Improve Wallet Interoperability and Federation in Blockchain-Based User-Centric Authentication for Healthcare*

Biagio Boi[1,*], Franco Cirillo[1], Marco De Santis[1] and Christian Esposito[1]

[1]University of Salerno, Via G. Paolo II 132, Fisciano, 84084, Italy

Abstract

The continuous enhancement and extensive digitalization of medical services have raised various challenges regarding security and privacy. Among these, authentication is one of the most critical, considering identity spoofing and weak passwords. Recently, novel authentication methods such as user-centric authentication are trying to solve the problem by moving identity data and relative claim verification away from a centralized identity manager. When turning this paradigm into the medical domain, it is needed to encompass that not all users are equal, but certain classes are characterized by precise privileges with respect to authentication, such as doctors that must be prioritized over patients. Moreover, it is unfeasible to impose a single technology and infrastructure within an ecosystem characterized by current medical applications; therefore, multiple different solutions need to coexist. In this paper, we discuss a novel framework able to cope with the interoperability, backup and restore of Blockchain-based Self-Sovereign Identity (SSI) wallets. We particularly evaluated the system in a medical context by outlining the different roles of holders with related wallet typologies. Our approach demonstrates its feasibility through the use of a shared registry and smart contract that can smoothly work with two kinds of wallet implementation in a federation of issuers and verifiers.

Keywords

User-centric authentication, Verifiable Credentials, Medical Authentication

1. Introduction

In the continuous evolution of digital applications in the medical domain, the need for robust identity management solutions has never been more pressing. With each passing day, the threat of data breaches looms large, casting a shadow of uncertainty over the integrity of personal information, especially in sensitive areas such as medical records. In this situation, the traditional

TDI 2024: 2nd International Workshop on Trends in Digital Identity, April 9, 2024, Rome, Italy

*This is the author's version of the work. It is posted here for your personal use. Not for redistribution. The paper has been presented at the 2nd International Workshop on Trends in Digial Identity. Personal use of this material is permitted. Permissions must be obtained for all other uses, in any current or future media, including reprinting / republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

*Corresponding author.

†These authors contributed equally.

bboi@unisa.it (B. Boi); fracirillo@unisa.it (F. Cirillo); mdesantis@unisa.it (M. De Santis); esposito@unisa.it (C. Esposito)

0000-0003-3044-5345 (B. Boi); 0009-0006-9599-5996 (F. Cirillo); 0009-0004-6514-4168 (M. De Santis); 0000-0002-0085-0748 (C. Esposito)

centralized approach to identity and claim management systems has come under intense scrutiny. Recently, novel authentication methods rely on delegation to ease the usability for non-expert or impaired users [1], but this may cause the issue of user profiling because it could result in the delegate engaging in malicious actions by exploiting the acquired data. To overcome these problems, novel authentication means have been proposed with the help of hardware devices. The concept of password-less authentication and more in general of mechanisms based on *Proof of Possession (PoP)* started to take place in almost all contexts, including the medical one, though the usage of Hardware Security Module (HSM)[2]. By eliminating the reliance on easily compromised passwords, this approach not only enhances security but also streamlines the user experience, making access to critical medical information more seamless and intuitive. This new approach well aligns with the concept of Self-Sovereign Identity (SSI)[3]. Empowering individuals with the ability to assert and verify their identities without the need for intermediaries, SSI represents a paradigm shift towards greater autonomy and control over personal data. By leveraging cryptographic principles, SSI ensures that individuals retain ownership of their digital identities, mitigating the risks associated with centralized authority. Moreover, SSI aligns seamlessly with the principles of Verifiable Credentials (VCs)[4], offering individuals the ability to securely manage and share self-verifiable attributes. Through the use of cryptographic properties, VCs enable individuals to selectively disclose pertinent information while maintaining privacy and confidentiality. Anyway it's essential to recognize that in the medical context not all users bear the same level of responsibility. For instance, the role of physicians and doctors is paramount and should be prioritized over patients. Consequently, physicians should have stronger authentication measures, as the compromise of their identity carries a more significant impact, whereas patients may have less stringent requirements. This consideration leads to the conclusion that imposing a single technology and infrastructure within a medical ecosystem is not feasible. Various approaches exist for managing SSI wallets, which serve as the sole component necessary for storing credentials in almost all SSI-based solutions. Typically, the relationship between privacy and information security is further reinforced by integrating biometrics within SSI wallets. Technologies like fingerprint scans, facial recognition, and voice recognition offer unique physiological or behavioral identifiers that authenticate users and safeguard access to their SSI wallets, thereby reducing the risk of unauthorized access. Biometric data is directly tied to the individual and is less susceptible to compromise or theft compared to traditional passwords or PINs. On the contrary, these wallets often employ QR code-based authentication procedures, posing challenges for parties with limited time to complete such processes, such as doctors. Healthcare professionals are accustomed to traditional identity verification methods and access to medical records, which typically involve centralized systems and familiar procedures. Introducing new technologies like SSI wallets necessitates substantial education and training to ensure healthcare professionals can use them effectively and securely [5]. Additionally, SSI requires users to locally store the credentials used for identification. While this enhances privacy, it also presents challenges for users who frequently change devices, such as doctors who often switch devices used for access.

