Zentrum für sichere Informationstechnologie – Austria
Secure Information Technology Center – Austria

A-SIT

Seidlgasse 22 / 9, 1030 Wien
Tel.: +43 1 503 19 63–0
Fax: +43 1 503 19 63–66

Inffeldgasse 16a, 8010 Graz
Tel.: +43 316 873-5514
Fax: +43 316 873-5520

http://www.a-sit.at
E-Mail: office@a-sit.at

DVR: 1035461
ZVR: 948166612
UID: ATU60778947

SSI STRONG AUTHENTICATION

Version 1.0 – 12.03.2021
Author – Andreas Abraham andreas.abraham@egiz.gv.at

Abstract: Digital identities are an integral part of today's digital world. These digital identities are used to perform identification and authentication in order to access online services or resources. The level-of-assurance (LoA) describes the level of confidence that the service provider (SP) can have in the provided authentication means. Various standards specify these LoAs. SSI is a new identity model aiming to give the users control back over their identity data. Mobile phone-based identity wallets are often used within SSI systems to manage cryptographic keys and identity credentials. Nevertheless, none of the available wallet implementations achieve an LoA high. This work aims to define a generic concept that supports identity wallets to reaches an LoA high. To achieve this, we started with assessing the related standards and used the outcome to define requirements. These requirements were used to design the solution architecture as well as to evaluate it. Finally, we define measures of our concept how the requirements are being met and an LoA is achieved.

Table of Contents

1. Introduction

Digital identities are an essential part of the digital world. Identity management (IdM) manages those digital identities throughout the whole identity lifecycle [1]. IdM evolved over time, starting with the isolated identity mode in which the same party is representing the service provider (SP) and the identity provider (IdP). IdM models evolved over the federated IdM model to the user-centric IdM model in which user data and authentication means are stored within the user's domain like in the Austrian citizen card concept.

The recent Blockchain technology offers new opportunities in various fields, including IdM. The concept of Self-Sovereign Identity (SSI) arose with the emergence of Blockchain technology. SSI is an IdM model and can be seen as an evolvement of the user-centric identity model [2]. In contrast to the user-centric identity, the model focuses on SSI, giving the user full control over their identity data. Additionally, SSI also addresses the central trusted party by utilizing a Blockchain or Distributed Ledger Technology (DLT).

The potential of SSI was recognized early by various scientists performing research in the field of SSI [3]–[5] as well as by the European Commission, which founded the European Blockchain Services Infrastructure[1] (EBSI). Within EBSI, the European Self-Sovereign Framework[2] (ESSIF) use-case group was founded focusing on SSI in Europe.

Besides, the DLT is one of the fundamental parts of an SSI system, the so-called identity wallet. An identity wallet describes software with the main objectives to protect and store digital assets like key material or sensitive user data. Identity wallets often utilize special hardware like secure elements to achieve this [6].
Wallets can be deployed on various devices in the user's domain, such as the browser, as a cloud service or on the smartphone. Since the smartphone is becoming the main device of users used for many services such as online shopping, social media, video streaming, and even to access public administrations services, identity wallets on mobile phones are an important SSI component. Wallets store, besides the personal data of the user, also cryptographic key material both used for identification and authentication of the user.

Assurance in authentication means an important part of an identity system represented in the so-called level-of-assurance (LoA). These LoA are specified by various standards such as by the European Commission as implementation act [7], which is built upon the ISO standard [8] for entity authentication. NIST also specifies assurance levels [9] besides others. These assurance levels specify requirements and guidelines for the related levels on which the SP can rely on. The higher the LoA, the higher the guarantees in the authentication means, which further increases the trust in those data. Special services such as eGovernment services or online banking might require an LoA high, to name two out of many. This leads to the consequence that a mobile phone-based identity wallet that achieves an LoA high would be the next step since it was not achieved yet.

This report focuses on identifying a concept of a mobile phone-based wallet that can be used to achieve an LoA high. We start with an analysis of the related work described in Section 3, and Section 2 gives an overview of the building blocks of this work. Next, we assess LoA standards and derive requirements for such an identity wallet. We specify a generic concept that fulfills all of the previously defined requirements shown in Section 4. The findings and results of this work were published as a research paper [10].

[1] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI
[2] https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=262505734

2. Preliminaries

This section details the building blocks used within this work.

2.1. Self-Sovereign Identity (SSI) System

Zwattendorfer et al. detailed the evolvement of IdM models [1], starting with the isolated IdM model over the central IdM model to the user-centric model. SSI can be seen as the further evolvement of the user-centric identity model [2], giving the user full control over the own identity data back as well as addressing the central trusted party.

