VC-Vault: A User-Friendly, Secure, Privacy-Enhancing Verifiable Credentials Wallet

Chalima Dimitra Nassar Kyriakidou[1,*], George C. Polyzos[1, 2, 3]

[1] Mobile Multimedia Laboratory, Department of Informatics, School of Information Sciences and Technology, Athens University of Economics and Business, Greece
[2] School of Data Science, The Chinese University of Hong Kong-Shenzhen, China
[3] ExcID P.C., Athens, Greece

* Corresponding author. Email: dnassar@aueb.gr (C.D.N.K.)

Manuscript received January 28, 2024; accepted February 23, 2024; published March 22, 2024
DOI: 10.18178/IJBTA.2024.2.1.16–24

Abstract: The shift from centralized identity systems to decentralized alternatives is becoming more imminent. Users are increasingly encouraged to embrace the principles of Self-Sovereign Identity (SSI), relying on two key components, Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs), to regain total ownership and control over their identity and data, as well as how and to whom they are shared. This emphasizes a pressing need for VC wallet solutions that are not only user-friendly, but also uncompromisingly secure. In this paper, we introduce VC-Vault, an innovative wallet application that incorporates the principles of SSI and conforms to the European Blockchain Services Infrastructure (EBSI) standards. VC-Vault operates across both desktop and mobile platforms, delivering a coherent and effortless user experience. By establishing seamless integration with EBSI services, SSI principles, and VCs, VC-Vault places the control of digital identity and credentials firmly in the discretion of users.

Keywords: Decentralized Identifiers (DIDs), privacy, security, Self-Sovereign Identity (SSI)

1. Introduction

In an increasingly digital world, users are becoming progressively more concerned about the management and sharing of their personal data. This awareness arises from a growing understanding of the value and vulnerability of their digital identities and information. In response to these concerns, Self-Sovereign Identity (SSI) has emerged to empower users by returning the control of their digital identities and data back to their rightful owners-themselves. It emphasizes the principles of privacy and security. Recognizing the significance of trust services in a digital age, the European Commission has launched the European Blockchain Services Infrastructure (EBSI) initiative. EBSI is designed to leverage the potential of Blockchain technology to support secure, user-controlled digital identities and credentials, aligning with the core principles of SSI. In this way, EBSI represents a forward-looking and user-focused approach to identity, trust, and data management within the European digital landscape.

Wallets play a crucial role in facilitating the aforementioned shift towards this new paradigm of digital identity. They are essential tools that enable individuals to securely store, manage, and transact with their digital assets, providing a convenient means to access funds, protect private keys, and engage in secure transactions in the digital world. In the ever-expanding realm of digital wallets, the emphasis has predominantly been on mobile applications, catering to users' convenience and accessibility. However, the availability of secure and user-friendly desktop wallets is comparatively limited. We have developed and we present here VC-Vault, which offers a dedicated desktop application for Windows, macOS, and Linux, alongside its mobile application, providing users with a comprehensive solution across multiple platforms. Thus, it is a versatile choice for individuals seeking secure, seamless and user-friendly digital (verifiable) credential management solutions. It is a cross-platform wallet, which also provides cross-border services by adhering to EBSI Conformance. This all contributes to the enhancement of trust, security, privacy, and interoperability in the management of credentials and transactions within the European Blockchain ecosystem.

2. Background

2.1. Self-Sovereign Identity

SSI has emerged as a revolutionary concept that has the potential to reshape the way we manage and control our digital identities. SSI is based on the idea that individuals should have complete ownership and control over their digital identities, rather than relying on centralized authorities to manage their data [1]. Christopher Allen was the first to propose 10 principles that any SSI system must adhere to [2], and has since urged individuals in the digital identity community to incorporate and revise these principles, with some updates and critiques having already been proposed [3]. Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) are key components of SSI that enable secure and trustworthy interactions between entities. A typical overview of the SSI ecosystem is depicted in Fig. 1.

