The Smart Self-Sovereign Identity: The Power of Autonomy

Abstract - Dans un monde en rapide évolution marqué par l'émergence de technologies disruptives telles que l'intelligence artificielle, la blockchain, les cryptomonnaies et les metaverses, une dichotomie se dessine entre les early adopters technophiles et la majorité de la population, moins au fait de ces avancées. Notre white paper aborde cette problématique en présentant la "Smart Self-Sovereign Identity", une innovation permettant à chaque individu de forger et de gérer facilement une identité numérique autonome. Cette solution vise à intégrer l'ensemble de la population dans l'espace numérique, en fournissant autonomie et accessibilité, sans la nécessité d'une compréhension approfondie des technologies sous-jacentes. Notre objectif est de faciliter l'adaptation à l'espace numérique pour tous, indépendamment de leur familiarité avec la technologie.

Par Benjamin Arthuys, Arno Trigallez, Florent Arthuys, Vincent Fraisse.

Introduction

À l'ère de la numérisation croissante de nos vies et de l'accentuation de la protection des utilisateurs, tel que démontré par des initiatives régionales comme le règlement eIDAS ou eSSIF en Europe, émerge le Smart Self-Sovereign Identity (Smart-SSI), un projet novateur visant à redéfinir notre rapport à la sécurité et à la propriété de l'identité numérique. Alors que le règlement eIDAS 2.0 de la Commission européenne trace la voie vers une identité numérique omniprésente, le Smart-SSI s'inscrit dans cette dynamique en offrant une approche autonome, sécurisée et intuitive pour les utilisateurs, transcendant les frontières de l'Union européenne. En effet, l'évolution technologique offre désormais à notre présence numérique une autonomie et une intelligence renouvelées.

Toutefois, la protection et le contrôle insuffisants de nos données numériques deviennent de plus en plus évidents [1]. Dans cette dynamique, l'intégration d'un nouvel algorithme dans le cadre du Self-Sovereign Identity (SSI), avec ses méthodes cryptographiques associées (comme le zkProof), vise à offrir une véritable prise en charge de la propriété de l'identifiant numérique (DID pour Decentralized Identifier), donnant naissance à des badges certifiants (VC pour *Verifiable Credentials*)[2]. Cette avancée permet de reprendre le contrôle des informations personnelles sans dépendre de tiers centralisés, comme les réseaux sociaux, le cloud ou les sites marchands. Parallèlement, il devient crucial d'accompagner les utilisateurs dans la compréhension et l'utilisation judicieuse de ces *Verifiable Credentials*. L'implémentation d'un nouveau algorithme dans le SSI transforme l'expérience vers ce que nous appelons "Smart Self-Sovereign Identity" (Smart-SSI), révélant ainsi toute la puissance des *Verifiable Credentials* (VC) en analysant intelligemment les données, tout en assurant leur confidentialité et sécurité grâce à zkProof.

Cet essor vise un double objectif : replacer chaque utilisateur au cœur de son expérience, lui fournissant une compréhension approfondie et éclairée de son identité numérique, tout en garantissant la propriété et la sécurité de ses données dans le monde numérique. Cette évolution, axée sur la simplicité d'utilisation, ouvre la voie à une implémentation efficace de l'algorithme dans le SSI, facilitant ainsi une adoption généralisée de cette technologie.

La nécessité d'un nouveau système d'identité

La proposition du Smart Self-Sovereign Identity (Smart-SSI) comme nouveau système d'identité découle de manière évidente des défis critiques de notre ère numérique. Pour preuve, les utilisateurs, qui sont systématiquement contraints de confier la protection de leurs données numériques aux institutions, se trouvent ainsi dans une position compromettant leur capacité à défendre efficacement leur vie privée. Dans ce contexte, l'incertitude quant à l'avenir et l'écart entre la réalité technique et son utilisation individuelle remettent en question la confiance en ces tiers-institutionnels ou privés, particulièrement à l'ère d'émergence de modèles économiques contraignant l'utilisateur à accepter l'exploitation de ses données [3]. L'aspect fondamental du

