What is a (Digital) Identity Wallet? A Systematic Literature Review

Blaž Podgorelec
Graz University Of Technology
Graz, Austria
blaz.podgorelec@iaik.tugraz.at

Lukas Alber
Graz University Of Technology
Graz, Austria
lukas.alber@iaik.tugraz.at

Thomas Zefferer
A-SIT Plus GmbH
Vienna, Austria
thomas.zefferer@a-sit.at

***Abstract*—Identity management is crucial for any electronic service that needs to authenticate its users. Different identity-management models have been introduced and rolled out on a large scale during the past decades. Key distinguishing criteria of these models are the storage location of users' identity data and the degree of involvement of central entities such as identity providers, which can potentially track user behavior. Growing privacy awareness has led to a renaissance of user-centric identity-management models during the past few years. In this context, especially the concept of wallets applied to the digital identity domain has recently attracted attention, putting users into direct control of their identity data. Various approaches and solutions relying on this concept have been introduced recently. However, no generally accepted definitions of the concept "digital identity wallet" and of its related features and implementations exist so far, leading to considerable confusion in this domain.**

This paper addresses this issue by providing a systematic literature review on wallets applied to the digital identity domain to identify, analyze, and compare existing definitions, features, and capabilities of such solutions. By means of two research questions, this paper thereby contributes to a better understanding of identity wallets and the various recent developments in this domain.

***Index Terms*—Identity management, identity, wallet, review**

I. Introduction

Intensified by the pandemic, digitalization is moving more and more transactions to the digital world. We increasingly use electronic services to declare taxes, access our vaccination and test certificates, or file applications at public administrations, to mention just a few examples. Many of these electronic services require users to authenticate, i.e., to prove their electronic identity (eID), before access to personalized services and data is granted. Secure and reliable user authentication is a complex task typically enabled by so-called identity-management (IdM) systems.

Different models for identity-management systems have been proposed, introduced, and applied in practice during the past decades. Most of these models have in common that they involve four entities: a service provider (SP) offering electronic services (e.g., a tax-declaration service), a user aiming to access these services, an identity provider (IdP) authenticating the user on behalf of the SP and providing the SP with the user's identity data, and a controlling party (CP) enforcing relevant regulations [1].

From a historical perspective, the first IdM model broadly applied was the so-called isolated model. As the most rudimentary among the models, it simply combines the SP and IdP in one component. Accordingly, each SP not only implements specific business logic but also features its own IdP. In this model, user authentication is not outsourced to an external entity. Consequently, the user has to register separately at each service provider, which then stores all required identity information of its users. That implies a high burden for the user since she has to remember separate credentials for each service provider [1] she aims to access and use.

The central identity model has solved the problem of SP-specific registrations. In this model, IdP functionality is outsourced and implemented by a separate entity, which multiple SPs can then employ. This approach allows users to register only once at this central IdP and later use the IdP to access different SPs. As multiple SPs outsource user authentication to one IdP, users can authenticate at all these SPs using the same credentials. This characteristic is advantageous in terms of usability. However, it makes the central IdP a single point of failure since the IdP stores required identity information of users for all SPs. Also, the central IdP is directly involved in all authentication processes. Hence can potentially learn which user authenticates at which service provider at which time. Such information could be used to track users and learn their behavior. Still, the central IdM model has found application broadly. One prominent early example of an IdM system following this model is Kerberos [2]. Other prevalent examples are Google Identity[1] or Apple ID[2], in which the role of the identity provider is assumed by Google and Apple, respectively.

The crux of the central identity model is that, in practice, multiple IdPs exists, which all serve their own set of SPs. Hence, a user registered at IdP A can only authenticate at SP X if IdP A serves SP X. If another IdP instead serves SP X, e.g., IdP B, the user either needs to register at that IdP B or is excluded from SP X. The federated IdM model solves this problem by establishing trust relationships between multiple

This work was supported by the European Union's Horizon 2020 Framework Programme for Research and Innovation under grant agreement No. 959072 (mGov4EU).

[1]https://developers.google.com/identity, accessed on 24.01.2021.
[2]https://appleid.apple.com/, accessed on 24.01.2021.

IdPs. The goal is to form a circle of trust. IdPs that are part of this circle can delegate authentication requests to each other. In the example above, IdP B can delegate an authentication request from SP X to IdP A, as this IdP can authenticate the user. The user's identity information is then compiled by IdP A and returned to IdP B, which can then continue as if it had authenticated the user itself. In this model, users' identity information is stored in a distributed way by different IdPs. A well-known example of a federated IdM system is the European eIDAS interoperability framework, which federates national IdM systems of EU Member States to enable cross-border authentication processes.

In all models discussed so far, the IdP stores the user's identity data. By successfully authenticating against the IdP, the users authorize the IdP to forward their identity information to the requesting SP. This central storage of identity information can be problematic, making the IdP an attractive target for attacks. Hence, an approach that exposes the user's identity data less is the so-called user-centric IdM model. Instead of storing the identity data at an IdP, the data is stored in the user's domain (e.g., on a smartcard or the user's smartphone protected with a hardware-based security element). The fact that the user always remains in possession and full physical control of her identity data gives the model advantage in terms of privacy [1]. Typical examples of such solutions are national IdM solutions relying on smartcards like the card-based Austrian Citizen Card [3] or the German eID [4]. In solutions following the user-centric model, required identity information is retrieved from the user domain (e.g., read from a smartcard) and forwarded to the requesting SP at each authentication process. Still, some central IdP is typically in place, which merely serves as middleware between the SP and the token storing the identity information.