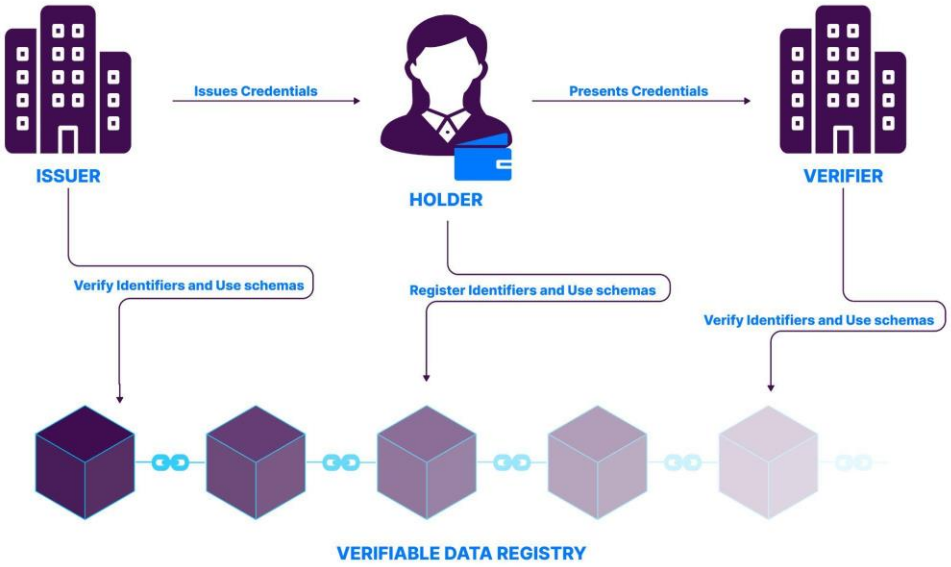

Issues Credentials
Presents Credentials
ISSUER
HOLDER
VERIFIER
Verify Identifiers and Use schemas
Register Identifiers and Use schemas
Verify Identifiers and Use schemas
VERIFIABLE DATA REGISTRY

Fig. 1. Typical overview of the SSI ecosystem.

DIDs have emerged as a fundamental component of SSI systems, providing a decentralized, secure and interoperable way to represent and manage digital identifiers. DIDs enable individuals and organizations to control their identities, relationships and interactions in a way that is private, secure, and trustworthy. The origins of DIDs can be traced back to the World Wide Web Consortium (W3C) [4], which recognized the need for a decentralized, standardized way to manage digital identities.

According to the recent recommendations by the W3C [5], VCs are digital credentials that verify and authenticate specific information or claims about individuals or organizations in a secure and tamper-evident manner. Traditional credentials suffer from several problems, such as susceptibility to forgery and counterfeiting, loss or damage, high cost of issuance and scalability challenges. Additionally, they frequently mandate the disclosure of excessive personal information beyond what is essential for the specific use case. The SSI architecture addresses the aforementioned problems associated with traditional credentials by providing a decentralized, globally unique, highly available, and cryptographically verifiable identifier system. According to Mühle *et al.* [6], VCs are an integral part of this architecture and offer a means for individuals to store and manage their credentials in a digital wallet that is not bound to a single vendor or device, meaning users can have several different wallets on various devices while retaining access to their credentials.

There exist several notable instances, where the application of VCs has demonstrated significant potential in addressing challenges related to conventional credentials. One such example pertains to the utilization of VCs for COVID vaccination certificates [7]. In this context, traditional physical credentials often necessitated the disclosure of a surplus of personal information to establish authenticity. Furthermore, the verification process associated with these physical credentials frequently proved time-consuming and prone to errors. However, the adoption of VCs in such scenarios presents a compelling alternative. VCs empower individuals to selectively share only the essential information required for verification, thereby mitigating the need to divulge excessive personal data. Moreover, the authentication process facilitated by VCs can be streamlined and automated, leading to increased efficiency, while minimizing the risk of errors. A more detailed presentation of SSI, DIDs, VCs and their applications, is presented in [8].

VCs have consistently demonstrated their utility and adaptability when integrated with various protocols, as evidenced by current research. One notable example is the seamless integration of VCs with the OAuth security protocol [9], which empowers users to grant access to their digital identities to third-party applications or services, while upholding the integrity of their credentials. An implementation of an authentication system that leverages OAuth 2.0 and incorporates VCs, is presented by Fotiou *et al*. [10]. Another example is the utilization of VCs within the framework of Fast Identity Online (FIDO), an open standard designed to improve both security and user experience in online authentication. An instance of this integration is the implementation for UK National Health Service (NHS) patients, proposed by Chadwick *et al*. 1]. Furthermore, the OpenID protocol, specifically OpenID Connect, supports OAuth 2.0 and JSON Web Tokens (JWTs). This enables the deployment of VCs as access tokens, thereby enhancing security and interoperability in identity verification processes [12]. Finally, several applications and frameworks have also proposed the utilization of SSI for enhancing security in Internet of Things (IoT) networks. Notable examples of such systems include [13–15].