Smart-SSI réside dans sa capacité à relever simultanément le défi de protéger les utilisateurs tout en simplifiant leur expérience sur internet. Cette démarche est d'autant plus cruciale à la lumière des systèmes d'identité centralisés vulnérables aux attaques, mettant en danger la sécurité des informations personnelles des utilisateurs, sachant que les données numériques sont une cible majeure des cyberattaques [4]. La dépendance envers des tiers centralisés tels que les réseaux sociaux, le cloud et les sites marchands souligne la nécessité de repenser le contrôle des utilisateurs sur leurs propres données.

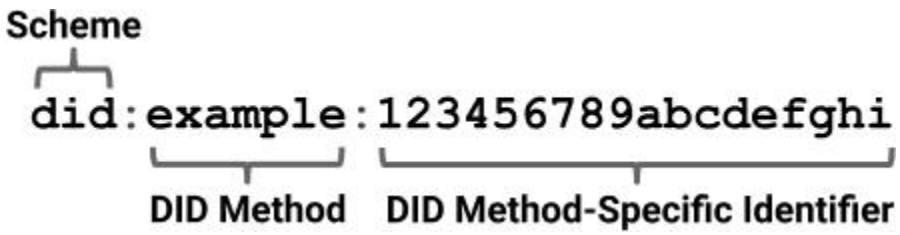
L'introduction du Smart-SSI s'impose comme une compréhension approfondie de ces problématiques vis-à-vis d'une utilisation judicieuse des *Verifiable Credentials* (VC) de sorte à garantir une expérience numérique autonome et personnalisée. Par l'implémentation de l'algorithme dans le SSI qui deviendrait alors le Smart-SSI chaque utilisateur se retrouve au cœur de son utilisation. En ayant comme visée la garantie de ses propriétés (matérialisé numériquement par dans les VC) et leur sécurité. Évidemment, une fois implémenté, le Smart-SSI se fait quasiment invisible pour les utilisateurs, permettant une facilité d'emploi exceptionnelle.

Face aux menaces telles que le deep fake, les citations tronquées hors contexte et l'usurpation d'identité sur les réseaux sociaux, le Smart-SSI souligne l'importance cruciale de l'E-réputation [5]. La difficulté croissante à distinguer le vrai du faux sur Internet, avec un coût estimé à 78 milliards de dollars par an [6], met en lumière l'ampleur des défis liés aux scams et aux fausses informations. Ainsi, au-delà de la sécurisation des données, le Smart-SSI émerge comme une réponse novatrice, relevant le double impératif de protéger les utilisateurs et de simplifier leur expérience en ligne. Ce protocole revêt une importance considérable dans la recherche d'une solution équilibrée entre sécurité et facilité d'utilisation dans l'environnement numérique complexe d'aujourd'hui.

Le standard SSI

Les identifiants décentralisés (DID)

L'identité Auto-Souveraine repose sur l'utilisation d'Identifiants Décentralisés comme l'indique les spécifications actuelles du DID de la W3C :



"Les identifiants décentralisés (DID) sont un nouveau type d'identifiant qui permet une identité numérique vérifiable et décentralisée. Un DID se réfère à tout sujet (par exemple, une personne, une organisation, une chose, un modèle de données, une entité abstraite, etc.) tel

que déterminé par le contrôleur du DID. Contrairement aux identifiants fédérés typiques, les DID ont été conçus de manière à être dissociés des registres centralisés, des fournisseurs d'identité et des autorités de certification. Plus précisément, bien que d'autres parties puissent être utilisées pour aider à découvrir des informations relatives à un DID, la conception permet au contrôleur d'un DID de prouver son contrôle sur celui-ci sans nécessiter la permission d'une autre partie. Les DID sont des URI qui associent un sujet DID à un document DID permettant des interactions fiables associées à ce sujet.

