Enhancing Security in User-Centered Authentication using KERI

Biagio Boi
dept. of Computer Science
University of Salerno
Fisciano, Salerno, Italy
bboi@unisa.it

Marco De Santis
dept. of Computer Science
University of Salerno
Fisciano, Salerno, Italy
mdesantis@unisa.it

Christian Esposito
dept. of Computer Science
University of Salerno
Fisciano, Salerno, Italy
esposito@unisa.it

***Abstract*—In the context of the widespread adoption of user-centric authentication methods, safeguarding the confidentiality of private keys during the exchange of credentials has become a critical concern. Key Event Receipt Infrastructure (KERI), distinguished by its distinctive design focusing on key events and receipts, aligns seamlessly with the ethos of user-centric authentication, eschewing the necessity for blockchain integration. This research leverages the architectural model of KERI to discern potential implications within the contemporary landscape of Self-Sovereign Identity (SSI) ecosystems, thereby contributing to the evolution of identity management practices. The need for this research arises from the recognition that while SSI obviates the need for central authorities, thereby augmenting privacy and security, the imperative to preserve and securely store private keys persists. Our primary findings confirm that the integration of KERI within the SSI ecosystem provides a more resilient protocol for authentication by preventing the exchange of any kind of key used for the generation of the proof. This approach aims to prevent attacks in line with the principles of decentralization and trustlessness inherent in blockchain technologies. This research contributes to the expanding body of literature devoted to security and access management within the dynamic realm of user-centric applications and authentication.**

***Index Terms*—Authentication, Web Authentication, User-Centric Authentication, Key Event Receipt Infrastructure (KERI), Security.**

I. Introduction

Authentication has always been a critical component when considering a system. Over the last few years, these mechanisms have changed frequently in order to increase the security and privacy of users. Nowadays, federated authentication, and in particular Single Sign On (SSO) can be intended as a standard, where OpenID Connect (OIDC) [1] is continuously expanding.

The main advantages of using federated authentication are related to the way in which user data are managed, especially relevant for the medical context [2], where data stored are particularly sensitive. In this mechanism, the service demands authentication and identity management tasks from an external service, which is responsible for authenticating users over multiple services. Despite the advantages of this approach, which does not require storing credentials on each service server, there are some privacy and security flaws that must be taken into account. Authentication Server (AS) can be seen as a single point of failure, compromising the availability and security of users data [3]. Such an approach takes the name of *administrative root-of-trust*, where there is one party responsible for the issuance of certificates, and users must rely on this party to verify and store their private keys.

User-centric authentication tries to prevent these attacks by putting the user at the center of the authentication procedure. Namely, the user is the only one responsible for managing his identity, typically leveraging Hardware Security Modules (HSMs) or Public Key Infrastructure (PKI) authentication. HSM and PKI typically use a server to assess credential validity, which creates new possible issues on the Certificate Authority (CA) side. A relevant and upcoming means for authenticating users in a completely decentralized manner is the paradigm of Self-Sovereign Identity (SSI), whose commercial solutions have already been deployed. Among these solutions, some of them leverage the so-called *algorithmic root-of-trust*, where the user relies on external parties, such as nodes within the blockchain who certificate the credentials. It is clear that such an approach is more advanced w.r.t. administrative root-of-trust, but some criticalities still exist, considering the dependence on these nodes responsible for certifying the identity. If we consider the verification nodes as a permissioned blockchain, then we may have problems related to scalability and costs [4]; while if we have a permissionless blockchain, assessing the genuinity of the nodes may be critical, and in some cases, such as the 51% attacks, they may disrupt the validity of the consensus protocol.