In this paper, we exploit existing SSI solutions to provide a definite solution to credentials restore and distinguish different kinds of users based on their responsibilities. The proposed solution also enhances the participation to the protocol from the parties, such as the doctors, that currently use hardware-based mechanism for the verification of the ownership of a VC.

Rather than having to remember complex passwords or undergo time-consuming authentication processes, doctors can simply insert their USB device into a computer or mobile device to securely access their SSI wallet. This streamlined authentication process saves time and reduces potential frustration for busy healthcare professionals.

The key contributions of the current manuscript are listed below:

- Propose an interoperable authentication framework in the medical context that is able to authenticate all parties w.r.t. their needs using user-centric authentication.
- Demonstrate the feasibility of a federative context where multiple hospitals collaborate to enhance trust and reliability.
- Provide a smart contract-based system able to provide backup and restore features to Verifiable Credentials (VCs) through the use of a Trusted Platform Module (TPM).

The rest of the paper is structured as follows: Section 2 provides background on the need for robust identity management solutions in the medical domain. In Section 3, the proposed interoperable authentication framework for user-centric authentication in the medical context is discussed. Section 4 explores the implementation of a federated approach to authentication among multiple hospitals, ensuring interoperability and data sharing, along with the smart contract-based system for backup and restore features to Verifiable Credentials (VCs) using a Trusted Platform Module (TPM). Section 5 delves into the advantages and challenges of the proposed architecture. Finally, Section 6 concludes the paper by summarizing the key findings and contributions in user-centric authentication and interoperability in the medical domain.

2. State of The Art

Decentralization in the medical domain has demonstrated its efficiency through multiple applications [6], with the most relevant ones being patient-centric health information [7] and blockchain-based solutions [8]. These solutions aim to remove the necessity for a centralized server where users' data are stored. Despite these advancements in data management solutions, some solutions still leverage centralized or federated authentication, which, if not developed securely, may potentially lead to illegal access [9, 10]. User-centric authentication is paving the way for a more secure paradigm for identifying patients [11]. However, considering the different use cases where SSI can be applied, there is a need to make these multiple solutions interoperable and always available, in both terms of time and space. Focusing our research on the second layer of SSI, identified as *Communications and Interfaces* in [12], it is possible to better understand which are the current limitations of existing solutions. A Communication protocol in SSI context is defined by DIDComm [13], which offers transport-agnostic, flexible, and interoperable communication. This protocol is currently implemented in a huge number of solutions, guaranteeing a good level of interoperability among different solutions. Transitioning the SSI paradigm into the medical domain necessitates wallets with enhanced functionalities compared to traditional contexts. Through our analysis, two primary requirements have surfaced: **wallets interoperability** [14] and the ability to **restore credentials**.

Wallets interoperability addresses the need to transcend the constraints imposed by a singular user definition [15]. The existence of multiple wallets enables tailored solutions for different

use cases, accommodating the diverse needs of various stakeholders within the system. Technical interoperability, crucial for seamless communication and information exchange among different software entities, remains paramount. Noteworthy efforts have been made to achieve interoperability across various wallets and technologies, as evidenced by recent discussions [16].

In device-sharing contexts or contexts where users frequently change devices to authenticate in a system, the credentials restore is another crucial point to make SSI available in any space and at any time. This is clearly difficult to award if we consider that credentials are typically stored on a single device, without any duplicates. This aspect highlights the importance of a mechanism to restore credentials seamlessly to ensure continuous access to essential services and information. Backup and restore mechanisms are currently implemented in commercial solutions such as Sovrin [17] uses a kind of social backup through the usage of custodians; while uPort [18] uses a smart contract as a mechanism for swapping private keys. In [19] an auditing service has been defined in conjunction with a distributed ledger which is able to promote new users and restore credentials. All the described mechanisms are based on the loss of the private key associated with the wallet, however, in our use case, the challenge lies not in key loss, but in seamlessly transitioning between devices for doctors who maintain control over their keys. Existing solutions, while effective in other domains, may not directly translate to the medical scenario, which involves diverse actors interacting with a shared registry. Our proposal aims to address this specific challenge by focusing on the implementation of each role within the medical ecosystem, along with their interactions and backup mechanisms. Instead of dealing with key loss, our solution will prioritize the seamless transfer of credentials between devices used as temporary or long-term wallets by doctors.

