A Review on Digital Wallets and Federated Service for Future of Cloud Services Identity Management

Fatemeh Stodt and Christoph Reich
Institute for Data Science, Cloud Computing, and IT Security; Furtwangen University,
Robert-Gerwig-Platz 1, 78120 Furtwangen, Germany
{Fatemeh.Stodt, Christoph.Reich}@hs-furtwangen.de

***Abstract*—In today's technology-driven era, managing digital identities has become a critical concern due to the widespread use of online services and digital devices. This has led to a fragmented landscape of digital identities, burdening individuals with multiple usernames, passwords, and authentication methods. To address this challenge, digital wallets have emerged as a promising solution. These wallets empower users to store, manage, and utilize their digital assets, including personal data, payment information, and credentials. Additionally, federated services have gained prominence, enabling users to access multiple services using a single digital identity. Gaia-X is an example of such a service, aiming to establish a secure and trustworthy data infrastructure. This paper examines digital identity management, focusing on the application of digital wallets and federated services. It explores the categorization of identities needed for different cloud services, considering their unique requirements and characteristics. Furthermore, it discusses the future requirements for digital wallets and federated identity management in the cloud, along with the associated challenges and benefits. The paper also introduces a categorization scheme for cloud services based on security and privacy requirements, demonstrating how different identity types can be mapped to each category.**

***Index Terms*—Digital wallet, Identity management, Federated service, Cloud**

I. Introduction

The management of digital identities has become a critical concern in today's digital age [1]. With the increase of online services and the widespread use of digital devices, individuals are constantly required to provide personal information to access different platforms, services, and applications [2]. This has led to a fragmented landscape of digital identities, where users have to manage multiple usernames, passwords, and authentication methods, which can be both cumbersome and insecure [3].

Digital wallets have emerged as a promising solution to tackle the challenge of managing digital identities [4]. These software applications enable users to conveniently store, manage, and utilize various digital assets, such as personal data, payment information, and credentials.

In addition, Gaia-X, a groundbreaking project [5], exemplifies the importance of federated services and the significant benefits they offer. Gaia-X is designed to provide users with a robust and secure data infrastructure, empowering them with unprecedented control over their personal information [6]. By adopting Gaia-X's unified digital wallet, users can conveniently access multiple platforms and services with a single digital identity, streamlining the management of their digital presence while bolstering security and privacy. This usercentric approach not only enhances individual control but also promotes innovation and competition within the digital landscape, reinforcing the advantages of Gaia-X's federated service model.

In the contemporary digital landscape, the significance of effective digital identity management cannot be emphasised enough. Fortunately, emerging solutions such as digital wallets and federated services provide promising avenues to address this intricate challenge. This paper aims to delve into the concept of digital identity management and shed light on its applications, specifically within the realm of digital wallets and federated services. Additionally, we will explore the utilisation of digital wallets for accessing cloud services, offering insights into their benefits and potential challenges.

The structure of this paper is as follows: Section II provides background information on digital wallets and federated services. Section III discusses the requirements for identity management in wallets to access the cloud. Section IV categorises cloud access based on identity group levels. Finally, in Section V, we draw a conclusion.

II. Background (State of the Art)

This section provides an overview of two key components: Digital Wallets and Federated Services, which play pivotal roles in ensuring secure and efficient digital experiences.

A. Digital Wallet

The digitisation of transactions has accelerated, particularly in response to the pandemic, resulting in an increased reliance on electronic services. Users now engage in various activities, such as tax declarations, accessing vaccination and test certificates, and interacting with public administrations, through digital platforms [7]. To access these services, users must authenticate themselves and provide electronic identification (eID) to secure personalised services and data. This authentication process is facilitated by identity management (IdM) systems, which ensure reliable and secure user authentication.

Digital wallets have emerged as a crucial component in managing identities in the digital identity domain. A digital wallet is a secure and encrypted storage solution that allows users to store and manage their digital identities, credentials,

 ISBN: 978-1-68558-043-8

and other relevant information [8]. It acts as a central repository where users can securely store their authentication data, such as usernames, passwords, and digital certificates [9].

Digital wallets offer several advantages in identity management [10]. They provide convenience by allowing users to have a single repository for all their identities across different services and platforms. Users can store and manage multiple sets of credentials within their digital wallet, eliminating the need to remember separate usernames and passwords for each service provider. This simplifies the user experience and reduces the cognitive burden of managing multiple identities [11].