Chaque document DID peut exprimer du matériel cryptographique, des méthodes de vérification ou des services, qui fournissent un ensemble de mécanismes permettant à un contrôleur de DID de prouver le contrôle du DID. Les services permettent des interactions fiables associées au sujet du DID. Un DID peut fournir les moyens de retourner le sujet du DID lui-même, si le sujet du DID est une ressource d'information telle qu'un modèle de données.

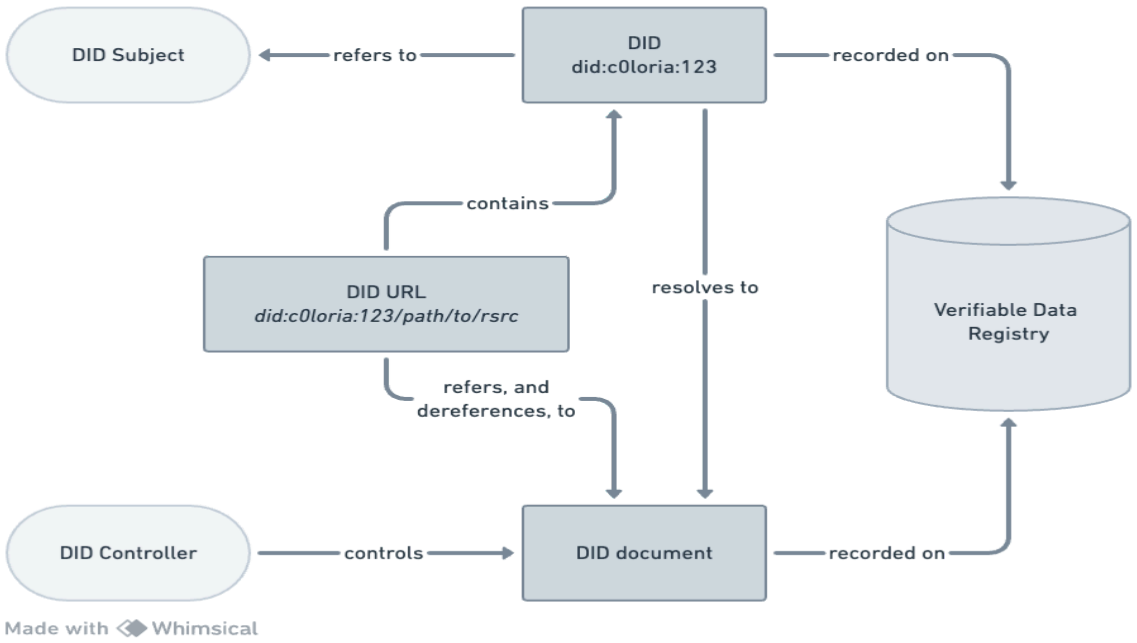
Ce document spécifie la syntaxe des DID, un modèle de données commun, les propriétés de base, les représentations sérialisées, les opérations des DID, ainsi qu'une explication du processus de résolution des DID vers les ressources qu'ils représentent."

Un document DID simple:

```
Unset
{
 "@context": [
  "<https://www.w3.org/ns/did/v1>",
  "<https://w3id.org/security/suites/ed25519-2020/v1>"
 ]
 "id": "did:c0loria:123456789abcdefghi",
 "authentication": [{
  // used to authenticate as did:...fghi
  "id": "did:c0loria:123456789abcdefghi#keys-1",
  "type": "Ed25519VerificationKey2020",
  "controller": "did:c0loria:123456789abcdefghi",
  "publicKeyMultibase": "zH3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"
 }]
}
```

Architecture

L'identité auto-souveraine (SSI) repose sur l'utilisation de DID, des identifiants décentralisés, conformément aux spécifications actuelles du W3C. Le DID, en soi, est simplement un identifiant, enregistré sur une blockchain, mais ne permet pas de lier directement un sujet à des informations sur son identité. Pour cela, il est utilisé en conjonction avec les Vérifiable Credentials (VCs).