Recent developments like Self-Sovereign Identity (SSI) go even one step further. While user-centric IdM solutions are still dependent in most cases on central IdPs, SSI aims to make the user the sole sovereign of her credentials. That is achieved through central authority agnostic identity data and peer-to-peer authentication. In many cases, a distributed ledger is used by various IdPs in the corresponding circle of trust to register new credentials. These credentials are then directly issued to the requesting user [5]. Examples of this model are the European Self-Sovereign Identity Framework (ESSIF)[3] or Veramo[4].

Recent steps in the historical development of identity-management systems indicate a trend towards user-controlled identity data. In this context, the term identity wallet has recently attracted attention. The trend has also been noticed by the European Commission. They recently published a proposal for a new European Digital Identity [6], which is also based mainly on the concepts of identity wallets. The Commission's proposal aims to extend and partly replace provisions of the EU's eIDAS Regulation [7]. The eIDAS Regulation currently defines the use and mutual acceptance of State-issued eIDs amongst the Member States. The proposal demonstrates that identity wallets are regarded as a future key technology in the eID domain not only by technicians but also by policymakers.

Unfortunately, the term *digital identity wallet* is only vaguely defined. Like many buzz words, the term is currently used (and misused) in multiple contexts and for multiple technical concepts and solutions. That adds significant confusion to discussions about the topic. To tackle this unsatisfying situation, we provide a thorough review of digital wallets in the digital identity domain while examining their underlying technical concepts and investigating opportunities, barriers, and current trends. The overview we present in this paper is developed through a systematic literature review and a survey of related scientific contributions. With the help of two concrete research questions, existing scientific work is analyzed to compile a clear picture of digital identity wallets and their underlying concepts.

The remainder of this paper is structured as follows. In Section II, the systematic literature-review approach is detailed, and two research questions are defined. It is followed by Section III, where thirteen groups of papers that passed the rigorous reviewing process are identified and presented. Next, Section IV employs the knowledge gathered from the review process to answer the previously defined research questions and to create a taxonomy of the wallet domain. Finally, we draw relevant conclusions in Section V.

II. Research method

We performed a systematic literature review based on the state-of-the-art method introduced by Kitchenham and Charters [8], wherein the review process is divided into three major phases. In the first phase, the review is planned, comprising the specification of research questions and the development of a review protocol. In the next phase, the review is conducted, including identification and selection of primary studies followed by data extraction and synthesis. In the third and last phase, the review's results are reported. The essential steps of the first and the second phase are recapitulated in this section, while obtained review results are presented and discussed in Section III.

A. Research Questions

To specify well-formatted research questions for the systematic literature review, we utilized the PICOC (*Population, Intervention, Comparison, Outcome, Context*) method criteria framework as defined in [8, 9]. In the targeted domain of digital wallets and digital identities, *Population* refers to digital wallets that are in some way used or play a role in the domain of digital identity. *Intervention* that affects the Population refers to characterization, data extraction, and synthesis actions. For the conducted review, the *Comparison* criterion is irrelevant, as no comparison will be performed. The *Outcome* of Intervention comprises the reasons for utilizing a digital wallet in the digital identity domain and the principal features of such a digital wallet. The Intervention on the

[3]essif-lab.eu, accessed on 11.01.2021.

[4]veramo.io, accessed on 14.01.2021.

before-mentioned Population will be carried out in the *Context* of academic peer-reviewed articles.

With the help of the applied PICOC criteria framework, we had identified and clarified the main concepts that were the focus of this research and derived the following two research questions:

- **RQ1**: What are the primary motivations for applying digital wallets in the digital identity domain?
- **RQ2**: What are the main features of digital wallets concerning digital identity, i.e., digital identity wallets?

B. Identification and Selection of Studies

To identify relevant studies for the literature review, we composed a search strategy consisting of two phases. The automated search on selected academic databases was performed in the first phase. The following academic databases, mostly used when performing systematic literature reviews on computer science-related fields, were selected: IEEEXplore, ACM, ScienceDirect, Web of Science, and SCOPUS. The search was performed using search strings within the databases' search engines. The search string was composed of the keyword *Wallet* indicating digital wallet, and the keyword *Identity* describing digital identity domain. The two keywords were combined with the logical operator *AND*. A logical operator was used to restrict results to studies incorporating both concepts in the respective article's metadata (i.e., Title, Abstract, or Keywords). That yielded the final search string: *Wallet AND Identity*.

Studies considered in the review phase had to satisfy some predefined inclusion and exclusion criteria. Concretely, considered studies had to be written in English language (IC1), scientifically peer-reviewed (IC2), content-wise related to the specified keywords and research questions (IC3), and available as a full paper in digital academia databases (IC4). Therefore, considered studies were not allowed to be published as Editorial, Abstract, Poster, Demonstrators or Short Paper (EC1), scientifically non-peer-reviewed (EC2), and were not allowed to be content-wise unrelated to the specified keywords and research questions (EC3).

It should be noted that some of the inclusion and exclusion criteria could already be used thanks to the database search engines. Figure 1 shows that after extraction of all the relevant studies (i.e., 285 studies in total) from academic databases using the search string as mentioned earlier within automated search, IC1, IC2, IC4, EC1, and EC2 were applied, which decreased the total number of relevant studies to 253. After we removed duplicate studies, the search resulted in 141 studies. All the other inclusion and exclusion criteria (i.e., IC3 and EC3) were applied within the next important step in the study selection process, i.e., Screening. In the Screening step, we read 141 studies titles and abstracts and manually rejected irrelevant studies for the conducted review. This step reduced the number of relevant studies to 42. We continued the Screening step, where we read the full text of the remaining 42 studies thoroughly, reducing the number of relevant studies to 23. These 23 studies were finally accepted for review.