SSI uses Decentralized Identifiers (DIDs) for representing the identity of the user and a DID Document is associated with such an identifier for the verification of the identity. Depending on the specific implementation of SSI, it may decide to implement a *self-certifying root-of-trust*, where there are no external parties responsible for certifying the identity of the users. Currently, the majority of existing DID Methods, use a distributed ledger for the verification of the identity, which does not follow the paradigm of *self-certifying root-of-trust*. On the contrary, a small slice of these DID Methods, correctly implements the paradigm, but since there is no authority for managing credentials, it is possible that a user will completely lose the private key associated with the wallet. It is clear that in such an approach, it is not possible to use such an identity, or, more critically, an attacker can use such a key for performing attacks.

KERI [5] tries to give a complete solution to the problem of *self-certifying root-of-trust* using an approach where the users are directly responsible for the credentials and for the key pairs released. Moreover, it proposes a mechanism for producing key rotation, which can be particularly relevant for the credentials released using the SSI paradigm without the need for having a blockchain as a method for assessing the identity and validity of credentials. In particular, the approach introduces a new perspective on identity management, where the user is the only one responsible for managing his identity. The current paper first analyzes the approach proposed by KERI and then implements KERI-based verification in traditional SSI systems. The major contribution can be summarized as follows:

- Exploit the KERI ecosystem in order to evaluate the feasibility and possible combination with SSI-based authentication. The article will analyze each component of KERI to underline its benefits and potential.
- Analyze possible improvements to existing security measures within the context of user-centered authentication. By leveraging KERI, the authors offer a new system for enhancing the security of SSI-based authentication.
- Propose an identity revocation system for a non-blockchain based SSI system. Recalling that revocation is hard to implement without a ledger empowered by a blockchain, we propose KERI as a means for introducing revocation in these systems.
- Evaluate the proposed approach using the STRIDE attack model, highlighting the inherence and security of the protocol and paving the way for future security analysis against SSI-based authentication.

The document is structured into five sections. The second describes related work on security mechanisms for enhancing user-centric authentication. The third section offers a background and a general introduction to the KERI framework, describing the main components. The fourth section introduces the proposed architecture, highlighting the relevant components and offering a primary security analysis of the system. The fifth and last section concludes the work by discussing the main advantages of adopting such architectures and providing insights about future works.

II. Related Works

User-centric authentication increases privacy by moving user data away from centralized servers [6]. In the beginning, this kind of authentication was intended as a physical characteristic that users hold, such as biometric characteristics (face, fingerprint, iris), achieving good results when combining them [7] for authentication [8]. Despite being a secure mechanism for identifying users within a system, these mechanisms, in some cases, expose sensitive information. SSI tries to solve these issues by offering the user a mechanism for reliably demonstrating identity [9]. SSI is implemented through the mechanism of Verifiable Credentials (VCs), which creates a trust triangle between the Issuer, Holder, and Verifier. A trust triangle can be managed using a shared registry that contains information on public-facing claims or using cryptographic signatures applied on credentials that prove the identity [10]. The greatest part of commercial solutions such as Sovrin [11], or uPort [9] uses a distributed ledger for managing the identity of the user and publishing or revoking the credentials. A huge challenge in these approaches is related to the scalability of the architecture [12], which typically involves the usage of permissioned blockchain for protecting the network from attacks. Additional challenges are related to the legal aspects, where a study conducted over the Belgian case [13], highlights the criticality of blockchain technology (BCT)-based systems with respect to current GDPR normative.

BCT-less solution, instead, solves the problem of scalability and compliance with GDPR but creates new challenges from the point of view of revocation [14]. Without the adoption of a distributed ledger, it is difficult to manage revocation in efficient and reliable way. In [15], a distributed attestation revocation is employed for gossiping the revocation of the credentials in all the networks, but this is bound to the capacity of the network to spread the information.

Distributed Key Management Infrastructure (DKMI) paved the way for managing revocation in BTC-less SSI systems, where secure key management in distributed environments is a critical challenge. Numerous studies and implementations have helped outline the challenges and solutions in this context, providing a solid knowledge base for continued progress. The study by J. Van Der Merwe et al. [16] proposes a new threshold-multi-signature scheme that combines the properties of group-oriented signature schemes with threshold and multiple signature schemes. The main goal of the work is to present a secure and efficient signature scheme that allows a threshold of group members to collaboratively sign an arbitrary message. In contrast to group signatures with a threshold, in this scheme, the individual signatories do not remain anonymous but are publicly identifiable through the information contained in the multi-signature with a valid threshold. In [17], the authors present an interesting decentralised identity verification framework, confirming the feasibility of BTC-less approaches.