2.2. European Blockchain Service Infrastructure

EBSI[1] is a notable initiative of the European Commission that aims to establish a secure and trusted infrastructure for cross-border digital public services using Blockchain technology [16]. EBSI offers core technical services, including Application Programming Interfaces (APIs), Smart Contracts, and the EBSI ledger, that operate in a decentralized manner across Europe through a network of nodes. The ledger copies are synchronized among the nodes, resulting in a distributed ledger, and all the core technical services provided by EBSI are made available to them.[2] With the goal of promoting efficiency and trust in digital transactions, EBSI enables the development of innovative digital solutions that can improve public services.

EBSI's functional capabilities are grouped into several Use Case families,[3] including VCs, Trusted Data

[1] European Blockchain Service Infrastructure (EBSI). Available online: https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Home (Accessed on 12 January 2023).

[2] What is EBSI? Available online: https://ec.europa.eu/digital-building-blocks/wikis/ display/EBSI/What+is+ebsi (Accessed on 12 January 2023).

[3] Business: What can you do with EBSI? Available Online: https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/What+is+EBSI#:~:text=Use%20Case%20families%20and%20domains,-

Exchange, and Track and Trace, each of which is further subdivided into specific domains. While exploring them, developers are encouraged to select a business scenario, which refers to a specific sector where EBSI can be utilized to support the creation of cross-border services. Since EBSI is a recently launched initiative, only the VCs Use Case family is currently available for exploration, covering credentials related to Social Security and Education. However, the Track and Trace family is being expanded to encompass Document Traceability and Small and Medium-sized Enterprises (SMEs) Financing, whereas the Trusted Data Exchange family will include general credentials for Trusted Data Exchange and Asylum Management.

3. Related Work

As part of the integration with EBSI, VC wallets undergo the Wallet Conformance Test, which includes two test case scenarios: requesting VCs (issuance) and presenting VCs (verification). There are 18 wallets that have achieved conformance with the second version of the EBSI specifications, demonstrating adherence to the corresponding standards.[4] Regarding their implementation approach, 14 wallets provided support for both desktop and mobile applications, while four wallets solely focused on mobile applications, as presented in Fig. 2(a). Among these, 16 wallets successfully implemented the Diploma Use Case, nine wallets integrated the Identity Use Case, seven wallets adopted the Student ID Use Case, and five wallets incorporated the PDA1 (proof of work arrangement within EU/EEA) Use Case, as depicted in Fig. 2(b).

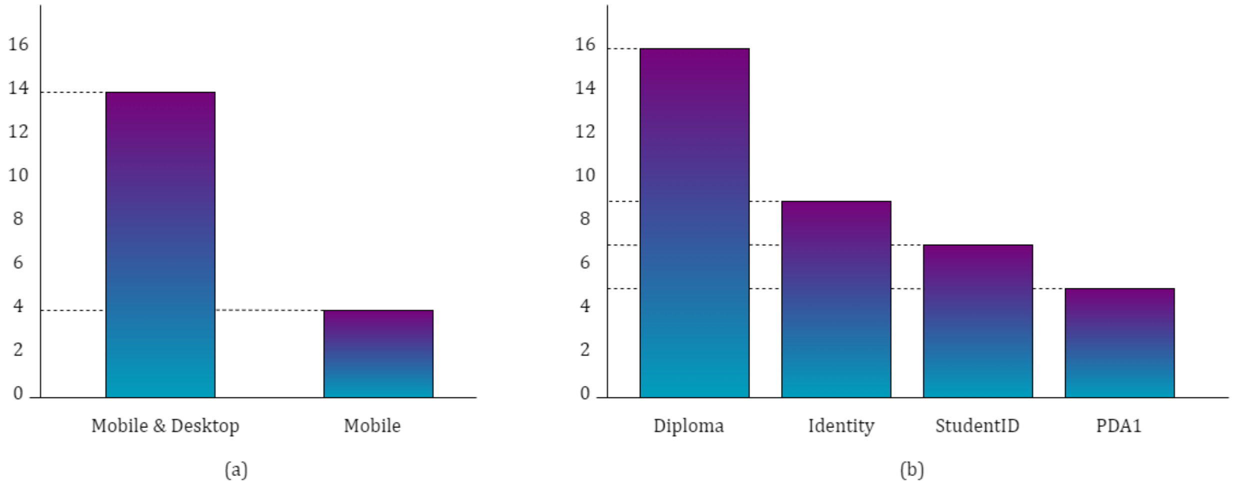


Fig. 2. EBSI v.2 Conformant wallets: (a) by implementation and (b) by use case.

