : Exemple de Verifiable Credential donné par une université à un de ses membres

Le Verifiable Credential contient les informations suivantes :

- Une entête pour indiquer que ce fichier est un Verifiable Credential
- Des “metadonnées” contenant ici le SDI de l’émetteur et la date de création (mais pouvant contenir aussi par exemple une date d’expiration, une image associée, des détails sur un mécanisme de révocation ou autres)
- Les données concernées par la requête initiale
- Le SDI du destinataire/propriétaire
- L’information précédemment vérifiée par l’émetteur (ici, le fait d’être membre de l’université)
- La preuve sous la forme d’une signature de cet ensemble par la clé privée de l’émetteur

Ce Verifiable Credential est envoyé à son propriétaire qui peut ainsi le vérifier et le représenter à la demande.
Chaque nouveau destinataire peut alors lui aussi effectuer cette vérification du Verifiable Credential.

La vérification consiste donc à remonter et vérifier depuis le Verifiable Credential :

- le SDI du propriétaire
- le SDI de l'émetteur
- la signature du Verifiable Credential

Comment vérifier un Verifiable Credential

(ex : Credential de membre d'une Université)

1. L'utilisateur fournit le Verifiable Credential
2. Le vérificateur vérifie le document SDI de l'utilisateur
3. Le vérificateur vérifie le document SDI de l'émetteur/fournisseur d'identité
4. Le vérificateur vérifie la légitimité de l'émetteur/fournisseur d'identité
5. Le vérificateur vérifie la trace publique du Verifiable Credential (horodatage)

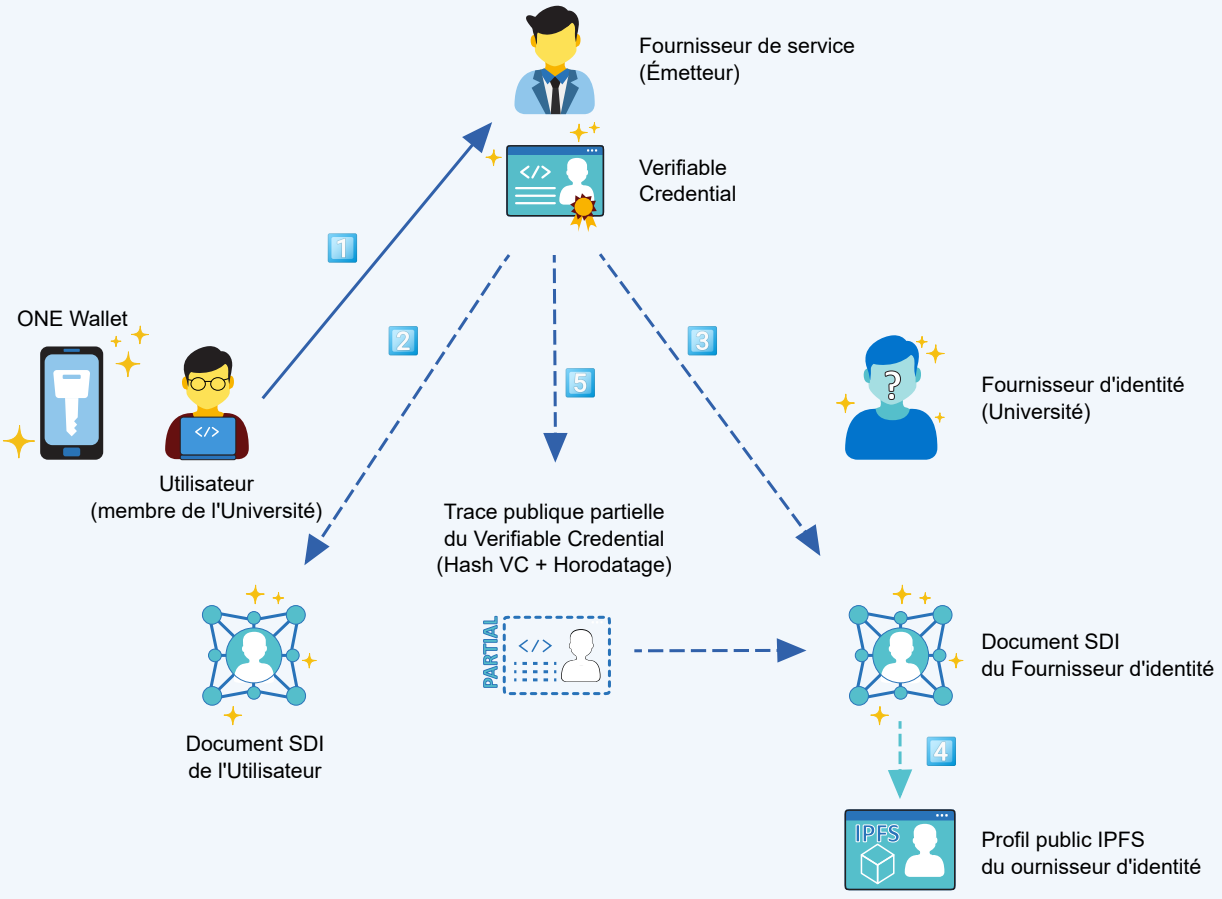


Illustration : Vérification d'un Verifiable Credential

3.1.3.4 Verifiable Presentation : requête, contenu et vérification

La présentation du Verifiable Credential se fait généralement à travers un autre format de fichier, la “Verifiable Presentation”. Celui-ci reprend le Verifiable Credential et l’associe à une signature liée à un challenge envoyé par celui qui demande le Verifiable Credential, pour éviter toute forme de réutilisation.

Comment demander et obtenir un Verifiable Credential d'un possesseur de VC

1️⃣ Le demandeur fournit un challenge aléatoire, un "domaine" (qui peut être un domaine d'un site Web ou de n'importe quel identifiant donnant un contexte), avec des détails sur quel credential est demandé et une raison pour la demande.