Different from the previous investigation in this context, our work wants to provide a fully decentralized mechanism for managing revocation and enhancing the security of user-centric authentication, and in particular, SSI. Moreover, comparing this approach to [17], our aim is to provide a simple schema for enhancing authentication instead of modifying the definition of the SSI protocol. Such mechanisms leverage new distributed technology such as KERI, which can provide a schema that automatically revokes and generates new key pairs at each usage, enhancing the communication and exchange of

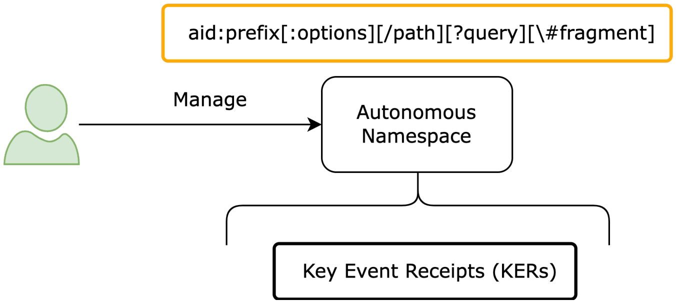
aid:prefix[:options][/path][?query][\#fragment]
Manage
Autonomous Namespace
Key Event Receipts (KERs)

Fig. 1. KERI Arichitecture

credentials without the use of BCT.

III. Key Event Receipt Infrastructure (KERI)

As KERI [5] establishes a cryptographic link between an identifier and a pair of keys, there is no requirement for any additional source of trust beyond the controller who has generated the keys and consequently holds the private key. This is why KERI makes a significant contribution to Decentralized Key Management: it enables every digital wallet used by a controller to perceive itself as a self-certifying root of trust in any context. In the current section, the main components of KERI architecture are discussed, depicted in Figure 1.

A. Autonomic Namespace

The Autonomic Namespace (AN) is self-certifying and, hence self-administrating identifier. It is a namespace with a self-certifying prefix that allows so-called Autonomous Decentralized Key Management, where the users are the only one responsible for the creation of a key pair and do not depend on any third party. Each AN identifier includes a prefix, which is the public key that is uniquely derived.

$$aid : prefix[: options][/path][?query][\#fragment] \quad (1)$$

An AN is a way to create distinct and isolated spaces within the KERI system. Each AN operates independently, managing its own cryptographic keys, events and key state machine. Such an approach fully metch the concept of SSI by offering an self-sovereigned space owned by the users, where each of them is responsible for the operation performed over the key. Moreover, the approach agree with the scalability of the system since there is no central authority responsible for tracking users. The AN structure completely matches that defined by the Decentralized Identifier (DID), which is typically used in SSI. In the following subsections, we will refer to AN, as DID.

B. Event Message

KERI is able to track every event performed over the cryptographical key. Common event types include *ICP (Inception)*, *ROT (Rotation)*, *IXN (Interaction)*, *DIP (Delegation inception)*, and *DRT (Delegation rotation)*, among others. The decentralized event message management approach completely meets the SSI requirements, making the users directly responsible for storing these messages. Each message is signed by the user using the private key so that everyone can assess the validity of a chain of events. Once a new event is generated, it is disseminated to all the participants of the networks to advertise the variation on the key. The users can answer this message using the Key Event Receipts (KER), which is a signed acknowledgment of the variation. These special receipts are needed to verify that a given node of the network, at a given time, has received the event message. Considering the case of decentralized consensus, such dissemination can be used for enhancing the reliability of a key, or the trustworthiness of a node. KERI aims to provide complete decentralized trust, which increases together with the widespread of KERs.