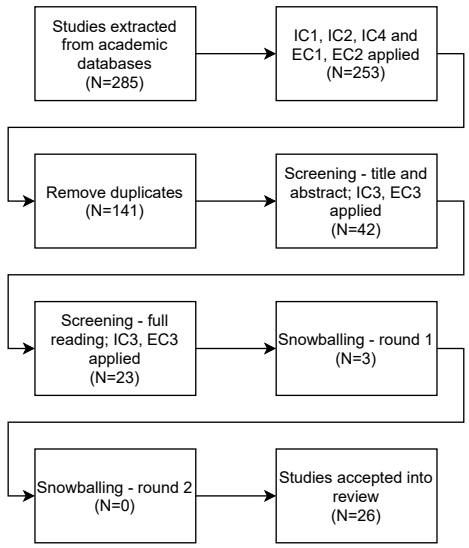

Fig. 1. Study identification and selection process.

We identified 23 relevant studies that concluded the first phase of the applied search strategy. The 23 identified studies then served as input to the search strategy's second phase. In this second phase, we applied the Snowballing method to identify additional studies that should be considered in the review but had been for any reason missed within the automated search approach we performed in the first phase. The Snowballing method includes two techniques for identifying relevant studies, i.e., Backward Snowballing, which identifies new studies using a reference list, and Forward Snowballing, where new studies are identified based on citations of already examined studies. The input of studies, i.e., start set examined within Snowballing, are the studies that have been identified and selected based on automated search in the first phase. The Snowballing method is iterative and executed as long as new studies can be identified. Newly identified studies then serve as input for the next Snowballing iteration. All studies identified in an iteration were screened by applying the screening process already known from the first phase. As depicted in Figure 1, in the first iteration of Snowballing, we identified, selected, and accepted to the literature review three new studies. However, the second iteration of Snowballing already did not yield any new study to be accepted for the literature review. Thus, we accepted a total of 26 studies to the review phase.

C. Data Extraction and Synthesis

We thoroughly read the studies accepted for our literature review to extract the necessary information and answer the predefined research questions. For this reason, a data-extraction form, consisting of the following items, was outlined to ensure the equal processing of all studies: Study ID, Title, Author, Year, Keywords, IdM considered, Digital wallet features, Conclusions. Based on extracted data, a synthesis strategy was defined. The initial step in data synthesis was to group studies from the same authors or authors with the same content-

wise concepts. This step comprised the studies accepted in the review phase that were logical successors, predecessors, or content-wise related to the same domain of the same subset of authors. After that, the extracted data relevant to answer each predefined research question was additionally synthesized, i.e., categorized on the iterative definition to be ready for analysis to provide answers to the predefined research questions.

III. Results

As a result of the steps mentioned above, we identified thirteen contentwise related groups. Each group is comprised of one or more studies. A brief overview of identified groups is presented in Table I, while below each group and identified study is described in more detail and placed in the scope of our research. Further, we extracted the IdM in the focus and information about the role of the digital wallet from each identified group of studies. The aforementioned extracted information was reconsidered and synthesized when answering RQ1. Moreover, we extracted information concerning digital wallet features for each group of studies. Extracted pieces of information were later synthesized and in-depth analyzed when answering RQ2.

The first group is comprised of two studies by Abraham et al. [10, 11]. In [10], the authors extended the SSI model to support revocation and offline verification. In [11], the authors proposed a new generic concept that could enable mobile-based identity wallets to achieve an eIDAS-defined Level of Assurance High. In the context of these studies, the identity wallet was utilized to support the SSI model paradigm, including the Decentralized Identifier (DID) system, and to ensure that the identity-related data remains stored with the user on her mobile device. The identity wallet was used for storing and managing cryptographic material, identifiers, and identity data (in the form of Verifiable Credentials), including controlled sharing of identity-related information upon user consent.

The second group includes a study by Augusto and Correia [12]. A novel, user-centric identity management was proposed in the domain of the federated IdM. In the scope of the study, a digital identity wallet acts as an authorization broker to avoid a massive aggregation of users' identity attributes. Therefore, a digital identity wallet on a mobile device was used to store and aggregate identity attributes together with related cryptographic material inside a secure element. However, a wallet was also used to manage and revoke access to identity attributes towards a Relying Party (i.e., Service Provider).

The third group is comprised of articles by Bandara et al. [16, 14, 13, 15]. In [16] authors proposed a Cyber Threat Information platform, in [14] a Know Your Customer (KYC) platform, and in [13, 15] a digital contact tracing platform. The blockchain-based SSI model with an SSI-enabled mobile wallet was incorporated in all studies. A mobile identity wallet was used to store identity-related data, including cryptographic material, in a secure, local storage, while the identity proof, i.e., DID, was written in a blockchain network. The mobile wallet enables users to capture/verify identity proofs and share identity information between wallets upon user consent. The digital wallet was introduced to overcome privacy concerns related to storing identity data in centralized storage platforms and building data silos that could lead to massive data breaches.

The fourth group is comprised of two articles by Bernabe et al. [17, 18] that in the scope of the reliAble euRopean Identity EcoSystem (ARIES) project proposed a new identity-management system based on SSI principles that enable the use of privacy-preserving mobile identities through the usage of a secure mobile identity wallet. Linkage of identity-related attributes and identity providers to Relying Parties (i.e., Service Providers) was prevented with the identity wallet that acts as mediate. The identity wallet is part of a mobile application and stores identity-related data, including cryptographic material in secure storage (i.e., in the mobile device's secure element). A digital wallet was presented as a means by which the user could manage his identity data. Moreover, the authors stated that identity data should be exported from identity wallets only upon user consent, and if possible, selective disclosure of identity data should be enabled.