3. Proposed System

This section illustrates how the medical context employs SSI-based Decentralized Identifiers (DIDs) and VCs to award user-centric authentication. Considering the complexity of the medical domain, these parties operate at different levels, all awarding the decentralized authentication. This procedure necessitates an evaluation of their roles concerning the security equipment. Given the current focus of the work, which is to deploy interoperable solutions among all parties in the trust triangle, we will relax some technical details about the issuer and verifier's cryptographic wallet used while focusing more on the various typologies of cryptographic wallets owned by the holders and their interoperability.

3.1. Overview

The overarching system depicted in Fig. 1 delineates the hospital's role as the issuer of credentials and a web-based platform as the verifier. This platform, situated within the hospital's infrastructure, serves as the operational hub housing pertinent patient information. Aligned with the trust triangle paradigm, all involved parties necessitate interaction with a shared registry to facilitate user-centric authentication processes, encompassing the issuance, verification, and revocation of credentials. Central to our proposed system is the critical challenge of ensuring interoperability across diverse cryptographic wallet types, specifically hardware-based

and mobile wallets. Currently, multiple implementations exist for the creation of SSI solutions, but we have to consider that none of them gives us direct interoperability with heterogeneous wallets. In fact, most of the solutions offer a single way of providing wallets, which can be a desktop or a mobile wallet. Some experimental solutions, instead leverages IoT devices to offer authentication. In what follows, we want to cover this aspect by exploiting the security motivation behind the imperative for dual wallet implementations, along with a comprehensive analysis of the system components and possible technologies implementing interoperability. Finally, a practical demonstration showcasing the implementation of an access control system grounded in this model will be provided.

3.2. Scenario

Alice arrives at a hospital due to issues related to diabetes. Upon Alice's arrival at the hospital, she presents her identification documentation to the triage staff. Meanwhile, in the hospital's backend infrastructure, a robust authentication mechanism is at play to ensure secure access to Electronic Health Records (EHR). Dr. Bob, specializing in diabetes management, recognizes Alice's need for immediate attention. To provide effective care, Bob must access Alice's medical history stored in her EHR. However, accessing this sensitive information requires adherence to strict authentication protocols. Bob, like all healthcare professionals, possesses credentials issued by the hospital. These credentials, serving as his digital identity within the healthcare system, are fundamental to accessing patient records. When Bob attempts to log in to the platform, his credentials are verified through a secure authentication process. Once Bob identity is confirmed, the platform checks his authorization level. As a diabetes specialist, Bob is granted access to relevant medical records related to Alice's condition. This authorization verification ensures that Bob can only view information pertinent to his area of expertise, safeguarding patient privacy and confidentiality. In addition to facilitating access to medical records for healthcare professionals like Dr. Bob, the platform also offers a user-friendly interface for patients like Alice to engage with their EHR. Through the platform's patient portal, Alice gains the ability to review her medical history, upcoming appointments, and any prescriptions issued by Dr. Bob or other healthcare providers across different hospitals. Empowered by her mobile wallet, Alice can seamlessly access and navigate her EHR, ensuring a user-friendly experience. The mobile wallet serves as her digital gateway to the platform, providing convenient access to critical health information at her fingertips.

3.3. Roles Definition

The entities involved in a typical medical system bear various responsibilities. For instance, a physician should possess the capability to access patient data pertinent to their specialty while being restricted from accessing the data of other patients. Furthermore, given the critical role of physicians, stringent access control measures must be ensured. We delve into the three roles implicated in SSI-based authentication, which find applicability within a medical framework.