C. Key Rotation

The key rotation process begins with the creation of an Event Message specifically for key rotation. This Event Message is of the *ROT* type, and it represents the intention of updating the key material associated with the cryptographic key. The participant initiating the key rotation signs the *ROT* Event Message with the current key being rotated. As all the event messages, it is disseminated among all the nodes of a network, which can answer to the message with a KER. Upon answering to ROT Event Message, other participants or witnesses verify the cryptographic signature to confirm its authenticity and authority. This ensures that the key rotation request is legitimate. The interested parties update key material associated with the cryptographic key in order to remove from the memory the old key. In such a schema, every interested party of the system will be acknowledged of released key and in the meanwhile can authenticate the usage of the new key.

IV. Proposed Architecture

KERI unlocks the potential for having a root-of-trust individually managed by users. On the contrary, SSI offers the possibility of having verifiable credentials signed from issuers which is possible to present to the verifier and obtain access to resources. Considering the infrastructure offered by KERI, it is possible to have a secure and fully decentralized authentication system. It adheres to the principles of decentralization and trustlessness, enhancing security and user control over their digital identities. Adopting DID enhances the user-centric approach, making the user directly responsible for the key released starting from that decentralized identifier. In the current section, an overview of the proposed system is discussed, focusing on the relevant operations required for reliable decentralized authentication within the context of SSI. In the current section, an overview of the proposed system is discussed, focusing on the relevant operations required for reliable decentralized authentication within the context of SSI.

A. Design and Objectives

The proposed approach uses the previously defined credentials as in the traditional SSI system, but with the addition of KERI in order to manage the exchange of credentials. As depicted in Figure 2, the system use the distributed database

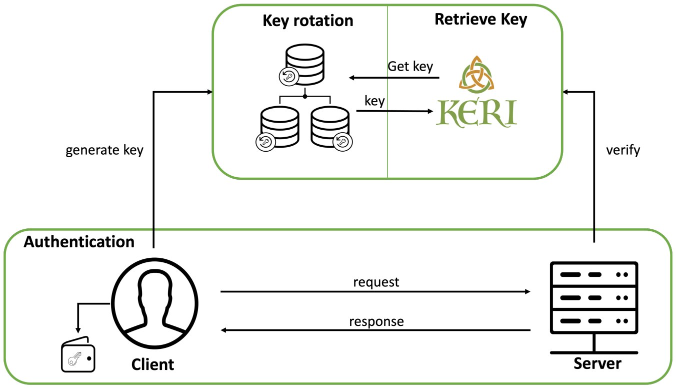

Fig. 2. Overall Architecture

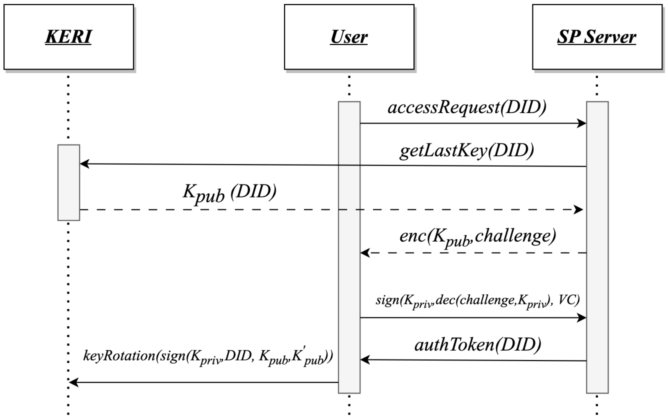

Fig. 3. Flow diagram of proposed authentication procedure

offered by KERI for managing the authentication of the user, which stores credentials in his wallet. Verifiable Credentials (VCs) use DIDComm protocol for exchanging credentials, but without giving any specification for the specific implementation of this protocol, it can be really insecure and subject to cyber-attacks with the aim of stealing sensitive information. Our architecture wants to enhance SSI architecture by protecting credentials both at storage and exchange. In particular, the following requirements can be defined:

- **R1**: Protect exchange between client and server: VCs and VPs are exchanged between holder and verifier without a specific protocol, which can lead to possible identity spoof or MITM attacks.
- **R2**: Protect user wallet: VCs are stored in the user wallet, and by using the user DID it is possible to assess the ownership of the credentials, which means that if the user loses access to the wallet or loses the private key, his credentials can be used without any possibility of revocation.