SSI systems consist of at least four parties, depicted in Figure 1. The users describe persons that want to use their digital identity to perform identification and authentication towards a verifier in order to, e.g., get access to a service or resource. The issuer is responsible for providing identity-related information like an IdP. The DL is used as a decentralized public key infrastructure (DPKI) where public information like public keys or public endpoints are being stored and retrievable. The SSI network consists of nodes where each node holds a copy of the ledger. The nodes utilize a consensus mechanism in order to reach a consensus about what is written to the ledger. Commonly, semi-trusted nodes host the DL in the SSI system like organizations like banks or universities, etc. This way, writing to the network is restricted, but reading is publicly possible.

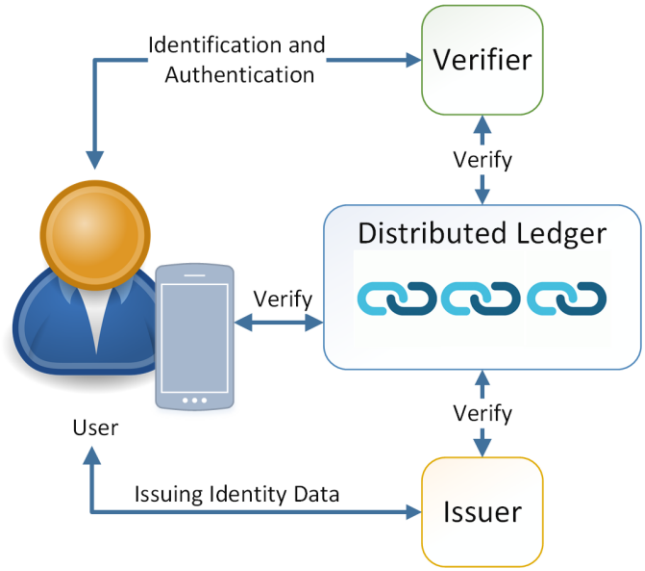

Figure 1: High-Level Architecture of an SSI System [10]

2.2. Decentralized Identifier (DID)

One of the main building blocks of SSI is the Decentralized Identifier (DIDs) [11]. Those DIDs were specified with the main objective to enable SSIs. DIDs are basically URLs that resolve to an entry on a DL. This entry is the counterpart of a DID and named DID document. The DID document is directly linked to the DID as well as to at least one of the user's public-private key pairs. When a digital document is issued to the verifier, it includes besides attributes of the user also the DID of the user as well as the DID of the issuer. These DIDs resolve to the related DID documents on the DL, which contains public information, like endpoints or public keys. Sensitive data are never stored on the DL; instead, these kinds of data are stored within the user's domain and off-ledger.

2.3. Level-of-Assurance (LoA)

The level-of-assurance (LoA) defines what level of confidence the verifier can have in the authentication of a user. These LoAs are defined by different standards like the eIDAS implementation act [7], the ISO standard on entity authentication [8] that also serves as a foundation for the eIDAS implementation act, as well as the NIST standard on digital identity guidelines: authentication and lifecycle management [9], besides others. This work focuses especially on the eIDAS implementation act and the related ISO standard also because one of the objectives is to be compliant with these standards.

These standards specify a framework that defines the technical as well as the organizational part. The technical part consists of the enrolment phase in which the user proves her identity and a registration party, followed by the credential management phase, which deals with the issuance, storage, and revocation of credentials. Finally, the authentication phase deals with the actual authentication procedures.

3. Related Work

This subsection lists the related work addressing first the identity wallet projects, including how they differ from our solution, and second the listing related research papers in this field.

3.1. Identity Wallet Projects

Many identity wallet projects are available focusing on different aspects, and many new ones arise, and many of them are not further maintained anymore. We were looking at various of those projects during our related work research and listing the most promising below. Interestingly, none of the projects that we investigated achieves an LoA high. Additionally, these projects' focus varies, and achieving a certain LoA is not even an objective for projects.

Jolocom SmartWallet [12] is an identity wallet implemented by Jolocom, a company aiming to implement an SSI system. Jolocom's SmartWallet can be used to manage identity data in an easy and user-friendly way but not focusing on achieving a certain LoA.

DIZME (this is me) [13] is an identity wallet implementation by the trust over IP foundation with the main objective to fill the gap between SSI and eIDAS. This project details various aspects of the wallet; notably, it is not open-source software. Nevertheless, one of DIZME's objectives is to achieve a certain LoA that they claim is substantial.