2️⃣ Le possesseur du VC lit le domaine, les détails et la raison et est invité à signer l'information recueillie : "Credential + domaine/contexte + challenge du demandeur".
Ce contenu, une fois signé, constitue le "Verifiable Presentation".

3️⃣ Le demandeur vérifie le document SDI du possesseur du VC sur la blockchain, vérifie si la signature est valide et vérifie si le Verifiable Credential est authentique.

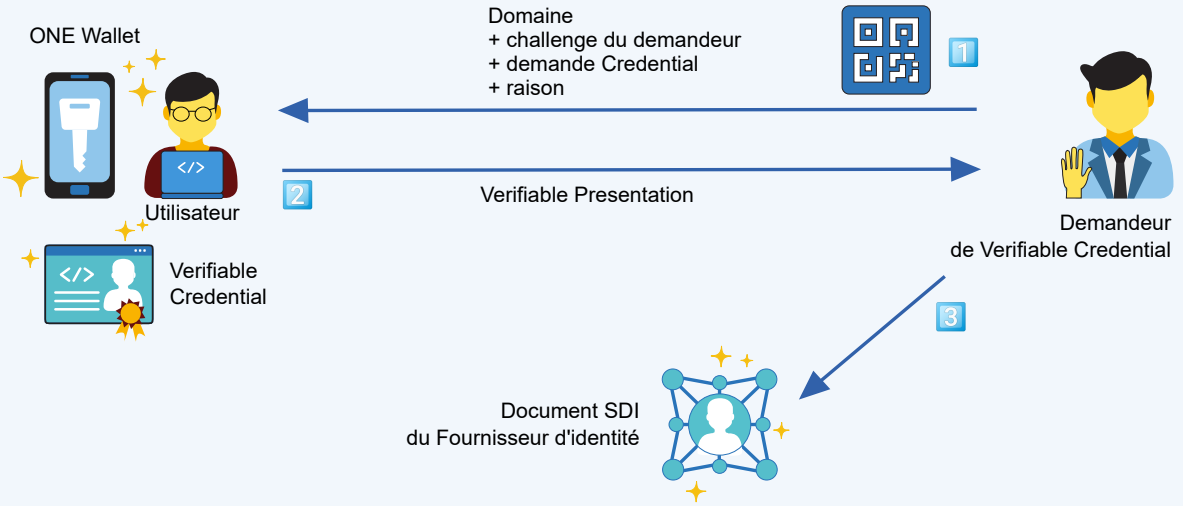


Illustration : Requête et obtention d’une Verifiable Presentation (Verifiable Credential signé)

Chaque Verifiable Presentation est unique et propre au contexte d’une requête et d’un évènement précis. La requête peut être présentée sous la forme d’un QR code directement lisible par l’application ONE, présentée dans la section 3.2.

VERIFIABLE PRESENTATION

Illustration : Étapes de la vérification d'un Verifiable Credential

Le propriétaire du wallet et du Verifiable Credential est donc informé du contexte avant de le signer pour créer la Verifiable Presentation.

La Verifiable Presentation peut être renvoyée au demandeur via une adresse spécifiée dans les détails de la requête (ou dans le “domain”) ou de visu via un QR code si le demandeur a effectué la demande en face à face.

Le demandeur ou quelqu’un qui intercepterait la Verifiable Presentation ne pourrait pas la réutiliser dans un autre contexte.

Le demandeur qui reçoit la Verifiable Presentation peut donc vérifier qu’il a bien affaire au propriétaire du VC, en vérifiant la signature de la Verifiable Presentation via la consultation du document SDI de son propriétaire avant de vérifier le Verifiable Credential.

3.1.4 DURÉE DE VIE D’UN SDI

Le droit à l’oubli est un élément essentiel lorsqu’il est question de données d’identité numérique. L’utilisateur du SDI peut à tout moment consulter l’historique de l’usage de son portefeuille pour un meilleur exercice du droit à l’oubli. Il est possible pour un utilisateur de révoquer publiquement un SDI (le signaler comme désactivé). Si l’utilisateur détruit manuellement sa clé privée, plus personne ne pourra modifier ni utiliser le contenu de son portefeuille d’identité.

3.1.5 SDI NON VÉRIFIÉ

Un SDI dispose d'une fonction de création rapide. Tout utilisateur peut recourir à cette fonctionnalité. Cette fonction pourrait être activée sur une borne de service, un point de paiement, ou encore un point de contrôle.

Cette fonction permettra d'engager la création d'une identité numérique imparfaite qui pourra ensuite être complétée par son détenteur. L'identité numérique temporaire pourra être réduite au minimum d'une seule information permettant à son propriétaire d'en prendre possession. Dans un tel cas de figure, une simple adresse e-mail peut être suffisante.

Le SDI non vérifié se compose :

- D'un élément d'identité de contact (adresse mail, numéro de téléphone)
- D'une fonction pour prendre possession de l'identité nouvellement créée pour passer à un niveau de vérification supérieur, impliquant le recours au KYC

La création d'un SDI non vérifié peut être associé à un futur avantage incitatif proposé au client ou à l'usager. L'obtention définitive de cet avantage ou du droit spécifique accordé nécessitera la complétion du SDI, le cas échéant via une connexion par le biais de l'application décentralisée ONE, ou à un service du site officiel qui sera mis à disposition des utilisateurs.

3.1.6 INTEROPÉRABILITÉ DU SDI

L'interopérabilité et le respect des standards (services et méthodes de résolution) sont des objectifs importants pour le SDI et sont assurés par la conformité avec les standards du W3C (World Wide Web Consortium) et les travaux de la DIF (Decentralized Identity Foundation).