The *issuer* assumes the responsibility for issuing new Verifiable Credentials (VCs), establishing a schema, and potentially executing the revocation of issued VCs. In our scenario, hospitals are regarded as autonomous issuers. They maintain a wallet integrated into the platform,

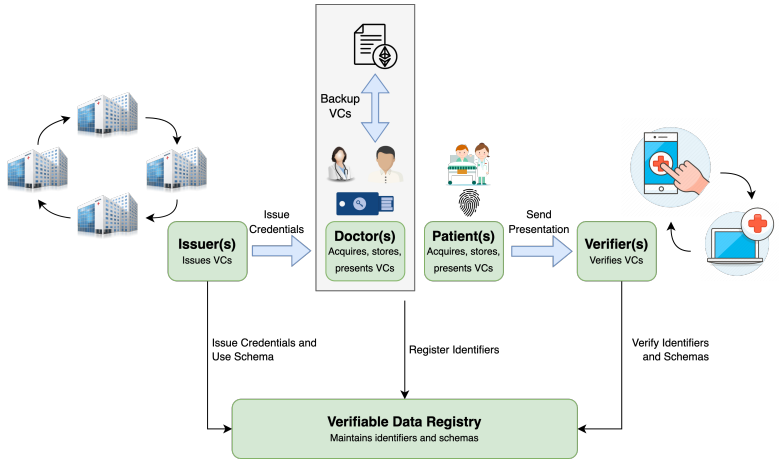

Figure 1: Proposed system based on SSI trust triangle data model.

enabling them to issue credentials to patients seeking access to the platform, thereby mitigating the involvement of malicious nodes. This approach also facilitates the depiction of hospital federation, wherein hospitals are enlisted to participate in the system either by other hospitals already authorized or by the System Administrator (SA). As we will introduce later in this section, the issuer is also responsible for releasing new keys to the doctors, needed for the authentication procedures. By now, we identify the hospitals with a unique public decentralized identifier DID_h^i associated with an asymmetric key pair $ID_h^i = (K_{pub}, K_{priv})$. We do not focus on the technical implementation of these keys, but simply suppose that these keys are connected to the DID, and securely managed by the owner. We refer to the set of hospitals authorized to the release of new credentials as $H = \{DID_h^1, DID_h^2, ..., DID_h^n\}$. Moreover, depending on the type of wallet and on the nature of the user (which as said, can be a doctor or patient), will check for the needed requirement and then release the credentials.

The *holders* of our system can be both patients and doctors, acting with different wallets, depending on their responsibilities and priority in the system. As depicted in Fig. 1 there are two holders:

- Patient(s) - Constituting the typical users of the proposed system, patients are tasked with receiving information from doctors within a hospital setting. Not confined to a singular hospital, patients possess the ability to authenticate across multiple platforms. A feasible means of categorizing patients involves the utilization of the Tax Identification (ID) code, which serves as a unique identifier within a federated system, thus transcending individual system boundaries. Given the imperative for patients to access the system at their discretion and from various devices, the facilitation of authentication through a mobile wallet proves advantageous. Furthermore, considering the ubiquity of mobile devices among patients, it is reasonable to assume the presence of an identity management application tasked with receiving credentials from the respective hospital(s). A backup system it is not needed since the users can always ask to the physical hospital to re-issue the credentials in order to access the system.

- Doctor(s) - Representing the most critical component of the proposed system, doctors engage with the system at a heightened frequency relative to patients. Given the exigencies of their professional obligations, doctors are unable to feasibly engage in authentication procedures reliant upon QR codes and mobile applications, as necessitated by patient data flows. Moreover, owing to the fluidity of doctors' work arrangements and the potential for device turnover, the adoption of a robust backup system becomes imperative for credential retrieval across disparate wallets. In this context, the employment of FIDO2 keys emerges as a viable means of doctor authentication within the medical system, with authentication predominantly facilitated through desktop-based wallets.

According to the description given in the scenario, the role of *verifier* is depicted by the platform used for managing EHR, such as the hospital platform. We suppose that this platform is a decentralized data management platform able to manage all the EHRs from the patients. Notice that it is also possible to consider a federation of verifier, where each platform store the data coming from a single patient and connect with the other with purpose-specific API. As it is conceivable that a federation comprising multiple hospitals adopts the proposed system for the release of credentials, the same is true for the verification platforms housing the comprehensive medical records of their respective patient cohorts. Under this framework, each hospital proffers its individualized platform, all of which are underpinned by a unified identification system, thereby ensuring seamless interoperability and data sharing among disparate healthcare entities. This party, as in the general SSI framework request Verifiable Presentation (VP) to the users to authenticate for the resources available in the system. At the end of this section we will exploit a role-based system for the access control of a medical system.