KERI fully meets our requirement; in particular, R1 can be achieved using self-certifying root-of-trust in combination with classical asymmetric authentication based on a digital signature. R2, instead, can be achieved using key rotation, which offers fresh key pairs whenever needed, and by using the KERs mechanism, it is possible to acknowledge all the Service Provider (SP) of this issuance.

B. Key Management

The user owns two key pairs at each time; let such keys be $[(K_{pub}, K_{priv}), (K'_{pub}, K'_{priv})]$. These keys are derived using the user AN, which is by definition a namespace with a self-certifying prefix. In such a space, the user can release new key pairs each time that belong only to a single namespace and can only be issued by the owner. Every time the user wants to rotate the key, a procedure of substitution of the key occurs:

1) The user emits a *ROT* message, which represents the intention of updating the key material. In particular, such a message contains the new K'_{pub} and is signed with the previous key K_{priv}.
2) The nodes of the KERI verify the signature to confirm that the request is legitimate and answer the *ROT* message.
3) The user removes the older key pair (K_{pub}, K_{priv}) from the key management application and only stores the (K'_{pub}, K'_{priv}) key pair.
4) The user generates a new key pair (K''_{pub}, K''_{priv}), that is not possible to use until a new key rotation.

Notice that the step involved in (4) can be done before (1) if we want to produce a new key as soon as we perform the key rotation. For the purpose of this research, we consider these keys to be stored in a local space, such as a key management application, but different approaches based on mobile applications can be used and adapted for the key management role. According to Figure 3, the described rotation occurs each time the user authenticates on a Service Provider (SP) server. Such rotation will prevent the possible usage of the message that will be exchanged on the communication, namely of Verifiable Credential (VC) in the case of SSI. Moreover, in the case of the compromise of the K_{priv}, do not authorize the attacker to perform future authentication using the same key since it is not more valid due to the KERs mechanism. In particular, the attacker must be able to break the KERI mechanism while the user is ciphering the message using the key.

C. Challenge and VC Exchange

The credential exchange began with a challenge exchange between the SP server and the user. The SP server uses the K_{pub} associated with the user DID for encrypting a challenge. In particular, the SP server will generate a message containing this challenge and will cipher it using the K_{pub} of the user. In such a way, the only party able to decrypt the message will be the owner of K_{priv} associated with the encryption key. At this point, the user will be able to decrypt the challenge and extract it from the received message. According to Figure 3, this challenge will be used for creating a new message that will be ciphered using K_{priv}. The message contains the challenge and the VC used in the traditional approach. If the user shows the credential that are suitable for SP then the server will provide a token for the user.

D. Key Rotation and Revocation

Once the user completes the authentication, a key rotation event will be generated, and the used key will be erased. In a typical authentication flow, the user does not need to revoke the credentials and can proceed with a simple key rotation using the described mechanism. This phase is the most important of the entire process since it communicates to the distributed database and to the entire KERI network the revocation of the used key and the issuance of a new key. In the event that an attacker gains access to a wallet containing the credentials, it is not possible to use such credentials since they do not have access to the private key associated with the newly issued public key. Moreover, if the user feels that the current public key has been compromised, they can publish a new rotation and revoke the credentials. The overall architecture works since the verifier will ask the holder to provide a sign on the challenge following the described protocol.