Despite the availability of several wallets supporting both desktop and mobile platforms, the user-friendliness of the desktop versions appeared to be compromised. This is primarily because desktop versions are typically designed for developers and lack a user interface tailored for the general user. This pattern continued with the third and latest version of the Conformance Test, with 16 wallets successfully achieving conformance. Among these, only 8 wallets are currently available for download, with 6 being mobile applications, one being a desktop, mobile and Web solution that utilizes the InterPlanetary File System (IPFS) and one being a Web-based platform with cloud-based storage. This further emphasizes the need for improved usability and security measures for desktop versions of EBSI Conformant wallets. Note that EBSI's Conformance Test versions are consistently evolving, and while we are currently at version 3, the next version is anticipated to be released soon.

EBSI%20developed%20several&text=These%20are%20grouped%20into%20%22Use,credentials%22%20for%20verification%2C%20etc. (Accessed on 12 January 2023).

[4] EBSI Conformant Wallets. Available online: https://ec.europa.eu/digital-buildingblocks/wikis/pages/viewpage.action?pageId=632521170&navigatingVersions=true (Accessed on 13 January 2023).

4. System Design & Implementation

A typical use case scenario of the VC-Vault wallet for Natural Persons, in accordance with the EBSI guidelines, is depicted in Fig. 3. From a high level perspective, the proposed wallet solution operates as follows: the issuer issues VCs to the holder, who is the user of the VC-Vault wallet utilizing either or both mobile and desktop devices. Verifiers then verify the credentials when presented (by the holder, at his discretion). VC-Vault creates a public-private key pair and a DID, utilizing the public key, for each user. When the user requires a credential, she visits the issuer's webpage, thus initiating communication between the issuer and VC-Vault on her behalf. The end result of this communication is a VC issued and signed by the issuer, which is then stored in the user's (holder's) device. The VC payload includes a Verifiable Attestation created during the communication, but not stored in local storage. When the user/holder is required to present a Verifiable Presentation (VP), the wallet initiates communication with the verifier and generates a VP containing one or more previously issued VCs. This VP is stored and signed using the user's private key. It is of significance to note that EBSI offers a GDPR-compliant SSI solution for Natural Persons, where their DIDs are not recorded on the ledger, ensuring privacy and compliance with data protection regulations.

In detail, the user initiates the VC issuance flow by visiting the issuer's website and providing a DID as the primary identification source. This process can be initiated either from the same device running the wallet or from a different device. In the former scenario, the wallet is activated through a deep link, as the user clicks on a button redirecting her to the wallet's interface. In the latter scenario, the user receives a QR code, typically from the issuer's webpage, which is then scanned using the wallet. Following the OAuth 2.0 and the OpenID protocols, the discovery phase ensues, during which the wallet requests and is presented with the configuration of the trusted issuer.

After obtaining the necessary configuration, the authorization phase begins, and the specific flow varies. For instance, if the user has previously authenticated with the issuer, the authentication process can be completed by providing the user with a PIN code. Alternatively, if the user has not been registered with the issuer before, authentication occurs with the assistance of a signed token created by the wallet. In this case, two distinct flows emerge. For a simple VC issuance, the token provided by the wallet to the Issuer's Auth server is a signed ID Token, aiming to authenticate the wallet as the user's intermediary for the upcoming VC issuance. The next step involves the wallet gaining access to the issuer's issuance endpoint. The Auth Server grants the successfully authorized wallet a Bearer Token, which is then used to request the VC from the Issuer Server. Depending on the scenario, the Issuer responds with the VC, in the case of an In-Time Issuance or with an Acceptance Token in the case of a Deferred Flow. In the Deferred Flow, the wallet continues to request the VC from the Issuer's Deferred Endpoint using the Acceptance Token obtained in the previous step until the VC is prepared by the Issuer. Finally, the successfully issued VC is stored in the user's device. In the second scenario, the VP-Exchange flow occurs, involving the wallet presenting a VP to a verifier. Specifically, the VP is presented through a signed VP Token containing the requested VCs as specified by the verifier.