The fifth group is comprised of studies by Gajek et al. [19, 20] and Bugiel et al. [21]. A new approach was presented to prevent classical and malware phishing attacks in the domain of centralized IdM. The approach is based on ideas of compartmentalization for isolating applications of different trust levels and trusted wallets. In [19, 20], a wallet-based authentication tool was introduced to enable secure storage of identity-related information, including cryptographic material, and to protect web-based authentication procedures. With a wallet, transfer (i.e., share) of identity-related data to Relying Parties (i.e., Service Providers) became possible. A digital wallet was used as an instrument that protects web-based authentication and acts as a man-in-the-middle proxy in the browser on behalf of the user between server and storage of identity-related data (i.e., login credentials). In that manner, authors claimed that identity theft through phishing attacks could be prevented. In [21], the authors proposed a further extension of the digital wallet to enable the protection of login credentials used in web browsers on mobile platforms. This addition was achieved by extending a digital wallet with secure hardware elements on mobile devices.

The sixth group is comprised of six studies [22, 23, 24, 25, 26, 27] published in the scope of the EU-funded research project CREDENTIAL - Secure Cloud Identity Wallet European. Because of the lack of privacy-preserving storage and advanced identity sharing services in the domain of Identity as a Service, a novel user-centric cloud-based data storage and sharing platform that enhances user privacy was proposed. Thus, a user could store, control, and share identity data and other sensitive data in a cloud wallet. However, the cloud provider never has access to plain (i.e., unencrypted) data because advanced cryptographic techniques (e.g., re-encryption, malleable digital signatures) are applied. The designated identity wallet acts as privacy-preserving storage deployed in the cloud, including sharing services based on selective disclosure.

TABLE I
STUDIES ACCEPTED INTO REVIEW CATEGORIZED IN GROUPS.

Group	Studies in group	Brief description
# 1	[10], [11]	Extends the SSI model with support for revocation and offline verification and presents a novel mobile-based identity wallet to achieve eIDAS LoA high.
# 2	[12]	Proposes a novel framework for user-centric IdM.
# 3	[13], [14], [15], [16]	Presents a mobile-based identity wallet based on blockchain-based SSI applied on different domains (i.e., threat information exchange and contact tracing).
# 4	[17], [18]	Proposes a novel IdM framework based on SSI principles.
# 5	[19], [20], [21]	Presents a wallet-based authentication tool for web-based authentication that prevents phishing knowing the authorized servers within a centralized IdM.
# 6	[22], [23], [24], [25], [26], [27]	Introduces a novel end-to-end secure and privacy-preserving cloud-based identity wallet.
# 7	[28]	Presents a holistic view of the DID system.
# 8	[29]	Proposes a context-aware service system architecture based on identity interchange layer including mobile digital identity wallet.
# 9	[30]	Proposes several specifications to evaluate any SSI IdM solution.
# 10	[31]	Derives privacy requirements for browser-based attribute exchange.
# 11	[32] [33]	Examines a proof of concept digital wallet in the SSI context and provides a novel practical decentralized key recovery solution.
# 12	[34]	Demonstrates how blockchain-based SSI can be used to solve challenges of KYC processes.
# 13	[35]	Introduces a decentralized, interoperable approach to IdM, discusses challenges of centralized IdM and investigates current developments of verifiable credentials and digital wallets.

The usage of data stored in the wallet is transparent to the user and can be exported from the identity wallet only with her consent.

In [28], which is the only study comprising the seventh group, the authors provided a holistic view on DID system. It serves to understand different DID building blocks that enable the SSI model, including identity wallet and its interactions with the DID system components. The DID identity wallet was presented as a piece of the software part of the Agent (Cloud or Edge). It serves as secure storage for identity-related data (in the form of Verifiable Credentials) and other cryptographic material (DID signing and verification keys, link secret, agent policy keys, and secret value commitments). Therefore, an identity wallet was used to avoid the storage centralization of identity-related data. Also, it enables user control over identity, aggregation of identity-related data (i.e., sharing), backup, and recovery.

The eighth group includes a study by Kim et al. [29]. In the scope of the user-centric IdM, the authors presented an identity interchange layer, including a mobile digital identity wallet. The latter is a personalized context-aware agent on a personal device. Every user's identity-related information flows through a digital identity wallet. The user can control when identity information is provided (i.e., shared) to the requesting entity – which can be done only upon user consent. With a digital identity wallet, storage and management of identity-related data (i.e., credentials) are provided. Moreover, the wallet use allows complete control, enabling users to enforce their security and privacy policies.

The ninth group is comprised of only one study by Naik and Jenkins [30], which built on existing specifications for evaluating federated IdM and proposed new specifications for evaluation of any SSI model. A digital wallet was described as a maintainer (i.e., storage) of all identity-related information fully controlled by the user (i.e., identity owner), who typically owns the device (i.e., edge agent) where the digital wallet resides. Digital wallet was introduced to give users control over identity-related data, including identity recovery and sharing of identity upon user consent. As secure storage of all identity-related information, the digital wallet could also be part of the Cloud agent, which should be protected from unauthorized access and enable full control and ownership of identity-related data only to the identity owner.