Synthèse

Le SDI consiste en une suite de caractères unique identifiant un utilisateur ou une autre ressource. Il est associé à un document SDI public et disponible sur une blockchain contenant des informations fonctionnelles telles que des sous-identifiants, des clés publiques et des informations liées à ces dernières, des informations sur le créateur du document, sa date de création et ses dates de mise à jour ainsi qu'une signature. Il ne contient aucune information d'identité.

Chaque sujet SDI (la personne ou la ressource associée à un SDI) possède un portefeuille d'identité où sont stockés ses Verifiable Credentials. Ce sont des références délivrées par des tiers au départ de la chaîne de confiance (institutions, entreprises, organismes ou utilisateurs vérifiés) contenant des informations d'identité sur le sujet SDI, ainsi qu'une signature qui prouve qu'il n'a pas été modifié et un horodatage qui certifie l'heure de son émission. Lorsque le sujet SDI souhaite prouver une information à une entité tierce, il émet alors une Verifiable Presentation signée avec sa clé privée qui peut contenir les informations d'une partie, d'un ou plusieurs Verifiable Credentials ou la seule preuve de la validité d'une information sans diffusion de données (Zero-Knowledge Proof).

Le SDI pourra être vérifié avec un service KYC (Know Your Customer) ou non vérifié pour une utilisation rapide. Il sera par ailleurs interopérable avec tous les autres identifiants décentralisés (DID) et pourra aussi être déployé sur tout type de blockchain.

3.2 ONE (Portefeuille DID)

3.2.1 PRÉSENTATION

3.2.1.1 Contexte

Les sections suivantes visent à définir les contours de l'écosystème bâti autour du wallet ONE. Ce projet s'inscrit dans la lignée des travaux autour des identités décentralisées qui visent à utiliser la blockchain pour prouver l'authenticité d'informations personnelles et encadrer davantage les accès à ces données.

3.2.1.2 Un wallet multi-identités

Nos existences numériques se composent aujourd'hui d'une multitude de données personnelles peu vérifiables et sollicitées abusivement à chaque création de compte utilisateur, sans que le service qui les demande ait un intérêt légitime à disposer de ces données. Jusqu'à présent, les internautes n'ont disposé ni d'outils permettant de réduire la diffusion de leurs données ni de moyens permettant de suivre ou lutter contre leur collecte.

Par ailleurs, la démonstration de son identité et de ses attributs est un réel défi dans un monde qui évolue toujours davantage vers le tout numérique.

La gestion des identités numériques comprend la gestion de :

1. La phase d'enrôlement de l'utilisateur et de validation de ses attributs
2. L'identification et l'authentification de l'utilisateur sur la base de ces informations vérifiées
3. La réception, le stockage et la présentation de Verifiable Credentials
4. L'accès à des services et à des transactions sur la base de ses Verifiable Credentials

L'utilisateur est ainsi informé de l'identité des sociétés auprès desquelles il fait la démonstration d'une partie de ses informations pour pouvoir accéder aux services qu'elles proposent. Ce consentement à la présentation d'informations peut être accompagné d'un contexte ou d'un accord d'utilisation (preuve temporaire, durée de stockage, partages potentiels ou autres).

Les fournisseurs de services en ligne endossent généralement le rôle de fournisseur d'identité. Dans le cas contraire, ils délèguent cette activité à des tierces parties, la plupart du temps les géants du web et réseaux sociaux.

Les États tentent, à travers diverses réglementations :

- d'encadrer l'utilisation de ces données personnelles pour limiter leur utilisation abusive (RGPD[32]), souvent à des fins de profilage publicitaire

- de renforcer les niveaux de sécurité des authentifications sur les services en ligne les plus sensibles (DSP2, eIDAS, TSP)

En matière de sécurité, les bonnes pratiques poussées par ces régulateurs reprennent les mêmes bases cryptographiques bien connues des amateurs d'actifs numériques : condensats, chiffrement des données, authentification forte, signature des données et des transactions.

Des rapprochements entre cybersécurité générique et sécurité des actifs numériques existent déjà avec par exemple le support de FIDO (protocole d'authentification forte issus de travaux des géants du web et abondés par les régulateurs) sur certains "hardware wallets" (Ledger, Trezor, Bitbox) ou le support du chiffrement de message au wallet logiciel Metamask[33].

Inversement, certains wallets d'actifs numériques peuvent maintenant effectuer des signatures de messages en dehors du cadre habituel des transactions et transferts d'actifs.

Les acteurs centralisés de la cybersécurité traditionnelle comme les autorités de certification peuvent eux aussi tirer profit de ce rapprochement.

3.2.1.3 Spécificités de ONE dans l'écosystème XSL Labs

ONE est ainsi une application décentralisée qui est la tour de contrôle de l'identité de l'utilisateur du SDI.

La décentralisation de cette application lui permet de ne pas être dépendante d'une autorité tierce en se libérant de tous les intermédiaires qui pourraient potentiellement exercer un contrôle sur les utilisateurs. Cette dApp, pour application décentralisée, permet l'interopérabilité de tous les services qui utilisent le SDI et constitue la porte d'accès vers l'écosystème SYL.

Chaque présentation de données personnelles effectuée par le propriétaire du portefeuille est ajoutée à un historique local consultable (comprenant la nature des données, le destinataire, le contexte, la date, l'heure).

L'application ONE dispose également d'un wallet permettant de gérer les tokens SYL de l'utilisateur ainsi que leur émission.

32 Réglement Général sur la protection des données, UE 2016/679.

33 Extension de gestion des portefeuilles, permettant d'accéder facilement à des applications décentralisées depuis un navigateur Internet.