In VC-Vault, the user's data, including keys, DIDs, VCs, and VPs, are meticulously organized within a config.json file, which we encrypt with Advanced Encryption Standard (AES) 256 encryption, using a robust 32-byte user (secret) password. This encrypted file serves as a secure repository and is stored on the user's device. To ensure data integrity and relevance, storage functions are activated before closing the app, updating the config.json file under specific conditions, namely the issuance of new VCs, the generation of new VPs, user-initiated deletions of VCs or VPs, and automatic removal of expired VCs or VPs. When a user wants to log in, the wallet retrieves the encrypted file. The user then inputs the password, initiating the decryption process. If successful, the user gains access to the wallet; otherwise, access is denied.

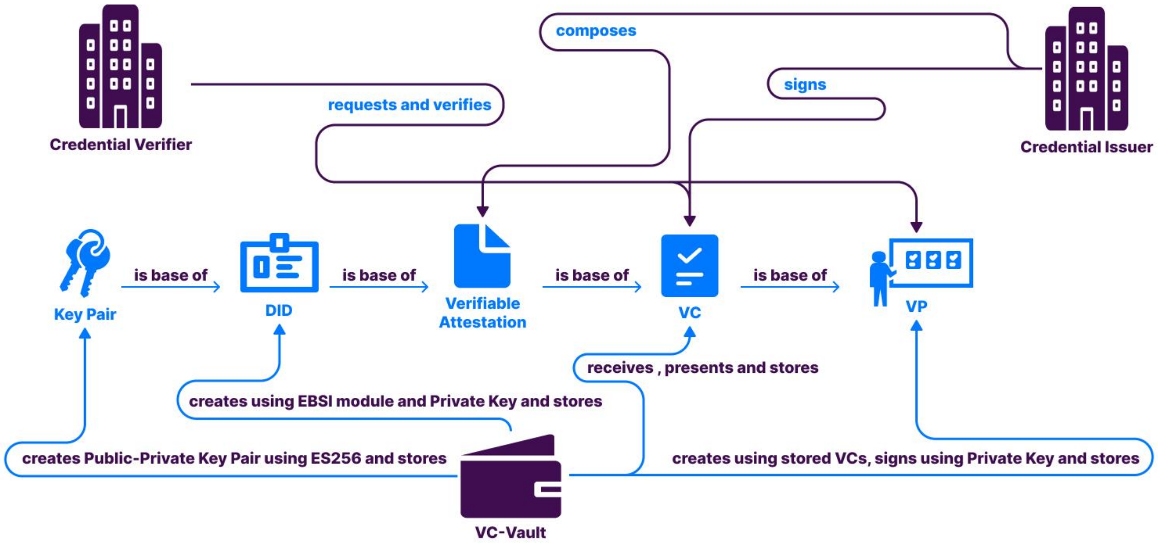
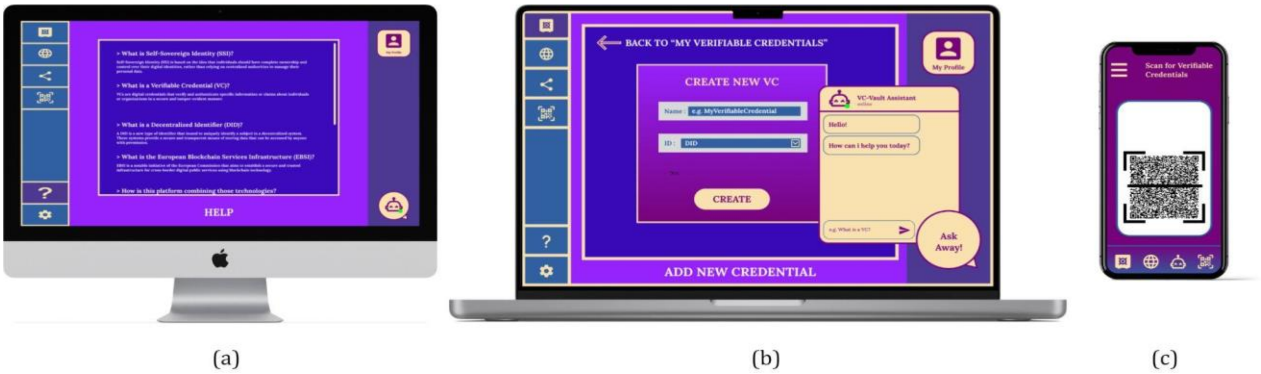