Dans notre architecture de Résolution d'URL DID, nous mettons en place un système robuste et interopérable, conforme aux standards émergents de l'identité numérique décentralisée. Au cœur de ce système se trouve l'URL DID, *did:c0loria:123/path/to/rsrc*, qui est un identifiant unique représentant une ressource numérique. Cette URL contient le DID, *did:c0loria:123*, qui est lui-même un identifiant décentralisé faisant référence à un sujet DID spécifique.

Le DID résout vers un document DID, qui est une structure de données contenant des informations essentielles telles que les clés publiques, les méthodes d'authentification et les contrôleurs DID. Ces contrôleurs DID ont l'autorité sur le document DID et peuvent effectuer des modifications.

Enfin, les documents DID sont enregistrés sur un Registre de Données Décentralisé et vérifiable, assurant ainsi l'intégrité et la traçabilité des informations. Cette architecture garantit non seulement la sécurité et la fiabilité des identités numériques mais favorise également leur intégration transparente dans diverses applications et services.

Verifiable Credentials (VCs)

Les VCs, couplés avec le DID, permettent aux tierces parties de vérifier l'exactitude des données liées à l'identité d'un sujet. Comme nous le savons le DID seul, ne suffit pas pour cette vérification; il sert de point d'ancrage pour les VCs. Les VCs peuvent être émis par l'utilisateur lui-même (self-asserted claims) ou bien délivrés par une entité de confiance. L'association entre le DID et les VCs est encryptée et stockée dans une base de données décentralisée type blockchain.

Pour bien saisir le processus nous parlerons de trois acteurs clés :

- l'émetteur (qui délivre les VCs)
- le détenteur (qui possède les VCs liés à son DID)
- le vérificateur (qui, grâce au DID, peut vérifier si un sujet possède les VCs correspondants).

C’est cette structure tripartite qui soutient le modèle d'identité auto-souveraine, dans laquelle les individus contrôlent pleinement leur identité numérique, sécurisée et vérifiable, dans et par, la base de données décentralisée.

En résumé, selon nous les DID et les VCs fonctionnent ensemble et ainsi permettent une véritable vérification de l'identité de manière fiable en accordant aux individus une maîtrise complète et facile de leur identité numérique.

Méthode cryptographique : Zero Knowledge Proof

Pour ce qui est de l’intégration de la méthode cryptographique zkProof dans les systèmes de Self-Sovereign Identity (SSI), c’est d’après nous essentiel afin d’assurer la sécurité et la confidentialité. Puisqu’en préservant l’intégrité des données et en minimisant l’exposition des informations sensibles, la combinaison SSI/ZKP place l’utilisateur au cœur de son système, de sorte à pouvoir justifier l’authenticité d’une information sans pour autant en révéler le contenu. En effet, la non-répudiation, en tant que caractéristique, renforce la sécurité de l'utilisateur en garantissant que les parties tierces, qui authentifient l'utilisation d'une donnée, ne peuvent pas nier cette authentification. Ajouté à cela, son interopérabilité, le zkProofs accentue la qualité du Smart-SSI, au-delà du double caractère sécuritaire et confidentiel, en permettant le partage des données dans différents systèmes entraînant, en plus, la consolidation de celui-ci.

Notez deux points importants à préciser : tout d'abord, pour l'utilisateur, en tant que récepteur, il est le seul à même de décider de l'utilisation du VC, et si nécessaire, de le "burn" (c'est-à-dire de le faire disparaître) lorsqu'il juge que celui-ci n'est plus pertinent pour son Smart-SSI. Ensuite, pour l'émetteur, il est tout à fait possible de révoquer les VC selon les choix de son protocole.

L’intelligence Artificielle au service de la SSI

Comment rendre la SSI intelligente ? C’est à dire capable d’interpréter vos données afin d’en proposer des déductions sur votre identité. En utilisant une double combinaison de techniques d’abord du traitement du langage naturel (NLP) et du Machine Learning (ML) qui permettent de transformer les données issues de diverses applications (réseaux sociaux, apps de musique, apps de sport, etc.) en un ensemble structuré de qualités intrinsèques, sous forme de VC.