E. Distributed System

The identity of the user is completely represented by a DID. In the context of KERI, a DID is referred to as the AN, which, as introduced in the previous section, is a self-certifying and self-administrating identifier. By using a so-implemented DID, it is possible to assess if the current public key belongs to a specific user. Taking into account the nature of AN, it is possible to create groups of users within a system, creating relationships between users. In the proposed approach, each user is identified through his DID, and the authentication procedure involves the use of KERI as an authentication means for producing key rotation events and certifying the event message needed for establishing new key pairs. This approach enables the extension of the architecture to the distributed system, where multiple DIDs can be released from the administering AN. It is possible to imagine root AN as a local root-of-trust able to produce new identities, and then the identities are able to produce and manage by themselves the identity released.

F. Security Analysis

Referring to Figure 3, the overarching process primarily revolves around the utilization of a key pair, denoted as (K_{pub}, K_{priv}), essential for implementing pre-authentication within a standard Self-Sovereign Identity (SSI) system. Key rotation events are employed to update these keys each time a user seeks access to a service. By adopting this approach, the user generates new key pairs for every authentication, effectively mitigating the risk of key compromise. In alignment with the STRIDE attack model, a preliminary analysis of the proposed methodology is feasible. Spoofing threats are mitigated through asymmetric encryption. Specifically, the proposed approach employs a form of session key for transmitting VC and VP through an unsecured channel. The SSI architecture safeguards against credential tampering. Credentials are securely stored with a key during issuance, rendering them impervious to compromise as they are transmitted securely using the proposed protocol. Non-repudiation is consistently addressed within the proposed architecture through the application of digital signatures during message exchange. Additionally, enhancing non-repudiation can be achieved by incorporating timestamps into the message signatures. Asymmetric encryption plays a pivotal role in preventing information disclosure. The credentials, encrypted using this method, thwart any unauthorized party from deciphering attribute values unless they are the intended recipient. Distributed denial-of-service attacks are thwarted by the decentralized architecture provided by KERI. This architecture contributes to consensus decentralization, making it arduous to execute a distributed denial-of-service attack. Elevation of privilege is curtailed through the AN system. This system permits only higher nodes (in the descent) to release credentials and sign new identities. The user wallet is fortified against attacks, while the adoption of the key rotation mechanism introduced in the preceding section. Traditional credentials are stored in crypto wallets, encrypted using a private key from the user's end.

V. Conclusion

The adoption of SSI signifies a practical stride towards enhancing security in user-centric authentication. Leveraging advanced technologies like KERI and its effective key rotation mechanism positions us to strengthen data protection within a realistic framework. This mechanism not only furnishes secure keys but introduces a crucial layer of security essential for autonomous and reliable identity management.

Within this framework, KERI assumes a significant role, underscoring its practical importance in fortifying the security of user-centric authentication. However, looking ahead to the future of SSI, it's evident that a measured approach is necessary to assess authentication performance and refine security. While KERI's key rotation serves as an initial improvement, ongoing innovations and developments are crucial to ensuring a progressively secure and dependable user-centric authentication experience.

Looking ahead, there is an urgent necessity to explore advanced methodologies meticulously for the evaluation of SSI performance. The ever-evolving landscape of online threats necessitates a proactive approach to uphold system security. Subsequent developments should be directed towards the implementation of sophisticated measures, addressing not only performance assessment but also the meticulous refinement of the intricate security aspects inherent in SSI. A persistent commitment to research and development assumes paramount importance in ensuring the continual evolution of a secure and self-sovereign digital identity environment. In this regard, the adoption of a measured approach becomes indispensable for the ongoing assessment of authentication performance and the meticulous refinement of security measures. It is imperative to acknowledge that while the initial implementation of KERI's key rotation represents a significant advancement, continuous innovations remain essential for a progressively secure and reliable user-centric authentication experience.

Acknowledgements

This work was partially supported by project SERICS (PE00000014) under the NRRP MUR program funded by the EU - NGEU.