The tenth group consists only of one study by Pfitzmann and Waidner [31]. The authors derived the privacy requirements of browser-based attribute-exchange protocols from general privacy principles. The browser-based attribute exchange is a three-party protocol that enables users to send identity-related information (i.e., attributes) via browser (i.e., client) to some destination site (i.e., to service provider) without remembering or typing them. In this protocol, the authors introduced a digital wallet to strengthen the privacy and security of identity-related data. The authors stated that the digital wallet could operate in different environments depending on where exchangeable information resides. Therefore authors differentiated between the local environment, i.e., local digital wallet where identity-related information to be exchanged reside on the user's local machine, and the remote environment, i.e., remote digital wallet where identity-related information to be exchanged reside at some other machine. Regardless of its actual type, the wallet was described as a collection (storage) of identity-related information (i.e., attributes), including cryptographic material and methods to use them. Moreover, the authors stated that the wallet should only send, i.e., share identity-related information to the service provider upon the user's explicit consent.

Two studies by Soltani et al. [32, 33] form the eleventh group. In those studies, a proof-of-concept digital wallet in

the context of SSI was examined, and a novel practical decentralized key recovery solution was proposed. A digital wallet was described as software that runs on a smartphone and acts as the electronic version of a physical wallet. It securely stores identity-related information, including cryptographic material, on the mobile device within the secure element. Moreover, a digital wallet is able to connect with other entities to exchange information (e.g., for user authentication). Besides, within a digital wallet, only the identity owner, i.e., the user, should be able to perform operations with identity-related information, for which cryptographic means are required. Thus, a digital wallet was introduced to empower users to control identity-related data, including cryptographic material, mitigate password-based authentication, decrease data fragmentation, and prevent identity breaches.

In [34], which is part of the twelfth group, the authors demonstrated how blockchain-based SSI using DIDs could be applied to solve the challenges of KYC processes. A digital wallet, also called a digital agent, operated on a smartphone, computer, or cloud, serves as storage for DIDs, cryptographic materials, and identity-related information (e.g., credentials). Users have complete control over their data, regardless of the storage, i.e., digital wallet location (e.g., edge or cloud). Moreover, the authors stated that data stored in the digital wallet could be shared, and the digital wallet should enable backups of identity-related information. Hence, a digital wallet was introduced to foster user control of identity-related data, avoid centralization storage, and enhance privacy.

The last and thirteenth group consists of a study by Sedlmeir et al. [35]. In this study, the authors discussed the challenges of the centralized IdM, examined current trends in development regarding verifiable credentials, and emphasized that digital wallets could be a promising research area. A digital wallet was presented as a tool for storing identity-related data (i.e., verifiable credentials), including cryptographic material on mobile devices or any other edge device or cloud. The authors stated that users could control digital identity-related data and share it with other stakeholders using a digital wallet. Moreover, the authors stated that with digital wallets, identity silos could be avoided, users' privacy and security increased, and fast-machine exchange of identity-related information enabled.

This section described and exposed essential data of all 13 identified groups of studies accepted into the review, relevant and crucial to recognizing the primary motivations for applying digital wallets in the digital identity domain and identifying the main features of such digital identity wallets. In the next section, that data is further utilized and analyzed to provide an answers to the predefined research questions.

IV. Discussion of Results

Based on the data extracted from the categorized groups of studies presented in Section III, this section discusses findings and synthesizes data. This way, answers to the predefined research questions are derived.

As can be observed from Table II, most groups of studies (9 of 13) reported that digital wallets were introduced to the digital identity domain in order to improve the storage security of identity-related data and to enhance user privacy when sharing identity-related data with service providers (M1). The second most recognized motivation for introducing digital wallets to the digital identity domain (mentioned in 7 of 13 studies groups) was to avoid centralization of identity-related data (M2) and thus prevent the formation of large data silos of identity-related data. To keep identity-related data under user control (M3) was noted as motivation in 4 of 13 studies groups. Facilitating ease of use of digital identity (M4) was reported in 3 of 13 studies groups. IdM, which was in the focus of each group of studies, and the environment, where digital wallet operates were extracted to understand better the motivations for introducing digital wallets into the identity domain. All extracted pieces of information are presented in Table II.

While we already described IdMs in Section I, it is crucial to recognize, define, and also describe the environments in which digital wallets are supposed to operate. Two environments where digital wallets operate were identified from extracted data: local and remote environments. In a remote environment – also called a Cloud environment – the digital wallet's infrastructure is not owned and managed directly by the user but by the remote-environment provider. In contrast, the user controls and owns the required infrastructure (e.g., a mobile device) in the local environment.

Except for one group of studies, the local environment was identified in most of the studies (12 of 13). However, in some studies (5 of 13), both (i.e., local and remote environments) were identified as possible. Nonetheless, in the majority (7 of 13), only the local was identified as the digital wallet's environment. In those groups of studies (9), where security and privacy were recognized as motivation to apply digital wallets to the digital identity domain (M1), most of the studies (5 of 9) identified the local environment as the sole environment where a digital wallet operates. However, in 3 out of 9 studies, both environments were mentioned as options. In contrast, only one group of studies identified the remote environment suitable for a digital wallet solely. Almost the same pattern occurred in groups of studies (7) where avoiding centralization (M2) was specified as the primary motivation for introducing digital wallets into the digital identity domain. The majority of those groups (4 of 7) foresee only the local environment. Nevertheless, in 3 out of 7 studies, both environments were identified. In groups (4), where providing control over identity-related data (M3) was defined as motivation, half of the groups foresee only the local environment, and half of the groups mentioned both environments are possible. Further, only a remote environment should be in place was identified in 1 out of 3 groups of studies motivated to ease the use of digital identity (M4). In comparison, 2 out of 3 groups mentioned both environments as possible. Based on these results, it can be concluded that those groups of studies, where security and privacy of identity-related data (M1), avoiding centralization (M2), and providing control (M3) were the primary motivations for introducing digital wallets, mainly assumed or suggested to operate digital wallets in a local

TABLE II

IDM, DIGITAL WALLET ENVIRONMENT, MOTIVATIONS BEHIND APPLYING DIGITAL WALLET TO DIGITAL IDENTITY DOMAIN, AND IDENTITY DIGITAL WALLET FEATURES IDENTIFIED WITHIN GROUPS OF STUDIES ACCEPTED INTO THE REVIEW.