3.2.2 CARACTÉRISTIQUES ET PILIERS DE ONE

CARACTÉRISTIQUES PRIMAIRES DE ONE

- La création d'un espace utilisateur
- L'envoi et la réception de tokens SYL
- La réception, le stockage et l'utilisation d'informations vérifiées réutilisables (Verifiable Credentials)
- L'historique complet des interactions du compte avec son environnement
- Les services liés à l'usage des clés cryptographiques listées dans son SDI (authentification forte, signature électronique, chiffrement de données)

LES 4 PILIERS DE ONE

- La protection des données personnelles

ONE utilise le SDI dans l'intégralité des services auxquels il sera possible de se connecter, afin de protéger les données des utilisateurs. De plus, il fournira un accès direct aux paramètres du SDI et un historique de l'ensemble des interactions issues de l'activité de l'utilisateur.

- L'évolutivité et l'adaptabilité

Au travers des différentes applications décentralisées qui seront proposées au sein de l'écosystème, ONE peut s'adapter aux besoins de chaque utilisateur.

- Le portefeuille d'identité (Wallet ID)

Le portefeuille d'identité (Wallet ID), servira à la réception et au stockage des Verifiable Credentials émis par des tiers de confiance et à l'émission de Verifiable Presentations.

- Le portefeuille de SYL

Le portefeuille intégré directement à ONE permettra de recevoir ou d'envoyer des SYL et de pouvoir en toute autonomie accéder aux différents services de l'écosystème.

3.2.3 SERVICE KYC (KNOW YOUR CUSTOMER)

3.2.3.1 KYC et dispositif AML

L'une des grandes forces de ONE réside dans le stockage de Verifiable Credentials liés à des KYC, ce qui rend possible une conformité aux réglementations AML (Anti-Money Laundering).

Cet avantage de la solution proposée par XSL Labs vise notamment à considérablement alléger les coûts en temps et en argent pour les entreprises soumises à ces impératifs légaux.

Le secteur financier, représenté par les établissements de paiement, les banques, les plateformes de financement classiques mais aussi les nouveaux prestataires "crypto" sont ainsi soumis à de nombreuses règles (KYC et AML). Cet objectif de lutte contre la fraude, le blanchiment d'argent et le financement du terrorisme se traduit par la nécessité de demander et redemander à leurs utilisateurs un certain nombre de renseignements et justificatifs d'identité (lors de l'ouverture d'un compte par exemple).

Chaque banque dépense environ 60 millions de dollars par an pour les processus KYC.

XSL Labs pourrait faire économiser une grande partie de cette somme aux institutions financières grâce au SDI et à l'application ONE.

3.2.3.2 Coût du KYC

Le coût porté par un KYC qui nécessite l'accès à un service tiers pourra soit être supporté par les fournisseurs de services, soit par le client en fonction du plan d'affaire de chaque service.

Le KYC n'est par nature pas une nécessité mais il peut constituer un prérequis à la fourniture de service, auquel cas le coût du KYC pourrait être intégré dans l'achat d'un service. Lorsque celui-ci sera réalisé, il sera valable requérant le même niveau de vérification.

DOCUMENT TECHNIQUE ONE

3.2.4 TECHNOLOGIE DE ONE

Les attributs des comptes en ligne sont pour le moment souvent hébergés par le service à l'origine de leur création. Dans cette situation courante, le fournisseur de service (Service Provider ou SP) en ligne fait aussi office de fournisseur d'identité (Identity Provider ou IDP) avec son propre portail d'authentification (Single Sign On).

Fournisseur de services avec un fournisseur d'identité intégré

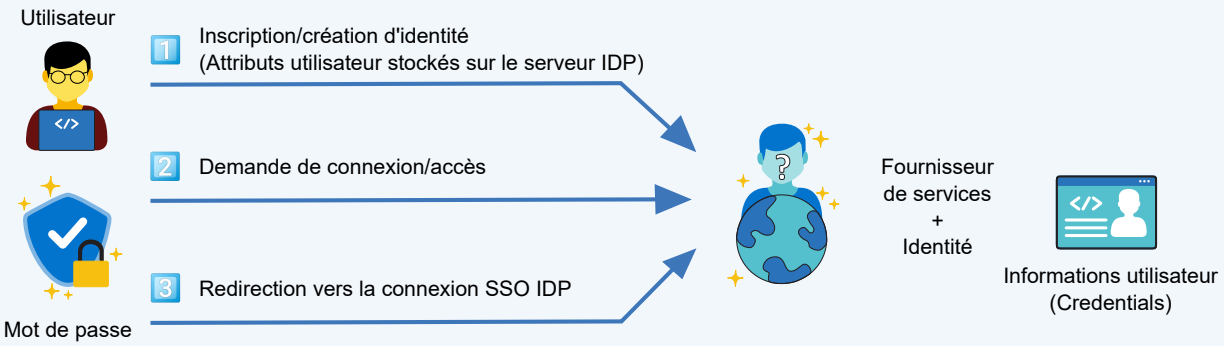


Illustration : Le fournisseur de services (SP) crée le compte de l'utilisateur et ses attributs

Les rôles de fournisseur d'identité et de fournisseur de service peuvent être dissociés, c'est le principe des ouvertures de comptes et partages d'informations à travers l'authentification sur le portail des réseaux sociaux.

Fournisseur de services avec un fournisseur d'identité

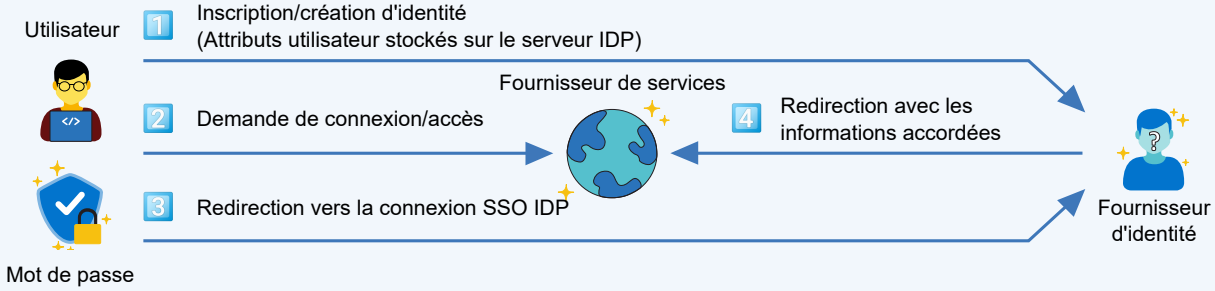


Illustration : Le fournisseur de service (SP) utilise les attributs d'un compte créé chez un fournisseur d'identité (IDP) externe

3.2.4.1 La transition vers les architectures décentralisées

Dans une architecture décentralisée, les actifs numériques sont attribués en référence à une adresse publique, dépendant d'une clé privée conservée par l'utilisateur dans son portefeuille. L'utilisateur effectue uniquement des signatures de transactions qui sont vérifiées.

