The Smart Self-Sovereign Identity: The Power of Autonomy

Abstract - In a rapidly evolving world marked by the emergence of disruptive technologies such as artificial intelligence, blockchain, cryptocurrencies, and metaverses, a dichotomy is forming between tech-savvy early adopters and the majority of the population, who are less aware of these advancements. Our white paper addresses this issue by presenting the "Smart Self-Sovereign Identity", an innovation that allows each individual to easily forge and manage an autonomous digital identity. This solution aims to integrate the entire population into the digital space, providing autonomy and accessibility, without the need for a deep understanding of the underlying technologies. Our goal is to facilitate adaptation to the digital space for everyone, regardless of their familiarity with technology.

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

Introduction

In a context of continuous growth in the dynamism of the digital world and the increasing focus on user protection, illustrated by initiatives such as the eIDAS regulation or eSSIF in Europe, the growing interest in the evolution of digital regulations suggests a reevaluation of our security, set in an international landscape tinged with both passion and divisions. Technological evolution now offers our digital presence renewed autonomy and intelligence. However, the insufficient protection and control of our digital data are becoming increasingly evident [1]. In this dynamic, the integration of a new algorithm within the framework of Self-Sovereign Identity (SSI), with its associated cryptographic methods (such as zkProof), aims to provide genuine management of the ownership of the digital identifier (DID for Decentralized Identifier), giving rise to certifying badges (VC for Verifiable Credentials) [2]. This advancement allows for the regaining control of personal information without depending on centralized third parties, such as social networks, cloud services, or commercial websites. Concurrently, it becomes crucial to accompany users in understanding and wisely using these Verifiable Credentials. The implementation of a new algorithm in SSI transforms the experience into what we call "Smart Self-Sovereign Identity" (Smart-SSI), thus revealing the full power of Verifiable Credentials (VC) by intelligently analyzing data, while ensuring their confidentiality and security thanks to zkProof. This development aims for a dual objective: to place each user at the heart of their experience, providing them with a deep and enlightened understanding of their digital identity, while ensuring the ownership and security of their data in the digital world. This evolution, focused on ease of use, paves the way for an effective implementation of the algorithm in SSI, thus facilitating widespread adoption of this technology.

The Need for a New Identity System

The proposal of Smart Self-Sovereign Identity (Smart-SSI) as a new identity system arises evidently from the critical challenges of our digital era. Users, who are systematically forced to entrust the protection of their digital data to institutions, find themselves in a position compromising their ability to effectively defend their privacy. In this context, uncertainty about the future and the gap between technical reality and individual usage challenge trust in these institutional or private third parties, particularly in the era of emerging economic models compelling users to accept the exploitation of their data. The fundamental aspect of Smart-SSI lies in its ability to simultaneously address the challenge of protecting users while simplifying their experience on the internet. This approach is all the more crucial in light of centralized identity systems vulnerable to attacks, endangering the security of users' personal information, given that digital data is a major target of cyber-attacks. Dependence on centralized third parties such as social networks, cloud services, and online merchants underscores the need to rethink user control over their own data.

The introduction of Smart-SSI emerges as a deep understanding of these challenges regarding the judicious use of Verifiable Credentials (VC) to ensure an autonomous and personalized digital experience. By implementing the algorithm into SSI, which would then become

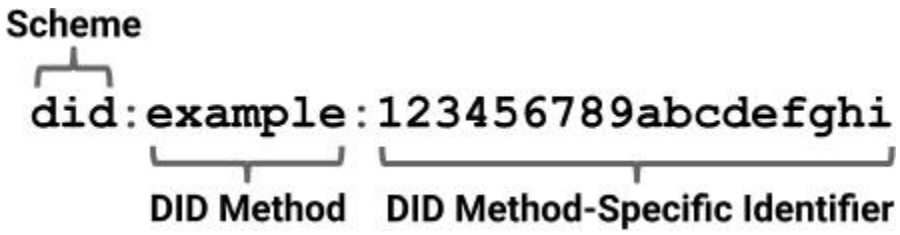
Smart-SSI, each user finds themselves at the core of its usage. With the aim of guaranteeing their properties (digitally materialized in VC) and their securities. Obviously, once implemented, Smart-SSI becomes almost invisible to users, allowing exceptional ease of use.

Facing threats such as deep fakes, out-of-context misquotes, and identity theft on social networks, Smart-SSI emphasizes the crucial importance of E-reputation. The increasing difficulty in distinguishing truth from falsehood on the Internet, with an estimated cost of 78 billion dollars per year, highlights the magnitude of the challenges related to scams and misinformation. Thus, beyond securing data, Smart-SSI emerges as an innovative response, addressing the dual imperative of protecting users and simplifying their online experience. This protocol holds significant importance in the search for a balanced solution between security and usability in today's complex digital environment.