Étape 1 : Collecte et Pré-traitement des Données

Les données de vos applications quotidiennes sont collectées. Par exemple, vos posts sur les réseaux sociaux, vos playlists musicales, et vos statistiques d’activité physique. Ces données

sont ensuite normalisées et transformées en tokens (T = {t_1, t_2, …, t_n}), qui sont de petits éléments de texte ou d'information.

Étape 2 : Extraction des Caractéristiques via TF-IDF

Pour chaque token (t_i) dans vos données, nous calculons un poids numérique appelé TF-IDF, qui mesure à la fois la fréquence du token et son importance unique dans l'ensemble des données :

$$TF - IDF(t_i, j) = TF(t_i, j) \times log(\frac{N}{DF(t_i)})$$

Étape 3 : Classification et Extraction des Qualités

Ces vecteurs TF-IDF sont ensuite analysés par un modèle ML, comme un modèle SVM. Le SVM travaille à classer ces vecteurs en différentes catégories, correspondant à des qualités intrinsèques :

$$H: w \cdot x + b = 0$$

Étape 4 : Résultats de l'Algorithme et Création de VCs

L'algorithme produit une liste de qualités intrinsèques, avec des degrés de confiance. Par exemple, "Créativité : 85%", indiquant que les données analysées suggèrent fortement que vous possédez cette compétence. Ces compétences sont ensuite converties en VCs dans votre SSI, offrant une preuve numérique de vos compétences basée sur votre utilisation réelle des applications.

Étape 5 : Validation et Fiabilité

La précision de l'algorithme est mesurée par des scores de validation, tels que la précision :

$$P = \frac{Total\ number\ of\ predictions}{Number\ of\ correct\ predictions}$$

By combining these mathematical and algorithmic methods with in-depth analysis of your personal data from applications, the algorithm offers a sophisticated and personalized digital representation of your intrinsic qualities. This scientific approach ensures that the generated VCs are not only accurate but also meaningful and relevant to your personal profile.

En combinant ces méthodes mathématiques et algorithmiques avec une analyse approfondie de vos données personnelles issues des applications, l'algorithme offre une représentation numérique sophistiquée et personnalisée de vos qualités intrinsèques. Cette approche

scientifique assure que les VCs générés sont non seulement précis, mais aussi significatifs et pertinents pour votre profil personnel.

Scénario d'Utilisation : c0loria

c0loria se présente comme une Application, incarnant l'idéal d'une âme décentralisée, appelée : Digital Soul. Dans son fonctionnement, c0loria intègre le concept Smart SSI, qui permet aux utilisateurs de créer et de gérer leur identité numérique. L'application se distingue d'abord par son interface utilisateur ludique, centrée sur les utilisateurs, de sorte à démystifier l'accès au Web3, que nous savons encore compliqué pour la majorité des utilisateurs d'internet.

L'innovation principale de c0loria réside dans son processus d'analyse des VC, c'est-à-dire des habitudes et comportements en ligne, de l'utilisateur et utilisatrice. La technologie Smart-SSI dans c0loria permet alors aux utilisateurs de créer leur véritable identité réflexive, ce qui ouvre à la possibilité d'avoir accès autonome à sa réflexion numérique. D'où l'emploi du terme "Soul" (âme) qui suggère quelque chose de profond et d'essentiel à chaque individu mais invisibilisé dans nos pratiques *connectées*. En l'associant au digital, cela évoque l'idée d'une réplique numérique ou d'une représentation des sens d'une personne, en lien avec ses compétences, ses intérêts et son comportement digital.

La première interaction de l'utilisateur avec c0loria commence par un questionnaire simple, conçu pour cerner son profil créatif ou son "Âme Créative". Ce questionnaire est le point de départ d'une exploration plus profonde, où l'application utilise les réponses fournies pour orienter l'analyse des données collectées via le Smart-SSI. Ensuite, l'application identifie et valide des compétences spécifiques et des traits de personnalité. Par exemple, nous pouvons penser qu'une interaction fréquente avec des contenus artistiques sur les réseaux sociaux pourrait être interprétée comme un indicateur de créativité ou de curiosité.