Portefeuille (clés générées localement) pour les actifs cryptographiques (blockchain)

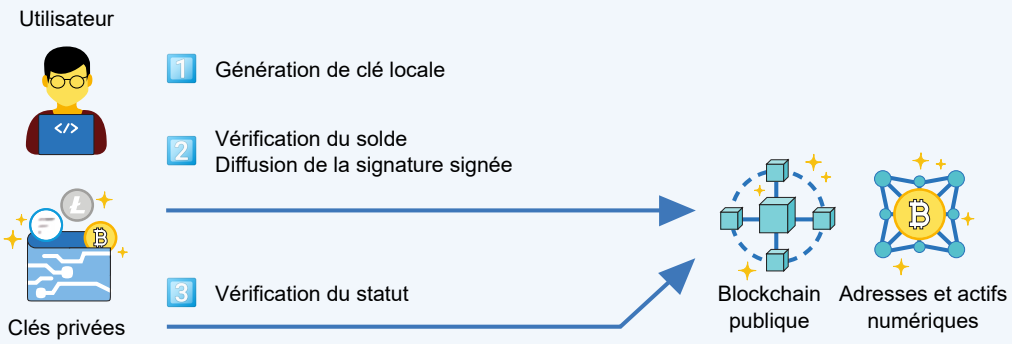


Illustration : Aucune information personnelle n'est conservée hors du portefeuille local du détenteur de SYL

Le wallet ONE permet également de recevoir et de contrôler les Verifiable Credentials.

Wallet One : Gestion du SDI et des actifs cryptographiques

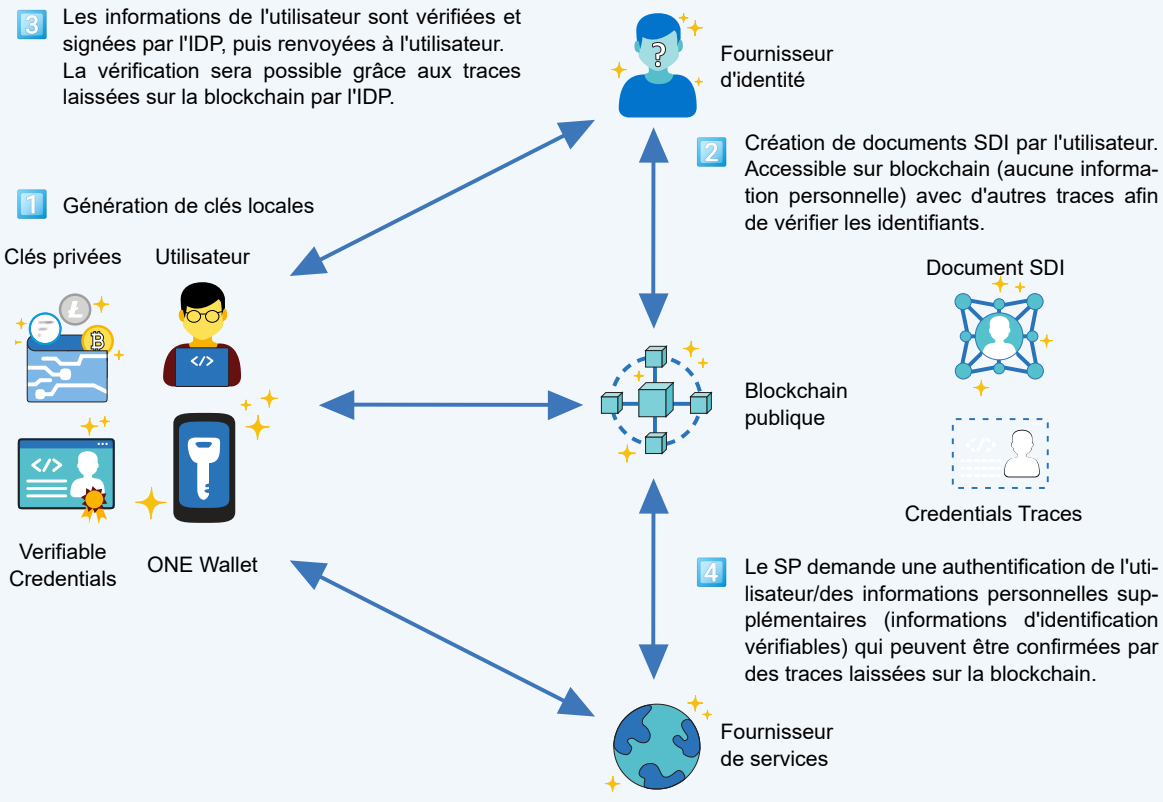


Illustration : le wallet ONE permet de recevoir et contrôler les Verifiable Credentials

Le portefeuille qui gère la clé privée lié au SDI de l'utilisateur doit savoir gérer les Verifiable Credentials reçus et doit aussi :

- Démontrer cryptographiquement à l'IDentity Provider qu'il contrôle bien son SDI
- Tester la validité et la vérifiabilité du "Verifiable Credentials" fourni par l'IDP
- Obtenir les fichiers référencés dans les Verifiable Credentials sur des espaces de stockage centralisés et décentralisés

- Stocker les Verifiable Credentials
- Utiliser les autres clés cryptographiques spécifiées pour d'autres usages (chiffrement, signature générique, signature pour l'authentification)
- Diffuser les Verifiable Credentials sur les bons canaux de communication
- Gérer certains SDIs d'autres chaînes par souci d'interopérabilité/capacité d'évolution

Ce wallet peut profiter des avancées significatives des Hierarchical Deterministic Wallets[34] et proposer une procédure de sauvegarde et restauration simplifiée.