3.4. Patients Wallet

Patient(s) are normal users of the system, with no responsibilities in the system because they cannot influence other users as doctors can instead accomplish this. Anyway, such users must be able to protect their data, as well as the credentials needed for access to the platform. A well-established platform is Credo.js, which offers all the support for interacting with a distributed ledger and provides all the tools needed for securing communication. As depicted in Fig. 2 we developed a mobile application able to perform all the tasks required by the platform, requiring the users to access it using the biometric source (i.e. face, fingerprint), depending on the device in which the application is installed. On the left side of Fig. 2 we show the standard procedure used to accept proposals for new VCs. This procedure entails users scanning a QR Code for connection establishment and subsequently either accepting or rejecting proposals for new VCs. Once the user stores the credentials in his wallet, it is possible to use them for authentication on the platform. Likewise, as shown in the right side of Fig. 2, users can access services by initiating connections with the service provider and awaiting requests for Verifiable Presentations (VPs). As it is possible to notice, once the VP has been received by the patient, it can be both accepted or rejected. Moreover, by looking at the top of the right side, it is possible to notice a case where the service is asking the user to provide a VP about non-existing credentials, blocking access. This authentication method aligns with the familiarity of the majority of users, particularly considering that the national authentication system relies on QR Codes.

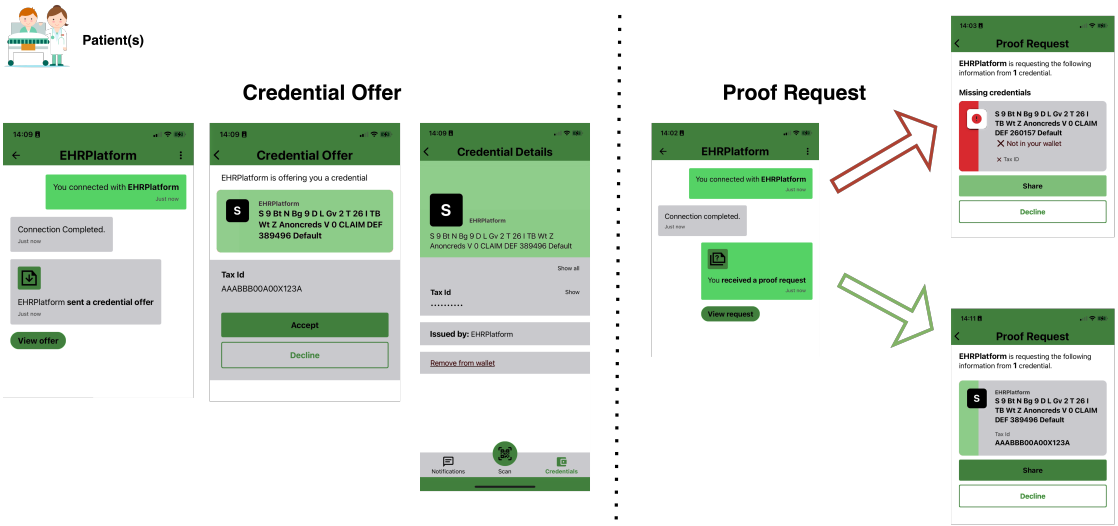

Figure 2: Interaction between patient and mobile wallet

3.5. Doctor Wallet

Despite presenting a valuable solution for identity management, mobile wallets are not recommended for the role of doctors. As we can imagine, within a hospital, doctors do not care about mobile phones and do not have enough time for the authentication procedure, or more critically change the device. We demonstrated that the QR Code-based approach requires much more time and actions by the users (i.e. scan the QR Code, accept the request, and so on). Doctors, instead, already trust the service, which is the platform used within the hospital, and do not need to check for the VPs before releasing credentials. To be more clear, the doctors will always connect with the same hospital, without requiring to change hospitals or to check for which hospital is asking the credential.

In light of the motivation explained, we adopted a Trusted Platform Module (TPM) able to protect the key pairs used in the SSI ecosystem. Each doctor will leverage this module for the authentication procedure. A typical TPM used in the context of authentication is the FIDO2 hardware key. As depicted in Fig. 3, the doctors hold a key that is used for the authentication procedure. By going deeper in analyzing the proposed approach, we outlined a desktop wallet instead of a mobile wallet. The key difference between these two systems is the usage of a single device as a multiple wallets container. In this way, a single desktop computer may be used by multiple doctors who will authenticate themselves with a different key.

This is possible through the usage of Veramo SDK, which offers the possibility to manage multiple wallets in one device through the encryption of this wallet with a custom key. Let the doctor hold a single key pair associated with the FIDO2 device, and define it as $ID^i_{doc} = (K_{pub}, K_{priv})$. The private key will be used by the desktop wallet to both generate a public DID for the wallet and the encryption of the associated wallet, as well as encrypt the credentials. In this way, more than a single doctor can access a desktop and authenticate itself in the system.