Connect Me [14] is an identity wallet by Evernym focusing on an implementation that supports an easy way of sharing and holding identity credentials. They also state that their wallet uses one-to-one communication channels implemented through agents as well as zero-knowledge proofs to get selective attribute disclosure, which protects the user's privacy.

Alastria Wallet [15] is a wallet provided by Alastria, a company that the main objective describes to achieve an SSI system. The Alastria Wallet implementation is open source and was created for easy onboarding to the Alastria network. Nevertheless, reaching a certain LoA level is not the main objective of this wallet.

3.2. Research Papers on Identity Wallets

This section details the research publications in the field of identity wallets.
In the work of Dai et al. [16], focuses on utilizing the Trustzone[3] on mobile devices to create and store cryptographic key material. Security relevant operations like signing etc., are performed in this Trustzone as well in order to mitigate attacks. This work addresses an important aspect when trying to achieve a certain LoA. Nevertheless, taper-resistant storage is only one requirement when looking at LoAs.

In contrast, the work of Iqbal et al. [17] investigates mobile phone-based wallets. In particular, this work focuses on applying fingerprint verification as an authentication factor especially considering the needs of the elderly. Usability is one of the key aspects for the older generation and also the biggest obstacle when using it. Thus, this work tries to address this issue by still maintaining a high level of security but not aiming to achieve a certain LoA.

Naik and Jenkins [18] compare two SSI systems, namely Sovrin and uPort. A part of this work is also the evaluation of storage solutions for sensitive data, like the user's identity data or related cryptographic material, which details wallets.

4. Concept

This section details our generic concept with the main goal to achieve LoA high on a mobile phone-based identity wallet. We first introduce the involved actors, as shown in Figure 2. Next, we define requirements, which our system has to fulfill in order to achieve an LoA high. These requirements were the outcome of the assessment of the eIDAS implementation act as well as the ISO standard. Our concept consists of two main phases, depicted in Figure 2, and described Section 4.3. From our concept, we abstract measures that are used to fulfill our requirements detailed in Section 4.4.

4.1. Actors

- **User:** A user represents a person that wants to authenticate at an SP.
- **Identity Wallet:** The identity wallet is a software application running on the mobile phone utilizing the mobile phone's secure element to create, store, and use cryptographic key material. Additionally, this key material is protected through biometric encryption. Securely storing the identity data of the user is another objective of the wallet.
- **Hardware Key:** The hardware key is tamper-resistant hardware, which is used to create, store and use cryptographic key material. It provides a secure key-pair and supports key attestation so that the verifying party can ensure that a key used for singing something comes from secure hardware. This hardware key represents an additional authentication factor that strengthens the authentication.
- **Identity Provider (IdP):** In this concept, the IdP issues a related user's identity data after successful user authentication.
- **Verifier/Service Provider (SP):** In our concept, the verifier or service provider (SP) is a party to which the user wants to perform identification and authentication. This could either be a party that provides a service or a physical person like a police officer during a police check.
- **SSI Network:** The SSI network is responsible for hosting the DL. The nodes of the network are semi-trusted nodes like, for example, companies and organizations like banks, universities, etc. The nodes perform a consensus protocol to reach a consensus about what is written to the ledger. The SSI network serves as a decentralized public key infrastructure (DPKI).
- **Registration Authority:** The registration authority role can be taken over by any node of the SSI network. This role involves adding the user authenticated user to the SSI network. Notably, the node performing the user registration cannot see the identity data of the user.

[3] https://developer.arm.com/ip-products/security-ip/trustzone

4.2. Requirements

We have identified requirements based on the LoA standards assessment. These requirements have to be fulfilled in order to achieve an LoA high.

- **Binding of identity data to the user:** The identity data of a user must be bound to the related person.
- **Tamper-resistant storage of the key material:** The cryptographic key material used of a person for authentication must be stored in tamper-resistant storage.
- **Ensure the validity of the identity data:** The verifier must be able to verify the revocation status of the identity data of a user as well as the issuer.
- **Authentication mechanism:** The authentication mechanism must utilize multi-factor authentication to secure the revocation mechanism.
- **Identity Proving:** The user must prove her identity during the enrolment process. This can either be in person or the re-use of an already performed in-person identity proving.
- **Issuance of identity data:** The identity data must be issued to the related user only.
- **Revocation of identity data:** The IdP as well as the user, must be able to revoke the identity data.