ONE HD Wallet (Clés dérivées de la graine)

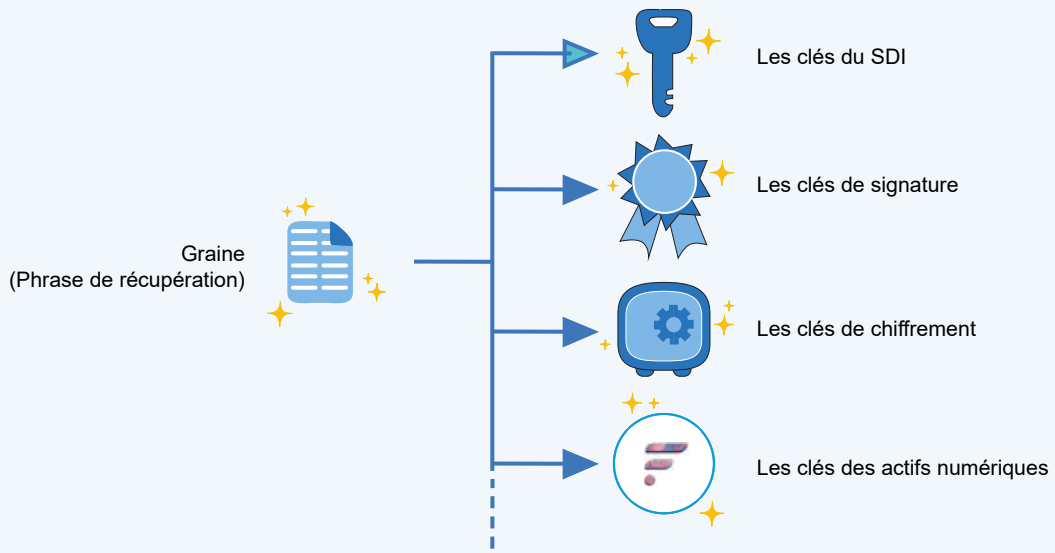


Illustration : le HD Wallet "ONE" gère l'ensemble des clés privées nécessaires à tous les usages cryptographiques

3.2.4.2 Interfaces web

Plusieurs services web optionnels pourront simplifier l'usage des DID et Verifiable Credentials :

- Un annuaire permettant de lister les services pour les utilisateurs, qu'il s'agisse d'émetteurs, sujets ou vérificateurs de Verifiable Credentials
- Un hébergeur de Verifiable Credentials publics quand cela est nécessaire
- Un vérificateur de Verifiable Credentials permettant la création de challenges (QR codes à scanner) et la réception puis vérification des Verifiable Presentations
- Une version web de wallet pour des acteurs devant gérer une identité commune automatisable

Synthèse

ONE est la tour de contrôle du SDI. Cette application décentralisée permet l'interopérabilité des services de l'écosystème SYL. Elle aura la fonction de wallet d'identité (DID wallet) en stockant les Verifiable Credentials de l'utilisateur et en permettant la diffusion de Verifiable Presentations ainsi que la gestion du token utilitaire.
La possibilité de réaliser un KYC au travers de l'application ONE facilitera grandement la gestion des obligations légales des entreprises soumises à ces obligations, tout en diminuant grandement les coûts.

34 "HD Wallet" : Permet de générer de nombreuses clés privées à partir d'un seul secret initial appelé graine (seed).

DOCUMENT SYL

4. SYL

4.1 CARACTÉRISTIQUES DU SYL

4.1.1 RÉSEAUX

Le SYL est pour le moment un token BEP-20 fonctionnant sur le réseau Binance Smart Chain.

4.1.2 ÉMISSION ET SÉQUESTRE

7 milliards de SYL, divisibles jusqu'à la sixième décimale, ont été mis en circulation. Le montant maximum de SYL en circulation ne dépassera jamais 10 milliards.

3 milliards de SYL ont été placés sous séquestre par XSL Labs en avril 2021.

Ce séquestre à libération progressive a été créé afin de débloquer les 3 milliards de SYL avec une libération par contrat intelligent qui respecte des règles fixes : 60 000 000 de SYL au maximum pourront être libérés du séquestre chaque mois et ce processus pourra être répété plusieurs fois jusqu'à ce que les 10 milliards de SYL soient en circulation.

Le compte séquestre ainsi que les règles immuables de fonctionnement sont librement consultables par le public dans un souci de transparence totale.

4.2 LEGAL OPINION ET CLASSIFICATION DU TOKEN

Pour le moment, trois Legal Opinions ont été formulés, au Japon, à Singapour et à Saint-Vincent-et-les-Grenadines, tous trois donnant au SYL la qualité de "utility token".

4.3 AUDIT

Le Contrat Intelligent du SYL a été audité par le cabinet d'audit Beosin, dont le compte-rendu est disponible sur notre site : xsl-labs.org

4.4 UTILISATION DU SYL

4.4.1 ÉMISSION DE VERIFIABLE CREDENTIALS

Le token SYL est impliqué dans le paiement de certains services (comme l'émission de Verifiable Credentials ou le paiement d' applications).

En effet, comme expliqué précédemment, une fois le SDI de chaque utilisateur créé, ceux-ci ont besoin d'obtenir des Verifiable Credentials qui sont fournis par des émetteurs de confiance. Ils attestent de certaines informations concernant l'identité des utilisateurs. Il peut s'agir d'un KYC (Know Your Customer), d'un diplôme, d'une attestation d'un employeur ou autres.