To perform the authentication as illustrated in Fig. 3, the enrollment procedure requires that

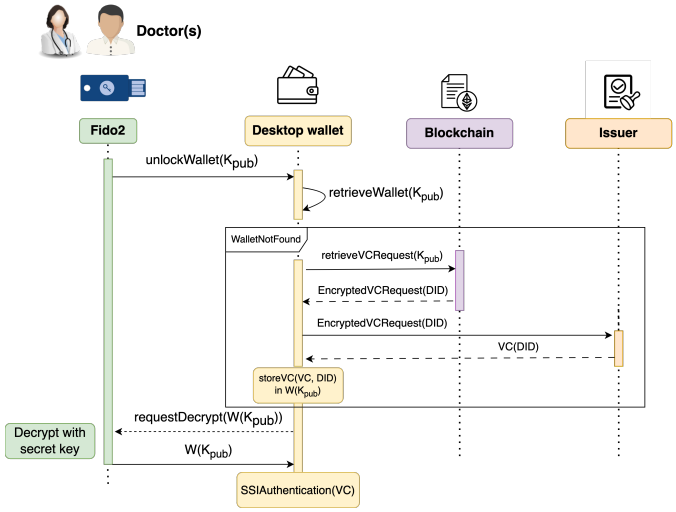

Figure 3: Interaction between doctor and desktop wallet

when a new doctor is taken by the hospital, then a FIDO2 key will be given to him. This choice efficiently solves the problem of identify the doctors across multiple platforms. To be more precise, this also solves the problem related to the backup. If the user loses the wallet or changes the desktop then he also misses the credentials contained in it. In what follows we will give a detailed explanation of this backup system that has been described as WalletNotFound alt in Fig. 3. If the user has already logged in on a computer, the desktop wallet has already been recovered and should only be unlocked. This is easily done by sending the cyphered wallet to the user, which by pressing the button on the FIDO2 key will be able to decrypt the wallet with the related secret key. As soon as he finishes the session, will remove the FIDO2 key, and the wallet will be again locked, waiting for a new key to authenticate.

3.6. VCs Backup

As introduced, it is hard to consider that doctors use a single desktop, which is used by only one doctor. Doctors typically use desktop computers in exchangeable ways and frequently change machines. When this happens from the patient side, there is no problem since they will be able to ask for new credentials without impacting the overall availability of the system. When this is turned on in the case of doctors, a challenge arises since they may not be able to ask the issuer for the release of a new credential in a timely way.

In Fig. 3, we depicted an alternative flow when a doctor uses a desktop without his credentials saved on a wallet. The proposed approach uses a smart contract for the retrieval of credentials previously released by the issuer. To be more precise, each time the issuer releases a new FIDO2 key, it then registers into the blockchain a new record. By looking at Fig. 4, we defined a mapping between a public address and a string named *addressToEncryptedUrl*. This mapping allows the issuer to map a credential release request to a given user wallet associated with the FIDO2 key by leveraging the key generation function. To prevent attacks we decided to encrypt

```
contract CredentialManager {
address public owner;
mapping(address => bool) public isIssuer;
mapping(address => bytes32) public addressToPublicKey;
mapping(address => string) public addressToEncryptedUrl;

modifier onlyOwnerOrIssuer() {
        require(msg.sender == owner || isIssuer[msg.sender], "Only owner or
issuer can call this function");
_;
}

event AddressAdded(address indexed ethAddress, bytes32 publicKey,
        address indexed addedBy);
event AddressRemoved(address indexed ethAddress, address indexed removedBy);
event CredentialMapped(address indexed ethAddress,
        string encryptedUrl, address indexed mappedBy);

AddressList public addressList;

constructor() {
        owner = msg.sender;
        isIssuer[msg.sender] = true;
        addressList = new AddressList();
}
```

```
function addAddress(address ethAddress, bytes32 publicKey)
 public onlyOwnerOrIssuer {
        addressToPublicKey[ethAddress] = publicKey;
        addressList.addAddress(ethAddress);
        emit AddressAdded(ethAddress, publicKey, msg.sender);
}

function mapCredential(address ethAddress, string memory encryptedUrl)
public onlyOwnerOrIssuer {
        require(addressToPublicKey[ethAddress] != 0, "Address not
authorized");
        addressToEncryptedUrl[ethAddress] = encryptedUrl;
        emit CredentialMapped(ethAddress, encryptedUrl, msg.sender);
}

function retrieveCredential(address ethAddress)
public view onlyOwnerOrIssuer returns (string memory) {
        require(bytes(addressToEncryptedUrl[ethAddress]).length > 0, "No
credential mapped for this address");
        return addressToEncryptedUrl[ethAddress];
}


function removeAddress(address ethAddress)
public onlyOwnerOrIssuer {
        delete addressToPublicKey[ethAddress];
        delete addressToEncryptedUrl[ethAddress];
        emit AddressRemoved(ethAddress, msg.sender);
}

function updateIssuer(address issuer, bool isIssuerAllowed)
public onlyOwnerOrIssuer {
        isIssuer[issuer] = isIssuerAllowed;
}
```