Une fois ces qualités intrinsèques identifiées, c0loria les convertit en VC dans le cadre de la SSI de l'utilisateur. Chaque VC représente une compétence ou un trait de personnalité, enrichissant ainsi l'identité numérique de l'utilisateur. Ce processus non seulement aide l'utilisateur à mieux se connaître et à comprendre son identité numérique, mais ouvre également la voie à des opportunités personnelles et professionnelles, en mettant en valeur des compétences et des talents qui pourraient autrement être soit inexploitées, pire exploitées par un tiers comme cela est initialement prévu sur le web.

En conclusion, c0loria est plus qu'une simple application; c'est un guide vers la compréhension de soi à travers le prisme numérique, facilitant l'accès aux technologies décentralisées et la propriété de son identité, tout en offrant une plateforme pour la découverte personnelle et le développement de l'identité numérique.

Conclusion

Nous avons introduit un système d'échanges numériques autonomes, se libérant de la nécessité d'une autorité centrale, grâce à l'utilisation astucieuse de la preuve sans divulgation et d'un réseau pair-à-pair, éliminant ainsi la dépendance à une tierce partie de confiance. En établissant les standards du Smart Self-Sovereign Identity (Smart-SSI), conjointement alimenté par les fonctionnalités du zkProof, des Identifiants Décentralisés (DID) et des Verifiable Credentials (VC), nous avons montré ce que ce protocole offre sur le contrôle de son identité numérique sans pour autant éviter une perte de la compréhension de ses données, alors sauvegardées. C'est pourquoi l'algorithme intégré au cadre du Self-Sovereign Identity (SSI) permet d'assurer la gestion de la propriété de l'identifiant numérique et des Verifiable Credentials (VC), tout en évitant leur perte et préservant ainsi leur pertinence pour leurs propriétaires c'est-à-dire les utilisateurs. Le Smart-SSI fait combiner la preuve sans divulgation pour assurer une confidentialité absolue tandis que les Identifiants Décentralisés offrent une manière sécurisée et autonome de créer, gérer et contrôler son identité numérique. Ajouté à cela les Verifiable Credentials, qui permettent de générer des attestations vérifiables, renforçant la confiance dans l'authenticité des informations partagées. Ainsi, le Smart-SSI offre aux utilisateurs le pouvoir de posséder et de gérer leur identité numérique de manière sécurisée et innovante.

References

[1] AMOR Samy Ben and GRANGET Lucia. "Digital Identity, From Construction to Suicide in 52 Minutes". Les Cahiers du numérique, number 7, January 2011, pp.103-115.

[2] PREUKSAT Alex and DRUMMOND Reed, Self-Sovereign Identity, Decentralized Digital Identity, and Verifiable Credentials, Manning, 2021.

[3] As Shoshana Zuboff reminds us in The Age of Surveillance Capitalism (2018), digital surveillance is an integral part of all our connected activities.

[4] Some examples are given to us about the extreme effectiveness of digital identity theft but more importantly about the advent of a transformation of cybercrime as a space for modifying behavior from fake, namely in our case from false identity, see the article by, MAZZUCCHI Nicolas, "Cyber-conflict and its evolutions, physical effects, symbolic effects", Revue Défense Nationale, 2019/6 (N° 821), pp. 138-143.

[5] For an understanding of the social stakes of deep fake, see GIRY Julien, "Fake news as a concept of social sciences. Attempt to frame from related concepts: rumors, conspiracy theories, propaganda, and misinformation", Questions de communication, 2020/2 (n° 38), p. 371-394.

[6] See,
https://s3.amazonaws.com/media.mediapost.com/uploads/EconomicCostOfFakeNews.pdf ; for a more journalistic approach see,
https://lejournal.cnrs.fr/articles/internet-lautoroute-de-la-desinformation.