References

[1] D. Recordon and D. Reed, "Openid 2.0: A platform for user-centric identity management," in *Proceedings of the Second ACM Workshop on Digital Identity Management*, ser. DIM '06. New York, NY, USA: Association for Computing Machinery, 2006, p. 11–16. [Online]. Available: https://doi.org/10.1145/1179529.1179532

[2] S. Kumar, A. K. Bharti, and R. Amin, "Decentralized secure storage of medical records using blockchain and ipfs: A comparative analysis with future directions," *Security and Privacy*, vol. 4, no. 5, p. e162, 2021.

[3] L. Lesavre, P. Varin, P. Mell, M. Davidson, and J. Shook, "A taxonomic approach to understanding emerging blockchain identity management systems," *arXiv preprint arXiv:1908.00929*, 2019.

[4] Y. Kwon, J. Liu, M. Kim, D. Song, and Y. Kim, "Impossibility of full decentralization in permissionless blockchains," in *Proceedings of the 1st ACM Conference on Advances in Financial Technologies*, 2019, pp. 110–123.

[5] S. M. Smith, "Key event receipt infrastructure (keri)," *arXiv preprint arXiv:1907.02143*, 2019.

[6] V. Parmar, H. A. Sanghvi, R. H. Patel, and A. S. Pandya, "A comprehensive study on passwordless authentication," in *2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)*. IEEE, 2022, pp. 1266–1275.

[7] A. Tarannum, Z. U. Rahman, L. K. Rao, T. Srinivasulu, and A. Lay-Ekuakille, "An efficient multi-modal biometric sensing and authentication framework for distributed applications," *IEEE Sensors Journal*, vol. 20, no. 24, pp. 15 014–15 025, 2020.

[8] G. Dahia, L. Jesus, and M. Pamplona Segundo, "Continuous authentication using biometrics: An advanced review," *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, vol. 10, no. 4, p. e1365, 2020.

[9] N. Naik and P. Jenkins, "uport open-source identity management system: An assessment of self-sovereign identity and user-centric data platform built on blockchain," in *2020 IEEE International Symposium on Systems Engineering (ISSE)*, 2020, pp. 1–7.

[10] Čučko and M. Turkanović, "Decentralized and self-sovereign identity: Systematic mapping study," *IEEE Access*, vol. 9, pp. 139 009–139 027, 2021.

[11] N. Naik and P. Jenkins, "Sovrin network for decentralized digital identity: Analysing a self-sovereign identity system based on distributed ledger technology," in *2021 IEEE International Symposium on Systems Engineering (ISSE)*. IEEE, 2021, pp. 1–7.

[12] A. Freitag, "A new privacy preserving and scalable revocation method for self sovereign identity–the perfect revocation method does not exist yet," *arXiv preprint arXiv:2211.13041*, 2022.

[13] S. Mahula, E. Tan, and J. Crompvoets, "With blockchain or not? opportunities and challenges of self-sovereign identity implementation in public administration: Lessons from the belgian case," in *DG. O2021: The 22nd Annual International Conference on Digital Government Research*, 2021, pp. 495–504.

[14] A. Hoess, T. Roth, J. Sedlmeir, G. Fridgen, and A. Rieger, "With or without blockchain? towards a decentralized, ssi-based eroaming architecture," in *Proceedings of the 55th Hawaii International Conference on System Sciences (HICSS)*, 2022.

[15] R. Chotkan, J. Decouchant, and J. Pouwelse, "Distributed attestation revocation in self-sovereign identity," in *2022 IEEE 47th Conference on Local Computer Networks (LCN)*, 2022, pp. 414–421.

[16] J. Van Der Merwe, D. S. Dawoud, and S. McDonald, "A fully distributed proactively secure threshold-multisignature scheme," *IEEE Transactions on Parallel and Distributed Systems*, vol. 18, no. 4, pp. 562–575, 2007.

[17] A.-S. Shehu, A. Pinto, and M. E. Correia, "Spidverify: A secure and privacy-preserving decentralised identity verification framework," in *2023 International Conference on Smart Applications, Communications and Networking (SmartNets)*. IEEE, 2023, pp. 1–7.