Group	IdM	Environment	(M1) Security & privacy	(M2) Centralization	(M3) Provide control	(M4) Ease of use	(F1) Store identity data	(F2) Manage identity data	(F3) Share identity data	(F4) Store crypto material	(F5) Combine identity data	(F6) Recover & backup
#1	SSI	Local	○	●	●	○	●	●	●	●	●	○
#2	Federated	Local	○	●	○	○	●	●	●	●	●	○
#3	SSI	Local	●	●	○	○	●	●	●	●	●	○
#4	SSI	Local	●	○	○	○	●	●	●	●	●	○
#5	Centralized	Local	●	○	○	○	●	●	●	●	○	●
#6	as a Service	Remote	●	○	○	●	●	●	●	○	●	○
#7	SSI	Remote or Local	○	●	○	○	●	●	●	●	●	●
#8	User-centric	Local	●	○	○	○	●	●	●	●	○	○
#9	SSI	Remote or Local	○	○	●	○	●	●	●	●	○	●
#10	Centralized	Remote or Local	●	○	○	○	●	●	●	●	○	○
#11	SSI	Local	●	●	●	○	●	●	●	●	○	●
#12	SSI	Remote or Local	●	●	●	●	●	●	●	●	●	●
#13	SSI	Remote or Local	●	●	○	●	●	●	●	●	●	○

environment. In contrast, requirements related to ease-of-use typically (M4) lead to digital wallets being operated in a remote environment.

In IdM solutions that most frequently apply digital wallets, i.e., SSI (8 of 13 studies groups), the environment is called an agent and is either Cloud (referring to the remote environment) or Edge (referring to the local environment, most usually mobile device). The motivation to enhance security and privacy (M1) was recognized within all identified IdM models. At the same time, the SSI model was in the focus of 6 out of 7 groups of studies, in which avoiding centralization (M2) was described as motivation. Only one group describing the avoidance of centralization as motivation (M2) focused on federated IdM. All groups where control over identity-related data (M3) was identified focused on SSI IdM. The Identity as a Service model was in the focus of one group of studies with ease-of-use motivation (M4), while two other groups of studies with the same motivation had SSI IdM in their focus.

Based on the discussed findings, which were extracted and synthesized from studies accepted into the review, we are now able to provide the following answer to Research Question 1:

The primary motivations for applying digital wallets to the digital identity domain are to avoid digital identity-related data centralization, enhance the security and privacy of identity-related data, provide control over identity-related data under user responsibility, and ease the use of digital identities.

The features of digital wallets applied to the digital identity domain were extracted and synthesized from studies accepted for review. They are presented in Table II separately for each identified group of studies. In all groups of studies, the following three digital-wallet features regarding the digital identity domain have been identified: storing identity-related data (F1), managing identity-related data (F2), and sharing identity-related data (F3).

Identity-related data storing refers to the digital-wallet feature that enables storage of identity and identity-related inside a digital wallet (F1). A feature that enables users to manage and control their identity-related data (F2) covers the following functionalities: select identity data to be stored in a digital wallet (FN2.1), remove identity data from the digital wallet (FN2.2), review identity data stored in a digital wallet (FN2.3), and select identity data to be shared outside the digital wallet (FN2.4).

Select identity data to be stored functionality (FN2.1) enables the user to decide which identity data should be stored in a digital wallet and enriches the storing identity-related data feature (F1), which focuses solely on storing abilities of the digital identity wallet. Similarly, the select identity data to be shared outside digital wallet functionality (FN2.4) extends the sharing identity-related data feature (F3). Thus with select identity data to be shared outside digital wallet functionality (FN2.4), only the user can (by providing explicit consent) decide which identity data could be exposed, i.e., shared out of a digital wallet. However, the sharing identity-related data feature (F3) focuses solely on the sharing abilities of identity-related data stored in the digital identity wallet.

The three features (F1, F2, and F3) mentioned above have been identified in all groups of studies, which implies that they are independent of the IdM and the digital wallet operating environment. The digital wallet feature, which describes the capacity of a digital wallet to store cryptographic material related to digital identity securely (F4), was identified in 12 of

13 groups of studies. All these groups presented the local or remote environment where the digital wallet can operate. In contrast, the only group of studies where the feature mentioned above (F4) was not identified envisioned that the digital wallet operates only in a remote environment, and identity-related cryptographic material is stored out of the scope of a digital wallet.

Next, the feature that a digital wallet applied in the digital identity domain should allow identity data to be combined before being shared outside the digital wallet (F5), including selective disclosure, was identified in 8 of 12 groups of studies. This feature (F5) could be understood as an extension of select identity data to be shared outside the digital wallet functionality (FN2.1). However, no pattern related to the digital wallet identity data-combining feature (F5) was identified with relation to IdM and the digital-wallet environment.