SSI Standard

Decentralized Identifiers (DID)

Self-Sovereign Identity relies on the use of Decentralized Identifiers as indicated by the current W3C specifications:



A simple example of a decentralized identifier (DID)

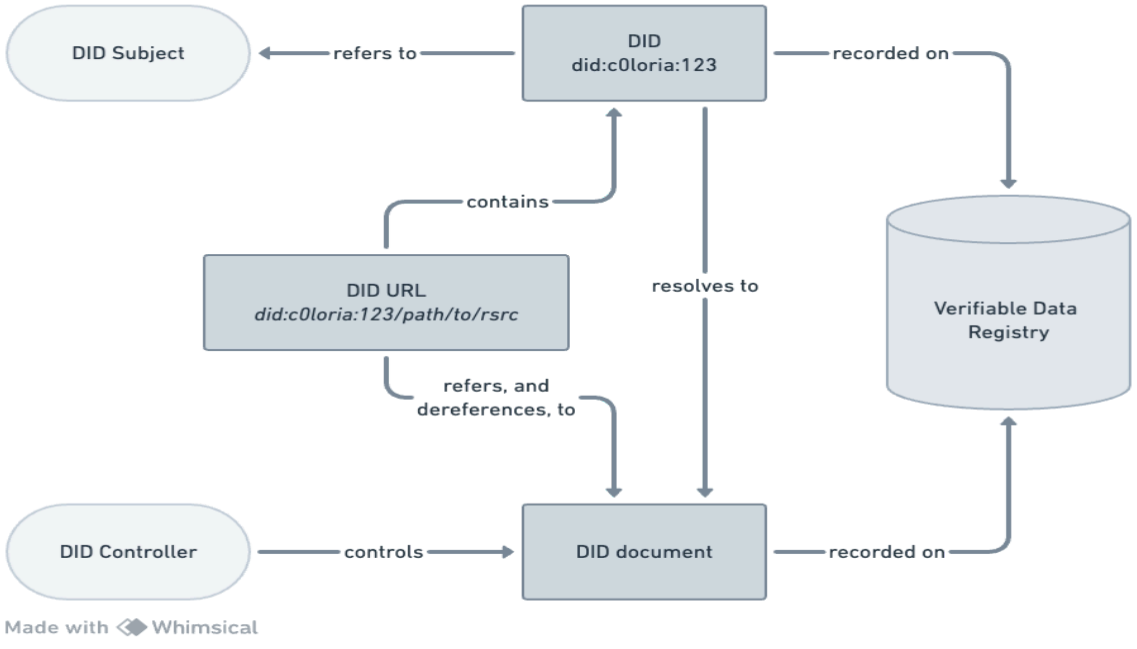
"Decentralized Identifiers (DID) are a new type of identifier that enables verifiable, decentralized digital identity. A DID refers to any subject (e.g., a person, an organization, a thing, a data model, an abstract entity, etc.) as determined by the DID controller. Unlike typical federated identifiers, DIDs have been designed to be dissociated from centralized registries, identity providers, and certification authorities. Specifically, although other parties may be used to help discover information about a DID, the design allows the controller of a DID to prove control over it without requiring permission from another party. DIDs are URIs that associate a DID subject with a DID document enabling reliable interactions associated with that subject. Each DID document may express cryptographic material, verification methods, or services, providing a set of mechanisms enabling a DID controller to prove control over the DID. Services enable reliable interactions associated with the DID subject. A DID may provide means to return the DID subject itself if the DID subject is an information resource such as a data model. This document specifies the syntax of DIDs, a common data model, basic properties, serialized representations, DID operations, as well as an explanation of the DID resolution process to the resources they represent."