Credential Verifier
requests and verifies
composes
signs
Credential Issuer
Key Pair
is base of
DID
is base of
Verifiable Attestation
is base of
VC
is base of
VP
receives , presents and stores
creates using EBSI module and Private Key and stores
creates Public-Private Key Pair using ES256 and stores
creates using stored VCs, signs using Private Key and stores
VC-Vault

Fig. 3. VC-Vault: Verification and issuance process

As previously mentioned, VC-Vault offers a desktop application for Windows, macOS and Linux. To achieve this it utilizes the Electron framework, which enables the development of cross-platform desktop applications. Electron seamlessly combines the versatility of Web technologies, such as HTML, CSS, and JavaScript with the robust capabilities of Chromium and Node.js. This empowers VC-Vault to offer users a desktop experience that closely mimics native applications. With Electron, our wallet solution delivers familiarity, responsiveness, and access to system-level features, ensuring that users can effortlessly navigate and interact with the application. Furthermore, VC-Vault extends its reach to mobile platforms through React Native. By adopting React Native, VC-Vault expands its accessibility to Android and MacOS mobile devices. This strategic choice enables users to enjoy a consistent and user-friendly experience, whether they are accessing VC-Vault on their desktop or mobile device. The result is a versatile wallet solution that seamlessly bridges the gap between Web technologies and native-like performance, catering to the diverse needs and preferences of our user community.

Our emphasis in presenting the interface of VC-Vault will primarily be on the desktop version. This aligns with our goal of showcasing it as a user-friendly solution tailored for end users. In the desktop version, the left-hand side features a user-friendly navigation bar. As depicted in Fig. 4(b), by clicking on the first tab users can conveniently find the VCs that they have already created and are readily accessible on their devices. In this figure, we focus specifically on the interface for creating a new VC, catering to users who seek to initiate the credential creation process. The Share tab allows users to effortlessly share specific VCs they already possess. Additionally, a QR scanner tab enables users to accept credentials from issuers by simply scanning QR codes, ensuring a user-friendly and streamlined experience.

For users seeking answers to common questions about SSI, VCs, DIDs, EBSI, and more, a tab marked with a question mark symbol provides easy access to frequently asked questions, as illustrated in Fig. 4(a). VC-Vault further enriches the user experience with a realtime chat feature, allowing users to seek immediate assistance or gain insights into the wallet's features and functionalities, which was also presented in Fig. 4(b). Finally, users can tailor their VC-Vault experience to their preferences through the Settings tab, customizing and personalizing the application to suit their unique needs. The mobile version of VC-Vault shares the same user-friendly design. The QR scanner feature, which is most likely to be used in the mobile version of VC-Vault is illustrated in Fig. 4(c). It's worth noting that the QR scanner functionality is also available in the desktop version, taking advantage of laptops equipped with dual cameras for this purpose.



> What is Self-Sovereign Identity (SSI)?

> What is a Verifiable Credential (VC)?

> What is a Decentralized Identifier (DID)?

> What is the European Blockchain Services Infrastructure (EBSI)?

> How is this platform combining those technologies?

HELP

BACK TO "MY VERIFIABLE CREDENTIALS"

CREATE NEW VC

Name : e.g. MyVerifiableCredential

ID : DID

CREATE

VC-Vault Assistant

Hello!

How can i help you today?

e.g. What is a VC?

ADD NEW CREDENTIAL

Scan for Verifiable Credentials

Fig. 4. VC-Vault's user interface: (a) Frequently asked questions, (b) VC creation and (c) QR scanner.

5. Discussion

VC-Vault offers a range of key features that make it a noteworthy solution in the field of VC wallets. One of its primary strengths is its interoperability, enabling seamless integration with various blockchain platforms and services. Unlike other EBSI-Conformant wallets that primarily target developers and offer desktop versions that require complex technical knowledge that the average end user lacks, VC-Vault prioritizes a user-centric approach, meaning that it offers options for general users with varying levels of technical expertise. This ensures that users can efficiently manage their digital assets across different ecosystems, promoting a unified and interconnected experience. User-friendliness is another key focus of VC-Vault, providing an intuitive and accessible interface that simplifies navigation and enhances usability. With VC-Vault, users can confidently interact with the wallet, irrespective of their chosen Operating System. This commitment to inclusivity sets VC-Vault apart, making it a wallet that truly addresses the diverse needs of the user community.