The last identified feature of the digital wallet, applied to the digital identity domain, was specified in 5 out of 13 groups. It describes the digital wallet's ability to recover and backup identity data (F5). However, in those studies, such a feature was partially always realized by using specific characteristics of the digital-wallet environment. Therefore, it could not be identified fully as a desired feature of the digital wallet applied on the digital identity domain.

Based on the findings extracted from studies, which were accepted into the review, and which have been discussed in this section, we are now able to provide the following answer to Research Question 2:

The digital identity wallet is software that operates in the remote or local environment and enables the storing, managing, and sharing of digital identity-related data. The digital identity wallet also provides secure storage for cryptographic material associated with digital identity-related data. With a digital identity wallet, the user controls and manages identity-related data. That includes removing and reviewing identity-related data stored in the wallet and explicitly selecting what identity-related data to store/share into/outside the wallet. Moreover, when selecting identity-related data to be shared outside the digital identity wallet, a user should be able to combine different identity-related data. Additionally, with the support of the underlying environment, a digital identity wallet can recover and back up identity-related data.

V. Conclusion

This paper provides a systematic review of literature on digital wallets applied to the digital identity domain. To support the systematic approach, we initially defined two research questions. Subsequently, we first identified relevant studies, then extracted data, and finally synthesized the remaining studies to answer these questions. That way, this paper revealed motivations for applying digital wallets in the digital identity domain and examined features provided by digital identity wallets. Even more important, this paper is – to the best of our knowledge – the first to survey and study the role of digital wallets in the digital identity domain, to contextualize relevant and frequently used terms and concepts related to digital wallets, and to hence provide a comprehensive overview of this increasingly important topic.

In future work, we plan to extend the systematic review, e.g., by extending the scope of considered scientific works and by defining further research questions with the goal further to enrich the overview of the state-of-the-art. Also, we aim to put particular focus on analyzing and incorporating input provided by the European Commission. The latter has recently published a proposal for a new European Digital Identity, which is also largely based on the concepts of identity wallets. These activities are supposed to further boost the relevance of digital-wallet technology, especially in Europe, and lift digital wallets' relevance to a new stage. Keeping an overview of relevant concepts and ongoing activities is vital for fully employing this technology's potential. The work presented in this paper and future extensions shall contribute towards that goal.

References

[1] B. Zwattendorfer, T. Zefferer, and K. Stranacher, "An overview of cloud identity management-models," in *WEBIST 2014 - Proceedings of the 10th International Conference on Web Information Systems and Technologies, Volume 1, Barcelona, Spain, 3-5 April, 2014*, V. Monfort and K. Krempels, Eds. SciTePress, 2014, pp. 82–92. [Online]. Available: https://doi.org/10.5220/0004946400820092

[2] C. Neuman, T. Yu, S. Hartman, and K. Raeburn, "The kerberos network authentication service (V5)," *RFC*, vol. 4120, pp. 1–138, 2005. [Online]. Available: https://doi.org/10.17487/RFC4120

[3] H. Leitold, A. Hollosi, and R. Posch, "Security architecture of the austrian citizen card concept," in *18th Annual Computer Security Applications Conference (ACSAC 2002), 9-13 December 2002, Las Vegas, NV, USA*. IEEE Computer Society, 2002, pp. 391–400. [Online]. Available: https://doi.org/10.1109/CSAC.2002.1176311

[4] J. Fromm and P. Hoepner, "The new german eid card," *Handbook of eID Security: Concepts, Practical Experiences, Technologies*, pp. 154–166, 2011.

[5] A. Abraham, C. Schinnerl, and S. More, "SSI strong authentication using a mobile-phone based identity wallet reaching a high level of assurance," in *Proceedings of the 18th International Conference on Security and Cryptography, SECRYPT 2021, July 6-8, 2021*, S. D. C. di Vimercati and P. Samarati, Eds. SCITEPRESS, 2021, pp. 137–148. [Online]. Available: https://doi.org/10.5220/0010542801370148

[6] "Proposal for a regulation of the european parliament and of the council amending regulation (eu) no 910/2014 as regards establishing a framework for a european digital identity," June 2021. [Online].

Available: https://digital-strategy.ec.europa.eu/en/library/trusted-and-secure-european-e-id-regulation

[7] "Regulation (eu) no 910/2014 of the european parliament and of the council of 23 july 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing directive 1999/93/ec," July 2014. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2014/910/oj

[8] B. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering," 2007.

[9] M. Petticrew and H. Roberts, *Systematic reviews in the social sciences: A practical guide*. John Wiley & Sons, 2008.

[10] A. Abraham, S. More, C. Rabensteiner, and F. Hörandner, "Revocable and offline-verifiable self-sovereign identities," in *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. IEEE, 2020, pp. 1020–1027.

[11] A. Abraham, C. Schinnerl, and S. More, "Ssi strong authentication using a mobile-phone based identity wallet reaching a high level of assurance," in *Proceedings-8th International Conference on Security and Cryptography (SECRYPT 2021)*, 2021.

[12] A. B. Augusto and M. E. Correia, "Ofelia–a secure mobile attribute aggregation infrastructure for user-centric identity management," in *IFIP International Information Security Conference*. Springer, 2012, pp. 61–74.

[13] E. Bandara, X. Liang, P. Foytik, S. Shetty, C. Hall, D. Bowden, N. Ranasinghe, K. De Zoysa, and W. K. Ng, "Connect-blockchain and self-sovereign identity empowered contact tracing platform." in *MobiHealth*, 2020, pp. 208–223.