Afin de récompenser l'utilisation des DID et Verifiable Credentials, un montant en SYL peut être distribué aux utilisateurs lors de la création des premiers SDI, aux émetteurs des premiers Verifiable Credentials, voire à certains vérificateurs.

Aussi, les utilisateurs entre eux pourront s'échanger des Verifiable Credentials en devenant eux-mêmes des émetteurs, créant ainsi un réseau "peer-to-peer" de confiance.

4.4.2 BIBLIOTHÈQUES D'APPLICATIONS

Dans le cas de l'utilisation de l'écosystème XSL Labs par des applications de services tiers, une bibliothèque regroupant l'ensemble de ces applications pourra être mise en place avec la possibilité d'acheter ces applications ou services avec du SYL.

4.4.3 PASSERELLE DE PAIEMENT

Une passerelle de paiement sera développée dans ONE afin de simplifier et d'uniformiser les échanges au sein de celle-ci.

L'uniformisation du moyen de paiement entre tous les utilisateurs permet l'acquisition de Verifiable Credentials, peu importe les devises locales des utilisateurs et émetteurs.

Cette méthode permet de simplifier l'acquisition de Verifiable Credentials pour l'utilisateur. Elle lui donne la possibilité de payer grâce à un portefeuille unique les émetteurs de confiance de Verifiable Credentials commerciaux ou d'autres services payants tout en leur permettant de conserver une traçabilité des transactions effectuées.

4.4.4 CORTEX

Le SYL va s'avérer particulièrement utile lors du lancement du projet Cortex, qui vise à révolutionner le ciblage publicitaire en impliquant fortement le consentement de leur propriétaire et la préservation des données personnelles. Les annonceurs pourront ainsi démarcher de façon ciblée les utilisateurs qui ont consenti à ce démarchage, sans que ceux-ci ne partagent pour autant leurs données personnelles.

Une partie des revenus publicitaires sera aussi partagée directement avec les utilisateurs via un paiement en SYL incitatif. Au-delà des Verifiable Credentials acquis, l'utilisateur pourra aussi ajouter des informations personnelles supplémentaires.

Le litepaper de Cortex verra le jour courant 2022.

Synthèse

Le SYL est le token utilitaire de l'ecosystème SYL. C'est un token BEP-20 fonctionnant sur la Binance Smart Chain. Il sera utilisé dans le cadre de l'émission de Verifiable Credentials, permettra d'accéder à des services utilisant l'écosystème SYL, il pourra également être utilisé comme passerelle de paiement afin de simplifier et d'uniformiser les échanges au sein d'un écosystème pouvant être utilisé par de nombreux pays, utilisant de nombreuses devises différentes.

5. CAS D'UTILISATION

Les sections suivantes décrivent des cas d'utilisation possibles pour le SDI sans viser à l'exhaustivité.

5.1 VISION SDI

XSL Labs s'est associé à l'entreprise Swiss Biometrix[35] pour le développement d'un terminal ThermoVSN qui utilisera la technologie du SDI dans un nouveau réseau appelé Vision SDI afin de sécuriser la gestion des données biométriques de ses utilisateurs.

Le SDI garantit l'anonymat et la sécurité des données personnelles et biométriques, ce qui assure la conformité aux normes RGPD concernant le traitement et le stockage de ces données.

5.2 JEUX VIDÉO

L'utilisation du SDI dans le monde du jeu vidéo modifiera en profondeur l'écosystème vidéoludique. XSL Labs va lancer une première phase d'expérimentation de l'utilisation de son identifiant décentralisé.
Les jeux vidéo multi-joueurs font face à énormément de problèmes liés à l'utilisation de logiciels de triche[36].

L'utilisation de tels programmes tiers est interdite, et entraîne le plus souvent des bannissements chez les joueurs qui y recourent. Un problème se pose cependant, car si le bannissement d'un compte de tricheur rend ce compte définitivement inaccessible, rien n'assure qu'un tricheur ne revienne pas sur le jeu avec un autre compte. Ainsi, toute sanction peut être contournée, et le tricheur invétéré peut librement revenir nuire à l'expérience des autres joueurs. Le SDI pourra être associé à un identifiant anonyme unique permettant de pallier ce problème tout en intégrant diverses fonctionnalités qui ouvriront la voie à une nouvelle expérience utilisateur.

L'identification unique de chaque utilisateur sera possible après une procédure de KYC et rendra effective aussi bien les sanctions à l'égard des joueurs que leurs récompenses.

Aussi, des Verifiable Credentials contenant un historique du joueur pourra permettre aux recruteurs ou à d'autres joueurs d'avoir une connaissance des antécédents positifs comme négatifs de chacun.

Ces Verifiable Credentials pourront également servir à certifier l'expérience des joueurs dans différents jeux, facilitant ainsi le recrutement dans des équipes et guildes.

Il sera également possible sur la base de ces Verifiable Credentials de structurer des équipes en fonction du niveau des joueurs ou encore d'accorder des autorisations de connexions selon son âge, son expérience ou son niveau.

35 Pour plus d'informations : https://swissbiometrix.com

36 Comprenant notamment des fonctions "aimbot", "triggerbot", "wallhack" et "ESP", courantes dans les jeux de type first-person shooter (FPS). De tels programmes analysent les données reçues par le client du jeu afin de permettre la détection d'adversaires par le joueur (wallhack, ESP) et faciliter la visée (aimbot), voire la rendre automatique (triggerbot) ne laissant aucune chance au joueur régulier.

5.3 BILLETTERIE ANTI-FRAUDE

Afin de lutter contre la fraude et le marché noir de la revente, il sera possible pour des sites de billetterie de demander un SDI au client afin de garantir que la personne ayant effectué l'achat est bien la même personne que celle qui assiste au concert.