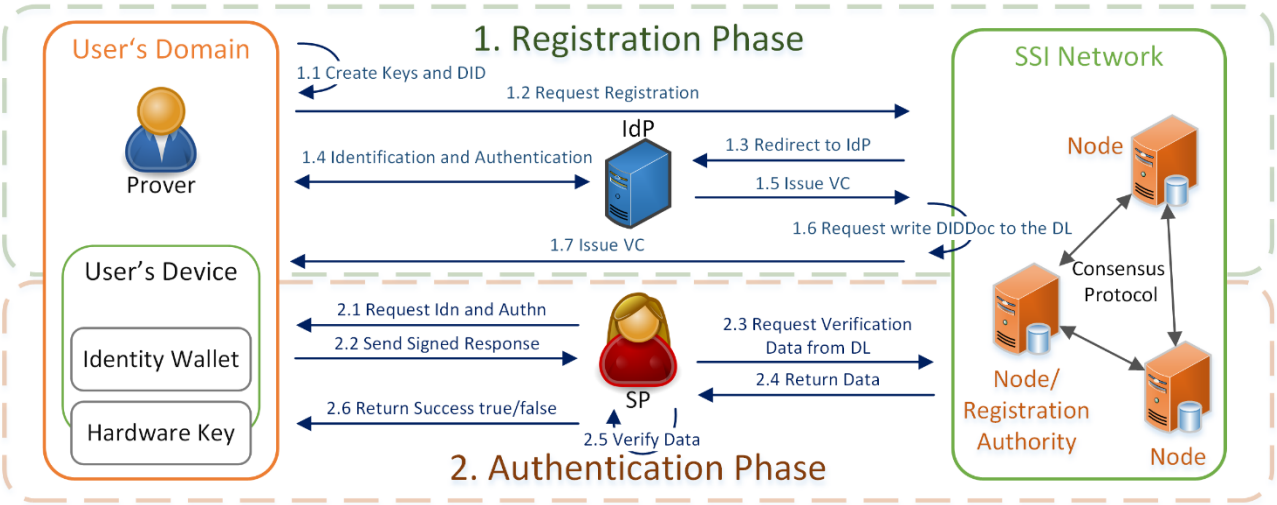

Figure 2: Overview of the Proposed Architecture including the main Actors and main Process Flows [10]

4.3. Phases Description

Our proposed concept consists of two main phases illustrated in Figure 2, namely the registration phase and the authentication phase. The registration phase deals with the enrolment of the user's identity data, including the binding of the data to the user as well as the identity proofing. The authentication phase deals with the actual authentication process towards an SP.

The registration phase starts at the user wallet by creating the public-private key-pairs. This concept involves two kinds of key pairs, first, a key pair on the mobile phone protected through biometric authentication second and a hardware key providing tamper-resistant storage. In the next step, The user requests registration at a registration authority. Each of the SSI nodes can take over the role of a registration authority. Next, the user is being redirected to the IdP to perform identification and authentication. Since we rely on the re-use of the identity proofing, the user has to perform a strong authentication towards the IdP. The IdP issues the credential for the user,

including the user's identity attributes. Additionally, revocation information will be written to the ledger as well. The identity assertion is encrypted for the user and issued to the registration authority. Next, the registration authority writes the DID document to the DL, which includes the public keys of the user. Finally, the identity credential is issued to the user and stored within the identity wallet.

The authentication phase deals with the fact that the user wants to perform identification and authentication either to access a service or resource or when verifying the identity during for example, a police check. It starts with the SP requesting identification and authentication of the user. The user creates and signs the response by using both keys, the wallet key on the mobile phone as well as the hardware key. The SP retrieves the DID document from the DL network containing the public keys of the user, a key attestation of the hardware key, as well as revocation information. The SP verifies the signatures using the public keys of the document. By verifying the key attestation, the SP can ensure that the hardware key was created and used on a special hardware created by a trusted hardware manufacturer. The revocation information state that the identity data are still valid. Finally, the SP verifies the identity attributes issued by the IdP. This phase concludes with successful or unsuccessful user authentication.

4.4. Measures

This subsection states the measures of our concept and further details how these measures are going to meet our defined requirements.

- **Identity Proving:** Since we are re-using already existing identity proving, we fulfill the requirement of identity binding.
- **Usage of Authorative IdP**: In our concept, we are using an IdP where the user already has an identity registered and also which supports an LoA high.
- **Authentication at IdP:** In our concept, the user performs strong authentication at the IdP in order to receive a VC.
- **Hardware Key:** We use a tamper-resistant hardware key store to fulfill the related requirement.
- **Hardware Key Attestation:** The hardware key used in this work supports key attestation, which is used to prove that the key is based on certain hardware from a trusted manufacturer.
- **Revocation Mechanism:** Our concepts include revocation, where the DL is utilized to store the revocation list. The verifier can retrieve revocation information during authentication. The user and the IdP are able to revoke a credential.
- **Mobile Phone with Biometry Support:** We utilize a mobile phone-based wallet that supports Biometric authentication like a fingerprint or face recognition to support both the binding to the actual user as well as to add an additional authentication factor.
- **Issue Encrypted VC:** We propose that the issued VC is encrypted for the related user from the IdP.