[14] E. Bandara, X. Liang, P. Foytik, S. Shetty, and K. De Zoysa, "A blockchain and self-sovereign identity empowered digital identity platform," in *2021 International Conference on Computer Communications and Networks (ICCCN)*. IEEE, 2021, pp. 1–7.

[15] E. Bandara, X. Liang, P. Foytik, S. Shetty, C. Hall, D. Bowden, N. Ranasinghe, and K. De Zoysa, "A blockchain empowered and privacy preserving digital contact tracing platform," *Information Processing & Management*, vol. 58, no. 4, p. 102572, 2021.

[16] E. Bandara, X. Liang, P. Foytik, and S. Shetty, "Blockchain and self-sovereign identity empowered cyber threat information sharing platform," in *2021 IEEE International Conference on Smart Computing (SMARTCOMP)*. IEEE, 2021, pp. 258–263.

[17] J. B. Bernabe, A. Skarmeta, N. Notario, J. Bringer, and M. David, "Towards a privacy-preserving reliable european identity ecosystem," in *Annual Privacy Forum*. Springer, 2017, pp. 19–33.

[18] J. B. Bernabe, M. David, R. T. Moreno, J. P. Cordero, S. Bahloul, and A. Skarmeta, "Aries: Evaluation of a reliable and privacy-preserving european identity management framework," *Future Generation Computer Systems*, vol. 102, pp. 409–425, 2020.

[19] S. Gajek, A.-R. Sadeghi, C. Stuble, and M. Winandy, "Compartmented security for browsers-or how to thwart a phisher with trusted computing," in *The Second International Conference on Availability, Reliability and Security (ARES'07)*. IEEE, 2007, pp. 120–127.

[20] S. Gajek, H. Löhr, A.-R. Sadeghi, and M. Winandy, "Truwallet: trustworthy and migratable wallet-based web authentication," in *Proceedings of the 2009 ACM workshop on Scalable trusted computing*, 2009, pp. 19–28.

[21] S. Bugiel, A. Dmitrienko, K. Kostiainen, A.-R. Sadeghi, and M. Winandy, "Truwalletm: Secure web authentication on mobile platforms," in *International Conference on Trusted Systems*. Springer, 2010, pp. 219–236.

[22] F. Karegar, C. Striecks, S. Krenn, F. Hörandner, T. Lorünser, and S. Fischer-Hübner, "Opportunities and challenges of credential," in *IFIP International Summer School on Privacy and Identity Management*. Springer, 2016, pp. 76–91.

[23] F. Karegar, D. Lindegren, J. S. Pettersson, and S. Fischer-Hübner, "Assessments of a cloud-based data wallet for personal identity management," in *26th International Conference on Information Systems Development (ISD2017 Cyprus). Larnaca, Cyprus, September 6-8, 2017*, 2017.

[24] A. Kostopoulos, E. Sfakianakis, I. Chochliouros, J. S. Pettersson, S. Krenn, W. Tesfay, A. Migliavacca, and F. Hörandner, "Towards the adoption of secure cloud identity services," in *Proceedings of the 12th International Conference on Availability, Reliability and Security*, 2017, pp. 1–7.

[25] S. Krenn, T. Lorünser, A. Salzer, and C. Striecks, "Towards attribute-based credentials in the cloud," in *International Conference on Cryptology and Network Security*. Springer, 2017, pp. 179–202.

[26] U. Haböck and S. Krenn, "Breaking and fixing anonymous credentials for the cloud," in *International Conference on Cryptology and Network Security*. Springer, 2019, pp. 249–269.

[27] F. Veseli, J. S. Olvera, T. Pulls, and K. Rannenberg, "Engineering privacy by design: lessons from the design and implementation of an identity wallet platform," in *Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing*, 2019, pp. 1475–1483.

[28] B. G. Kim, Y.-S. Cho, S.-H. Kim, H. Kim, and S. S. Woo, "A security analysis of blockchain-based did services," *IEEE Access*, vol. 9, pp. 22 894–22 913, 2021.

[29] S.-H. Kim, S.-R. Cho, and S.-H. Jin, "Context-aware service system architecture based on identity interchange layer," in *2008 10th International Conference on Advanced Communication Technology*, vol. 2. IEEE, 2008, pp. 1482–1486.

[30] N. Naik and P. Jenkins, "Self-sovereign identity specifications: Govern your identity through your digital wallet using blockchain technology," in *2020 8th IEEE International Conference on Mobile Cloud Computing,*

Services, and Engineering (MobileCloud). IEEE, 2020, pp. 90–95.

[31] B. Pfitzmann and M. Waidner, "Privacy in browser-based attribute exchange," in *Proceedings of the 2002 ACM workshop on Privacy in the Electronic Society*, 2002, pp. 52–62.

[32] R. Soltani, U. T. Nguyen, and A. An, "Practical key recovery model for self-sovereign identity based digital wallets," in *2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*. IEEE, 2019, pp. 320–325.

[33] ——, "Decentralized and privacy-preserving key management model," in *2020 International Symposium on Networks, Computers and Communications (ISNCC)*. IEEE, 2020, pp. 1–7.

[34] V. Schlatt, J. Sedlmeir, S. Feulner, and N. Urbach, "Designing a framework for digital kyc processes built on blockchain-based self-sovereign identity," *Information & Management*, p. 103553, 2021.

[35] J. Sedlmeir, R. Smethurst, A. Rieger, and G. Fridgen, "Digital identities and verifiable credentials," *Business & Information Systems Engineering*, vol. 63, no. 5, pp. 603–613, 2021.