Figure 4: Smart Contract used for the recovery of the issue credential request

the credential issue URL with the K_{pub} stored in the key so that only the real owner can decrypt the content using the K_{priv}. When the wallet retrieves the credential request, it can proceed with the recovery by automatically receiving the credential from the issuer.

4. Discussion

One of the key challenges in implementing a decentralized authentication system in the medical domain is ensuring interoperability and federation among various stakeholders, including hospitals, healthcare providers, and patients. To address this challenge, our proposed system adopts a federated approach, wherein multiple hospitals use the proposed trust triangle to release credentials and authenticate users. Each hospital acts as an independent issuer within the federation, responsible for issuing and managing credentials for its respective patients and healthcare providers. However, users are able to change hospitals and to demonstrate their identity in a new platform through the usage of a Verifiable Data Registry (VDR), which is at the basis of the trust triangle. The proposed system well adapts to the needs of each party of the systems by using a different approach for managing the identities of the users. To ensure seamless technical interoperability, our system implements standardized protocols and data formats for credential exchange and verification. This interoperability has been made possible by using an SSI implementation able to cope with multiple wallet representations. In fact, we implemented our system by leveraging Credo.js from patients side and Veramo SDK from doctors side. Both implementations communicate with a shared VDR which is supported by Cosmos. This VDR takes the name of Cheqd and tries to solve the problem of interoperability, by supporting semanthical interoperability. Additionally, our system leverages the Cosmos ecosystem to facilitate interoperability among different cryptographic wallet types and platforms. By adopting a modular and extensible architecture, we enable seamless integration with existing healthcare systems and third-party applications, allowing for easy adoption and scalability. Furthermore, our federated approach to authentication enables patients to access healthcare

services across multiple hospitals using a single set of credentials. This not only simplifies the user experience but also enhances security by centralizing credential management and reducing the risk of credential misuse or duplication. Through the use of DIDs, which are unique and intrinsically linked to the identity of an individual or entity; it is not possible to replicate or duplicate a party. Each DID is unique and uniquely represents the specific identity associated with it. This fundamental feature ensures the integrity and uniqueness of identities in the context of credential management and decentralized authentication. Suppose the doctor's DID is represented as follows: $DID_{\text{doctor}} =$ did:example:1234... This DID is unique and uniquely represents the doctor's identity in the system. This ensures that the system is secure and unique for both patients who have their own wallets in their devices and for doctors who keep it associated with the hardware security module (HSM). Furthermore, the smart contract mapping mechanism ensures secure credential management by establishing a link between users' wallet addresses and encrypted URLs. This ensures only the issuer can access the original URL and be able to release the VC. Clearly, if a malicious node tries to get the VC of a doctor, it will not be possible since VCs are encrypted with the public key of the original owner.

5. Conclusion

Decentralization of medical systems presents a promising avenue for enhancing efficiency, security, and patient-centricity in healthcare. Throughout this paper, we have explored the role of user-centric authentication, considering all the parties involved in a traditional application within the medical domain. These innovations aim to shift away from traditional centralized authentication models towards more secure and transparent systems. Further enhancements to the proposed system are related to the integration of other parties, such as Internet of Medical Things (IoMT) devices, as new holders able to perform sensing tasks. More fine-grained access control may be considered for the access of doctors to the platform. Finally, the introduction of eIDAS wallet must be taken into account when designing future SSI-based authentication.

Acknowledgements

This work was partially supported by project SERICS (PE00000014) under the NRRP MUR program funded by the EU - NGEU and by the project "DHEAL – COM- Digital Health Solutions in Community Medicine" under the Innovative Health Ecosystem (PNC) - National Recovery and Resilience Plan (NRRP) program funded by the Italian Ministry of Health.