Various models of identity management systems have emerged over the years. The isolated model, where each service provider has its own identity provider (IdP), was the earliest and most prevalent [12]. However, this model requires users to register separately with each service provider, resulting in the burden of managing multiple credentials. To address this, the central identity model was introduced, outsourcing the IdP functionality to a central entity that multiple service providers can utilise [13]. Users only need to register once with the central IdP and can then access various services with the same set of credentials.

While the central identity model improves usability, it raises concerns about the central IdP becoming a single point of failure and potential privacy breaches. To overcome these challenges, the federated IdM model was introduced, establishing trust relationships among multiple IdPs [14]. This model allows users registered with one IdP to authenticate themselves to service providers served by other IdPs within a circle of trust. An example is the European eIDAS interoperability framework [15], which enables cross-border authentication processes by federating national IdM systems of EU Member States.

Another approach is the user-centric IdM model, where identity data is stored in the user's domain, such as on a smartcard or a smartphone with a hardware-based security element [16]. Users retain control over their identity data, enhancing privacy. National IdM solutions utilising smartcards, such as the Austrian Citizen Card and the German eID, exemplify this model. During authentication, the necessary identity information is retrieved from the user's domain and forwarded to the requesting service provider.

Recent advancements include the concept of Self-Sovereign Identity (SSI), where users have sole control over their credentials [17] [10]. SSI reduces reliance on central authorities by utilising distributed ledgers among multiple IdPs within a circle of trust for registering new credentials. Initiatives like the European Self-Sovereign Identity Framework (ESSIF) [18] and Veramo [19] embody this model. These developments reflect a trend towards user-controlled identity data and have attracted attention from policymakers, as evident in the European Commission's proposal for a new European Digital Identity.

The OpenWallet Foundation (OWF) has emerged as a new opportunity in the realm of digital wallets [20]. Established under the umbrella of the Linux Foundation Europe, OWF aims to develop open-source software that facilitates interoperability across a broad spectrum of wallet applications [21]. These applications encompass various use cases, including payments, identity verification, and the secure storage of validated credentials.

B. Federated Services

The concept of a federated catalogue plays a vital role in identity management by facilitating the discovery and access to various services through a centralised repository [6]. In a federated catalogue model, multiple catalogues collaborate and share information about available services, creating a unified and comprehensive resource for users [22]. This collaborative approach allows users to search, browse, and access services from different providers using a single interface, streamlining the process of service discovery.

Inter-catalogue synchronisation is a critical aspect of federated catalogues. It ensures that information about services, including their availability, descriptions, and attributes, remains up-to-date and consistent across different catalogues. Through inter-catalogue synchronisation mechanisms, updates and changes made in one catalogue can be propagated and reflected in others, maintaining data integrity and ensuring accurate and real-time information for users. This synchronisation process enables a seamless user experience, where users can rely on the federated catalogue to provide reliable and consistent information about services.

The integration of wallets with federated catalogues introduces an additional layer of functionality and convenience to identity management [23]. Wallets, which store and manage users' digital identities and associated credentials, can interact with federated catalogues to enhance the service discovery and access process. When a user accesses the federated catalogue through their wallet, the wallet can authenticate the user and provide relevant identity information to the catalogue. This interaction enables personalised service recommendations, tailored search results, and seamless authentication and authorisation processes, ultimately enhancing the user experience and security.

Federated services and federated catalogues are closely intertwined concepts in identity management. Federated services rely on federated catalogues to provide a centralised and comprehensive view of available services, allowing users to discover and access services using a single digital identity. The collaboration between service providers and catalogues within a federated model streamlines identity management processes, as the catalogue acts as a trusted intermediary, enabling authentication, authorisation, and seamless information exchange between users and service providers [24].

III. Requirements for Identity Wallets for Future Clouds

As cloud computing continues to shape the digital landscape, effective identity management becomes paramount to ensure secure and seamless access to cloud services. In this

 ISBN: 978-1-68558-043-8

section, we delve into the categorisation of identities required for different cloud services, discuss their unique requirements and characteristics, explore the future requirements for digital wallets and federated identity management in the cloud, identify potential challenges in implementing identity wallets for future clouds, and highlight the potential benefits of using digital wallets for identity management in the cloud.