5.4 APPLICATIONS DE RENCONTRE

Pour renforcer la sécurité sur les sites et applications de rencontre, le SDI pourra jouer un rôle primordial. L'émission d'un KYC sous la forme d'un Verifiable Credential sur le portefeuille d'identité de l'utilisateur de SDI permet d'être certain que le membre qui s'inscrit sur le site ou l'application de rencontre est bien celui qu'il prétend être.

Synthèse

Le SDI est voué à être utilisé par de nombreuses applications et services tiers, notamment le projet Cortex qui vise à révolutionner le mode de partage des données personnelles, le contrôle d'accès biométrique et l'industrie du jeu vidéo. D'autres cas d'usage se développeront au fil du temps, favorisant l'adoption de l'écosystème.

6. MÉDIAS

La liste suivante, non exhaustive, contient des liens vers des médias présentant les projets de XSL Labs.

10.03.2021 - Article en français de CoinTribune
https://www.cointribune.com/blockchain/ecosysteme/xsl-labs-syl-va-utiliser-la-smart-chain-de-binance-bnb

08.03.2021 - Article de U.Today
https://u.today/how-xsl-labs-builds-go-to-ecosystem-for-decentralized-identity-management?amp

26.02.2021 - Article de CoinTelegraph (disponible en plusieurs langues)
https://cointelegraphcn.com/news/the-internet-of-trust-why-secure-digital-identities-are-crucial-to-web-30

17.02.2021 - Article de Tron Weekly
https://www.tronweekly.com/here-how-xsl-labs-revolutionize-digitalidentity

15.02.2021 - Article d'AMB Crypto
https://ambcrypto.com/decentralised-identity-project-in-the-works-at-xsl-labs/

11.02.2021 - Article de Coin Speaker
https://www.coinspeaker.com/xsl-labs-data-identity-security/

15.01.2021 - Article en français du Point, annonçant notre partenariat avec Swiss Biometric
https://partenaires.lepoint.fr/block-chain/partenariat-thermo-vsn-xsl-labs-lutilisation-de-la-blockchain-dans-les-bornes-dacces-biometriques

30.01.2021 - Article en français de 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

JUILLET 2021

• Alpha publique testnet du contrat intelligent SDI sur BSC
• Alpha privée de l'application portefeuille ONE
• Alpha privée d'émetteur de VC de KYC
• Alpha privée des services web d'enrôlement et authentification via VC KYC

SEPTEMBRE 2021

• Alpha privée/Démonstration des services pour l'e-sport (gaming e-reputation)
• Alpha privée du vérificateur en ligne (verifiable presentation avec challenge)
• Alpha privée du vérificateur et hébergement en ligne (verifiable presentation sans challenge)

NOVEMBRE 2021

• Alpha privée des services pour le contrôle d'accès biométrique (démonstration reconnaissance faciale)
• Alpha privée de l'application séparée de vérification des Verifiable Presentations
• Beta publique testnet du contrat intelligent SDI
• Beta privée de ONE
• Beta privée du vérificateur en ligne (Verifiable Presentation avec challenge)
• Beta privée et hébergement en ligne (Verifiable Presentation sans challenge)
• Beta privée d'émetteur de VC KYC
• Ouverture des codes sources des outils pour e-sport
• Ouverture du code des services web d'enrôlement et authentification via VC KYC

JANVIER 2022

• Evaluation du support d'autres technologies "Blockchain"
• Version alpha du service Web + Hardware Security Module (HSM) centralisant les outils de gestion du côté émetteur
• Service alpha de récompenses pour l'utilisation des Verifiable Credentials
• Beta SDK pour intégration dans des applications tierces
• Audits et stress tests

FÉVRIER 2022

• Version 1.0 d'émetteur de VC KYC avec récompenses (KYC SYL Airdrop)
• Service Beta de récompenses pour l'utilisation des Verifiable Credentials
• Version 1.0 publique de ONE
• Version 1.0 publique du vérificateur en ligne (Verifiable Presentation avec challenge)
• Version 1.0 publique et hébergement en ligne (Verifiable Presentation sans challenge)

DEUXIÈME TRIMESTRE 2022

• Services publics commerciaux d'émetteurs de Verifiable Credentials dont KYC
• Version Beta du service Web + HSM centralisant les outils de gestion du côté émetteur
• SDK public pour intégration dans des applications tierces
• Ouverture des codes sources d'intégration d'authentification pour CMS/SSO

TROISIÈME TRIMESTRE 2022

• Version 1.0 du service Web + HSM centralisant les outils de gestion du côté émetteur

À suivre

8. CONCLUSION

Le vol de données est l'un des défis majeurs auquel notre société fait face. Son coût pour les entreprises et par conséquent pour l'économie mondiale est gigantesque et désavantage considérablement leur activité économique.

Les solutions de XSL Labs permettent de lutter efficacement contre ces problèmes. En se basant sur les 10 principes de la Self-Sovereign Identity, XSL Labs développe un identifiant décentralisé, le SDI, qui permet aux utilisateurs de conserver le contrôle sur leur identité et sur leurs données.

L'architecture décentralisée des solutions proposées par XSL Labs permet de limiter la nécessité de conserver des données personnelles sur des serveurs centralisés, tout en renforçant la fiabilité des informations présentées ainsi que l'authentification de leurs propriétaires.

L'application décentralisée ONE qui permet le contrôle du SDI va également simplifier les procédures de KYC (Know Your Customer) et AML (Anti-Money Laundering).

Les services publicitaires de Cortex profiteront aux annonceurs et utilisateurs, permettant de cibler une population d'internautes de manière plus éthique et respectueuse de leur vie privée et leurs données personnelles, tout en les rémunérant en SYL.

Fort de ces nouveaux outils, XSL Labs est résolu à bâtir pour l'avenir un véritable Internet de Confiance, ouvert et collaboratif.

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