References

[1] U. Khalil, A. Ahmad, A.-H. Abdel-Aty, M. Elhoseny, M. W. A. El-Soud, F. Zeshan, Identification of trusted iot devices for secure delegation, Computers & Electrical Engineering 90 (2021) 106988.

[2] M. A. Khan, I. U. Din, T. Majali, B.-S. Kim, A survey of authentication in internet of things-enabled healthcare systems, Sensors 22 (2022) 9089.

[3] A. Preukschat, D. Reed, Self-sovereign identity, Manning Publications, 2021.

[4] J. Sedlmeir, R. Smethurst, A. Rieger, G. Fridgen, Digital identities and verifiable credentials, Business & Information Systems Engineering 63 (2021) 603–613.
[5] M. Shuaib, S. Alam, M. S. Alam, M. S. Nasir, Self-sovereign identity for healthcare using blockchain, Materials Today: Proceedings 81 (2023) 203–207.
[6] H. Taherdoost, The role of blockchain in medical data sharing, Cryptography 7 (2023) 36.
[7] Y. Zhuang, L. R. Sheets, Y.-W. Chen, Z.-Y. Shae, J. J. Tsai, C.-R. Shyu, A patient-centric health information exchange framework using blockchain technology, IEEE Journal of Biomedical and Health Informatics 24 (2020) 2169–2176. doi:10.1109/JBHI.2020.2993072.
[8] A. Dubovitskaya, F. Baig, Z. Xu, R. Shukla, P. S. Zambani, A. Swaminathan, M. M. Jahangir, K. Chowdhry, R. Lachhani, N. Idnani, et al., Action-ehr: Patient-centric blockchain-based electronic health record data management for cancer care, Journal of medical Internet research 22 (2020) e13598.
[9] U. Khalil, O. A. Malik, M. Uddin, C.-L. Chen, A comparative analysis on blockchain versus centralized authentication architectures for iot-enabled smart devices in smart cities: A comprehensive review, recent advances, and future research directions, Sensors 22 (2022). URL: https://www.mdpi.com/1424-8220/22/14/5168. doi:10.3390/s22145168.
[10] Z. A. Khattak, S. Sulaiman, J.-L. A. Manan, A study on threat model for federated identities in federated identity management system, in: 2010 International Symposium on Information Technology, volume 2, 2010, pp. 618–623. doi:10.1109/ITSIM.2010.5561611.
[11] A. Constantinides, M. Belk, C. Fidas, A. Pitsillides, Design and development of a patient-centric user authentication system, in: Adjunct Publication of the 28th ACM Conference on User Modeling, Adaptation and Personalization, 2020, pp. 201–203.
[12] A. Satybaldy, M. S. Ferdous, M. Nowostawski, A taxonomy of challenges for self-sovereign identity systems, IEEE Access 12 (2024) 16151–16177. doi:10.1109/ACCESS.2024.3357940.
[13] D. D. Commun.WG, Didcomm messaging v2.1 editor's draft, 2023.
[14] H. Yildiz, A. Küpper, D. Thatmann, S. Göndör, P. Herbke, A tutorial on the interoperability of self-sovereign identities, 2022. arXiv:2208.04692.
[15] Z. E. Ansaroudi, R. Carbone, G. Sciarretta, S. Ranise, Control is nothing without trust a first look into digital identity wallet trends, in: IFIP Annual Conference on Data and Applications Security and Privacy, Springer, 2023, pp. 113–132.
[16] V. Bolgouras, A. Angelogianni, I. Politis, C. Xenakis, Trusted and secure self-sovereign identity framework, in: Proceedings of the 17th International Conference on Availability, Reliability and Security, ARES '22, Association for Computing Machinery, New York, NY, USA, 2022. URL: https://doi.org/10.1145/3538969.3544436. doi:10.1145/3538969.3544436.
[17] P. Windley, How sovrin works, Sovrin Foundation (2016) 1–10.
[18] C. Lundkvist, R. Heck, J. Torstensson, Z. Mitton, M. Sena, Uport: A platform for self-sovereign identity, URL: https://whitepaper. uport. me/uPort_ whitepaper_DRAFT20170221. pdf (2017).
[19] P. Jakubeit, A. Dercksen, A. Peter, Ssi-aware: Self-sovereign identity authenticated backup with auditing by remote entities, in: Information Security Theory and Practice: 13th IFIP WG 11.2 International Conference, WISTP 2019, Paris, France, December 11–12, 2019, Proceedings 13, Springer, 2020, pp. 202–219.