5. Conclusion

This work proposed a generic concept that serves as the foundation for other wallet projects if they aim to achieve an LoA high. In particular, during this project, we have evaluated related LoA standards and defined requirements that our concept has to fulfill. We further defined a generic concept and evaluated this by defining measures that address the before-mentioned requirements. We also illustrated the main process flows in our overall architecture diagram depicted in Figure 2. The full results are available in our scientific paper [10].

References

[1] B. Zwattendorfer, T. Zefferer, and K. Stranacher, “An overview of cloud identity management-models,” pp. 82–92, 2011.

[2] A. Abraham, “Self-Sovereign Identity,” pp. 1–39, 2017.

[3] B. Houtan, A. S. Hafid, and D. Makrakis, “A Survey on Blockchain-Based Self-Sovereign Patient Identity in Healthcare,” *IEEE Access*, vol. 8, pp. 90478–90494, 2020.

[4] A. Mühle, A. Grüner, T. Gayvoronskaya, and C. Meinel, “A Survey on Essential Components of a Self-Sovereign Identity,” *Comput. Sci. Rev.*, vol. 30, pp. 80–86, 2018.

[5] A. Abraham, K. Theuermann, and E. Kirchengast, “Qualified eID Derivation into a Distributed Ledger Based IdM System,” in *Proceedings - 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2018*, 2018.

[6] G. Kondova and J. Erbguth, “Self-Sovereign Identity on Public Blockchains and the GDPR,” in *Proceedings of the 35th Annual ACM Symposium on Applied Computing*, 2020.

[7] E. Commission, *Implementation Act 2015/1502*, vol. 235. 2015.

[8] International Standard Organisation (ISO), International Telecommunication Union (ITU), and International Electrotechnical Commission (IEC), “Information technology — Security techniques — Entity authentication assurance framework,” vol. 29115, 2011.

[9] P. A. Grassi James L Fenton Elaine M Newton Ray A Perlner Andrew R Regenscheid William E Burr Justin P Richer Privacy Authors, N. B. Lefkovitz Jamie M Danker Usability Authors, and Y.-Y. K. Choong Kristen Greene Mary F Theofanos, “Digital Identity Guidelines: Authentication and Lifecycle Management,” *Spec. Publ. (NIST SP) - 800-63B*, 2017.

[10] A. Abraham, C. Schinnerl, and S. More, “SSI Strong Authentication using a Mobile-Phone based Identity Wallet,” *Submiss.*, 2021.

[11] W3C, “Decentralized Identifiers (DIDs) v1.0 First Public Working Draft.” [Online]. Available: https://www.w3.org/TR/did-core/. [Accessed: 27-Jan-2020].

[12] “GitHub - jolocom/smartwallet-app: A decentralized self sovereign identity solution developed by Jolocom.” [Online]. Available: https://github.com/jolocom/smartwallet-app. [Accessed: 10-Mar-2021].

[13] “Dizme,” *2021*. [Online]. Available: https://www.dizme.io/. [Accessed: 09-Feb-2021].

[14] “Connect.me.” [Online]. Available: https://connect.me/. [Accessed: 10-Mar-2021].

[15] “GitHub - alastria/alastria-wallet: Wallet of ALASTRIA_ID.” [Online]. Available: https://github.com/alastria/alastria-wallet. [Accessed: 10-Mar-2021].

[16] W. Dai, Q. Wang, Z. Wang, X. Lin, D. Zou, and H. Jin, “Trustzone-based secure lightweight wallet for hyperledger fabric,” *J. Parallel Distrib. Comput.*, vol. 149, pp. 66–75, Mar. 2021.

[17] S. Iqbal *et al.*, “A Novel Mobile Wallet Model for Elderly Using Fingerprint as Authentication Factor,” *IEEE Access*, vol. 8, pp. 177405–177423, Sep. 2020.

[18] N. Naik and P. Jenkins, “Self-Sovereign Identity Specifications: Govern Your Identity through Your Digital Wallet using Blockchain Technology,” in *Proceedings - 2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering, MobileCloud 2020*, 2020, pp. 90–95.