As previously mentioned, VC-Vault is also EBSI Conformant, which enables reliable interactions with EBSI services and credentials, thereby reinforcing trust, security, and interoperability within the European blockchain ecosystem. EBSI conformance signifies that users' personal information and credentials are safeguarded and all processes adhere to the rigorous security protocols set forth by EBSI. As an open source solution, it also promotes transparency, fosters collaboration, and encourages community engagement.

VC-Vault stands out among other EBSI Conformant wallets in regard to security, due to its commitment to prioritize robust security and privacy measures in alignment with the OpenID specification [17]. This approach sets VC-Vault apart, emphasizing its commitment to ensuring security practices that some other wallets might not consistently uphold. The adherence to established standards and best practices positions VC-Vault as a trustworthy and secure choice for users looking for a wallet solution aligned with industry specifications. For instance, our wallet solution satisfies the requirement for holders to identify the issuers and verifiers of their VCs. User control and explicit consent is ensured through the wallet's interface, prompting users to make decisions regarding interactions between their wallet and entities, such as issuers and verifiers. Another feature that showcases VC-Vault's adherence to OpenID's security and trust requirements is that expired credentials are promptly deleted and users are also able to independently manage and delete them before they expire, which also aligns with the core principles of SSI.

VC-Vault prioritizes the protection of user information and credentials. The wallet implements robust security measures to ensure the integrity and confidentiality of user data. Currently, the wallet stores private keys, DIDs, VCs, and VPs in the user's device by creating an encrypted config.json file using AES 256. The user's password serves as the key for AES, and this process is facilitated by the electronstore module and the Async Storage module for the desktop and mobile versions respectively, which offer built-in mechanisms for secure data storage in the user's device. Notably, the user's password is never stored in the wallet but remains in the user's memory or preferred storage location. This, in combination with the use of AES 256, provides a highly secure environment, although the level of security also depends on how the user stores her password. Additionally, the wallet employs encryption techniques to safeguard sensitive information during storage and transmission, providing users with peace of mind regarding the privacy and confidentiality of their data. VC-Vault also enables users to track their transaction history, which not only enhances convenience, but also contributes to security. Specifically, users can easily identify any suspicious or unauthorized activities, enabling them to ensure the integrity of their digital assets. Finally, as the wallet follows SSI principles it ensures data minimization, meaning that there is no unnecessary data exposure, and users have full ownership and control of their digital identities and assets.

6. Conclusion

In considering potential future enhancements for VC-Vault, a few avenues for improvement can be identified. While the current encryption method using AES 256 and the electronstore module ensures robust security, it requires a longer password, presenting a trade-off for the heightened security measures implemented in VC-Vault. Since the wallet is built on Electron, it has the potential to enhance user-friendliness by exploring options, such as storing private keys in the OS's key management system using Electron's SafeStorage API. It is crucial to note that this API utilizes obfuscation for private keys, a method different from the more secure encryption employed by VC-Vault with AES 256. While obfuscation can deter casual inspection, determined attackers may still reverse-engineer the obfuscated code and retrieve the original private key. Striking the right balance between robust security and user-friendliness remains an ongoing focus for future improvements. Thus, one future enhancement we are currently exploring involves the incorporation of FIDO, which could contribute to our efforts to strike a balance between user-friendliness and robust security by providing users with more login options.

The development of VC-Vault addresses a critical need in the digital wallet realm by providing a seamless and user-friendly experience across both desktop and mobile platforms, while other existing EBSI Conformant wallets predominantly focus on mobile applications. By offering a dedicated cross-platform desktop app, VC-Vault ensures seamless and secure management of digital assets, regardless of users' preferred device or OS. With advanced security measures, such as the alignment with the requirements of OpenID's specification requirements, as well as the core principles of SSI and the utilization of AES 256, VC-Vault prioritizes the protection of user information and credentials. Furthermore, its EBSI conformance enhances trust, security, and interoperability within the European blockchain ecosystem. Being an open-source solution, VC-Vault encourages transparency, collaboration, and community involvement, enabling users to actively contribute to its continuous improvement. The wallet's cross-platform compatibility, user-friendliness, security, and EBSI conformance position it as a useful tool for users seeking a comprehensive and reliable digital wallet solution.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Chalima Dimitra Nassar Kyriakidou conducted the research, designed and implemented the system and prepared the first draft of the article. George C. Polyzos directed the research, contributed to the design and provided guidance during the implementation of the system. Both authors approved the final version of the article.

Acknowledgment

The authors thank Dr. Nikos Fotiou for valuable discussions and technical guidance throughout the project.