A simple DID document:

```
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

Self-Sovereign Identity (SSI) is based on the use of DID, decentralized identifiers, in accordance with current W3C specifications. The DID, in itself, is simply an identifier, recorded on a blockchain, but does not directly link a subject to information about their identity. For this, it is used in conjunction with Verifiable Credentials (VCs).



In our DID URL Resolution architecture, we have implemented a robust and interoperable system, compliant with emerging standards for decentralized digital identity. At the heart of this system is the DID URL, did:c0loria:123/path/to/rsrc, which is a unique identifier representing a digital resource. This URL contains the DID, did:c0loria:123, which is itself a decentralized identifier referring to a specific DID subject.

The DID resolves to a DID document, which is a data structure containing essential information such as public keys, authentication methods, and DID controllers. These DID controllers have authority over the DID document and can make modifications.

Finally, both the DID and the DID document are recorded on a Verifiable Data Registry, ensuring the integrity and traceability of information. This architecture not only guarantees the security and reliability of digital identities but also promotes their seamless integration into various applications and services.

Verifiable Credentials (VCs)

VCs, coupled with DID, allow third parties to verify the accuracy of data related to a subject's identity. As we know, DID alone is not sufficient for this verification; it serves as an anchor point for VCs. VCs can be issued by the user themselves (self-asserted claims) or issued by a trusted entity. The association between DID and VCs is encrypted and stored in a decentralized database such as a blockchain.

To fully understand the process, we will discuss three key actors:

- the issuer (who issues VCs)
- the holder (who holds VCs linked to their DID)
- the verifier (who, through the DID, can verify if a subject possesses the corresponding VCs).

It is this tripartite structure that supports the self-sovereign identity model, in which individuals fully control their digital identity, secured and verifiable, within and by, the decentralized database.

In summary, we believe that DID and VCs work together and thus allow for a true verification of identity in a reliable manner by granting individuals complete and easy control of their digital identity.

Cryptographic Method: Zero Knowledge Proof

Regarding the integration of the zkProof cryptographic method into Self-Sovereign Identity (SSI) systems, we believe it is essential to ensure security and confidentiality. By preserving data integrity and minimizing the exposure of sensitive information, the combination of SSI/ZKP places the user at the heart of their system, allowing them to justify the authenticity of information without revealing its content. Indeed, non-repudiation, as a characteristic, enhances

user security by guaranteeing that third parties, which authenticate the use of data, cannot subsequently deny this authentication. In addition to its interoperability, zkProofs accentuate the quality of Smart-SSI, beyond the dual security and confidentiality aspect, by enabling data sharing across different systems, thus further consolidating it.

Artificial Intelligence in Service of SSI

How to make SSI intelligent? That is, capable of interpreting your data to offer deductions about your identity. By using a double combination of techniques first of natural language processing (NLP) and Machine Learning (ML) that allow transforming data from various applications (social networks, music apps, sports apps, etc.) into a structured set of intrinsic qualities, in the form of VC.

Step 1: Data Collection and Pre-processing

Data from your daily applications are collected. For example, your posts on social networks, your music playlists, and your physical activity statistics. These data are then normalized and transformed into tokens (T = {t_1, t_2, …, t_n}), which are small elements of text or information.

Step 2: Feature Extraction via TF-IDF

For each token (t_i) in your data, we calculate a numerical weight called TF-IDF, which measures both the frequency of the token and its unique importance in the overall data:

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

Step 3: Classification and Feature Extraction

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 :

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

Step 4: Algorithm Results and VC Creation

The algorithm produces a list of intrinsic qualities, with confidence degrees. For example, "Creativity: 85%", indicating that the analyzed data strongly suggest that you possess this skill. These skills are then converted into VCs in your SSI, providing digital proof of your skills based on your actual use of applications.

Step 5: Validation and Reliability

The accuracy of the algorithm is measured by validation scores, such as precision:

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

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.

Use Case: c0loria

c0loria presents itself as an Application, embodying the ideal of a decentralized soul, called: Digital Soul. In its operation, c0loria integrates the Smart SSI concept, allowing users to create and manage their digital identity. The application distinguishes itself first by its playful user interface, centered on users, in order to demystify access to Web3, which we know is still complicated for the majority of internet users.

The main innovation of c0loria lies in its VC analysis process, i.e., user online habits and behaviors. The Smart-SSI technology in c0loria then allows users to create their true reflexive identity, which opens up the possibility of autonomous access to their digital reflection. Hence the use of the term "Soul," which suggests something profound and essential to each individual but invisible in our connected practices. By associating it with the digital, it evokes the idea of a digital replica or representation of a person's senses, linked to their skills, interests, and digital behavior.

The user's first interaction with c0loria starts with a simple questionnaire, designed to understand their creative profile or "creative soul." This questionnaire is the starting point for a deeper exploration, where the application uses the provided answers to guide the analysis of data collected via Smart-SSI. Next, the application identifies and validates specific skills and personality traits. For example, we might think that frequent interaction with artistic content on social networks could be interpreted as an indicator of creativity or curiosity.

Once these intrinsic qualities are identified, c0loria converts them into VCs within the user's SSI. Each VC represents a skill or personality trait, thus enriching the user's digital identity. This process not only helps the user better understand themselves and their digital identity but also opens up opportunities for personal and professional growth, by highlighting skills and talents that might otherwise be either untapped or worse, exploited by a third party as originally intended on the web.

In conclusion, c0loria is more than just an application; it is a guide to self-understanding through the digital prism, facilitating access to decentralized technologies and ownership of one's identity while offering a platform for personal discovery and digital identity development.

Conclusion

We have introduced a system of autonomous digital exchanges, freeing itself from the need for a central authority, through the clever use of non-disclosure proof and a peer-to-peer network, thereby eliminating dependence on a trusted third party. By establishing the standards of Smart Self-Sovereign Identity (Smart-SSI), jointly powered by Zkproof, Decentralized Identifiers (DIDs), and Verifiable Credentials (VCs), we have shown what this protocol offers in terms of controlling one's digital identity without avoiding a loss of understanding of one's data, then safeguarded. This is why the algorithm integrated into the Self-Sovereign Identity (SSI) framework ensures the management of digital identifier ownership and Verifiable Credentials (VCs), while avoiding their loss and thus preserving their relevance for their owners, i.e., the users. Smart-SSI combines non-disclosure proof to ensure absolute confidentiality while Decentralized Identifiers offer a secure and autonomous way to create, manage, and control digital identity. Added to this are the Verifiable Credentials, which allow for the generation of verifiable attestations, reinforcing trust in the authenticity of shared information. Thus, Smart-SSI offers users the power to own and manage their digital identity securely and innovatively.

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.