References

[1] R. Soltani, U. T. Nguyen, and A. An, "A Survey of Self-Sovereign Identity Ecosystem," *Security and Communication Networks*, pp. 1–26, 2021. https://doi.org/10.1155/2021/8873429

[2] C. Allen. (April 2016). The Path to Self-Sovereign Identity. Life with Alacrity. Available: https://www.lifewithalacrity.com/article/the-path-to-self-sovereign-identity/

[3] C. Allen. (March 2020). Web of Trust - Self Sovereign Identity. Github. Available: https://github.com/WebOfTrustInfo/self-sovereign-identity

[4] Decentralized Identifiers (DIDs) v1.0, World Wide Web Consortium (W3C) Recommendation-2022.

[5] Verifiable Credentials Data Model v1.1, World Wide Web Consortium (W3C) Recommendation-2022.

[6] A. Mühle, A. Grüner, T. Gayvoronskaya, and C. Meinel, "A Survey on Essential Components of a Self-Sovereign Identity," *Computer Science Review*, vol. 30, pp. 80–86, November 2018. https://doi.org/10.1016/j.cosrev.2018.10.002

[7] J. Sedlmeir, R. Smethurst, A. Rieger, and G. Fridgen, "Digital Identities and Verifiable Credentials," *Business & Information Systems Engineering (BISE)*, vol. 63, no. 5, pp. 603–613, September 2021. https://doi.org/10.1007/s12599-021-00722-y

[8] C. D. Nassar Kyriakidou, A. M. Papathanasiou, and G. C. Polyzos, "Decentralized Identity with applications to Security and Privacy for the Internet of Things," *Computer Networks and Communications*, vol. 1, no. 2, pp. 244–271, August 2023. https://doi.org/10.37256/cnc.1220233048

[9] RFC 6749-The OAuth 2.0 Authorization Framework. Internet Engineering Task Force (IETF)-2012.

[10] N. Fotiou, E. Faltaka, V. Kalos, A. Kefala, I. Pittaras, V. A. Siris, and G. C. Polyzos. "Continuous Authorization over HTTP using Verifiable Credentials and OAuth 2.0," in *Proc. Open Identity Summit 2022 (OID '22)*, July 2022, pp. 39–50. https://doi.org/10.18420/OID2022_03

[11] D. W. Chadwick, R. Laborde, A. Oglaza, R. Venant, S. Wazan, and M. Nijjar, "Improved Identity Management with Verifiable Credentials and FIDO," *IEEE Communications Standards Magazine*, vol. 3, no. 4, pp. 14–20, December 2019.https://doi.org/10.1109/MCOMSTD.001.1900020

[12] OpenID for Verifiable Credentials–Overview, OpenID Foundation-2023.

[13] P. N. Mahalle, G. R. Shinde, and P. M. Shafi, "Rethinking Decentralised Identifiers and Verifiable Credentials for the Internet of Things," *Studies in Systems, Decision and Control*, vol. 266, pp. 361–374, February 2020. https://doi.org/10.1007/978-3-030-39047-1_16

[14] S. K. Gebresilassie, J. Rafferty, P. Morrow, L. Chen, M. Abu-Tair, and Z. Cui. "Distributed, Secure, Self-Sovereign Identity for IoT Devices," in *Proc. 2020 IEEE 6th World Forum on Internet of Things (WF-IoT)*, New Orleans, LA, USA, June 2020, pp. 1–6. http://dx.doi.org/10.1109/WF-IoT48130.2020.9221144

[15] E. Zeydan, J. Mangues, S. Arslan, and Y. Turk. "Blockchain-based Self-Sovereign Identity Solution for Vehicular Networks," in *Proc. 2023 19th International Conference on the Design of Reliable Communication Networks (DRCN)*, Vilanova I la Geltru, Spain, April 2023, pp. 1–7, https://doi.org/10.1109/DRCN57075.2023.10108183

[16] M. Turkanović and B. Podgorelec, "Signing Blockchain Transactions Using Qualified Certificates," *IEEE Internet Computing*, vol. 24, no. 6, pp. 37–43, September 2020. https://doi.org/10.1109/MIC.2020.3026182

[17] D. Fett and T. Lodderstedt, "Security and Trust in OpenID for Verifiable Credentials Ecosystems," *Github*, September 2023. https://github.com/openid/OpenID4VC_SecTrust/blob/main/draft-oid4vc-security-and-trust.md