Categorising identities according to their usage in different cloud services provides a comprehensive understanding of the diverse identity landscape. These identities can be broadly classified into user identities, service identities, and device identities. User identities represent individuals accessing cloud services, service identities are associated with specific cloud services or applications, and device identities pertain to the authentication and authorisation of devices interacting with cloud resources. Each identity category has distinct requirements and characteristics that must be considered to ensure effective identity management.

R1: Secure storage of identity-related data: In the context of cloud services, it is crucial to securely store identity and identity-related information. This requirement ensures that sensitive data associated with user identities, service identities, and device identities is stored in a protected manner, safeguarding the integrity and confidentiality of the data.

R2: Effective management of identity-related data: Managing identity-related data in the cloud encompasses various functionalities. These include the ability to select, remove, and review identity data stored within the cloud environment, as well as the capability to choose which identity data should be shared outside the cloud. Such management ensures that users have control over their stored information, promoting privacy and data control.

R3: Secure sharing of identity-related data: Enabling the secure sharing of stored identity-related data outside the cloud is a critical requirement for cloud-based identity management. This involves establishing secure communication channels and protocols for sharing identity data with trusted entities, ensuring that data integrity and confidentiality are maintained during the sharing process.

R4: Secure storage of cryptographic material: As the cloud environment handles digital identities, it becomes essential to securely store cryptographic material related to digital identity. This requirement focuses on the need to protect cryptographic elements, such as keys and certificates, ensuring their confidentiality and preventing unauthorised access.

R5: Combining identity data before sharing: In the cloud context, the requirement to combine identity data before sharing aligns with the concept of selective disclosure. Users should have the ability to selectively share identity data, combining relevant information based on specific sharing requirements. This ensures privacy and controlled sharing of identity-related data.

The use of digital wallets for identity management in the cloud offers a range of benefits. Digital wallets enhance user convenience by providing a centralized platform for managing identities across multiple cloud services. They bolster security through secure authentication mechanisms, robust encryption of identity data, and efficient access control. Moreover, digital wallets empower users by giving them control over their personal information and the ability to selectively share it with trusted entities. The integration of digital wallets with federated identity management further streamlines identity management processes, enabling seamless access to cloud resources and promoting interoperability.

TABLE I
COMPARISON BETWEEN DIFFERENT DIGITAL WALLET BASED ON IDM AND WALLET REQUIREMENTS

Reference	IdM	Environment	R1	R2	R3	R4	R5
[17]	SSI	Local	✓	✓	✓	✓	✓
[23]	Federated	Local	✓	✓	✓	✓	✓
[9]	Centralized	Local	✓	✓	✓	✓	✗
[15]	as a Service	Remote	✓	✓	✓	✗	✓
[16]	User-centric	Local	✓	✓	✓	✓	✗
[13]	Centralized	Remote or Local	✓	✓	✓	✓	✗
[10]	SSI	Remote or Local	✓	✓	✓	✓	✓
[20], [21]	SSI	Remote or Local	✓	✓	✓	✓	✓

In this context, Table I provides a comprehensive comparison between different digital wallets based on their identity management (IdM) capabilities and wallet requirements. This table serves as a valuable reference for understanding the strengths and features of various digital wallet solutions in relation to identity management. It highlights key factors such as authentication mechanisms, encryption techniques, access control capabilities, and user control features. By referring to Table 1, readers can gain insights into the specific characteristics and functionalities of each digital wallet, aiding in the selection of an appropriate solution for their identity management needs.

IV. ACCESS MANAGEMENT AND CATEGORISING IDENTITIES FOR CLOUD SERVICES

In the realm of cloud computing, it is crucial to consider the security and privacy requirements of different types of cloud services. In this section, we introduce a categorisation scheme that classifies cloud services based on their security and privacy requirements. We then explore how different types of identities can be mapped to each category, considering their respective security and privacy features. Furthermore, we provide practical examples to illustrate how this categorisation scheme can guide the selection of the appropriate identity type for a given cloud service.

The categorisation scheme for cloud services is designed to capture the varying degrees of security and privacy requirements across different service types. We propose a three-tier categorisation: low-security services, moderate-security services, and high-security services as shown in Figure 1. Low-security services typically involve non-sensitive data and require minimal protection measures. Examples include publicly accessible websites or public information repositories. Moderate-security services handle moderately sensitive data, such as personal information or internal organisational documents. High-security services, on the other hand, handle highly

 ISBN: 978-1-68558-043-8

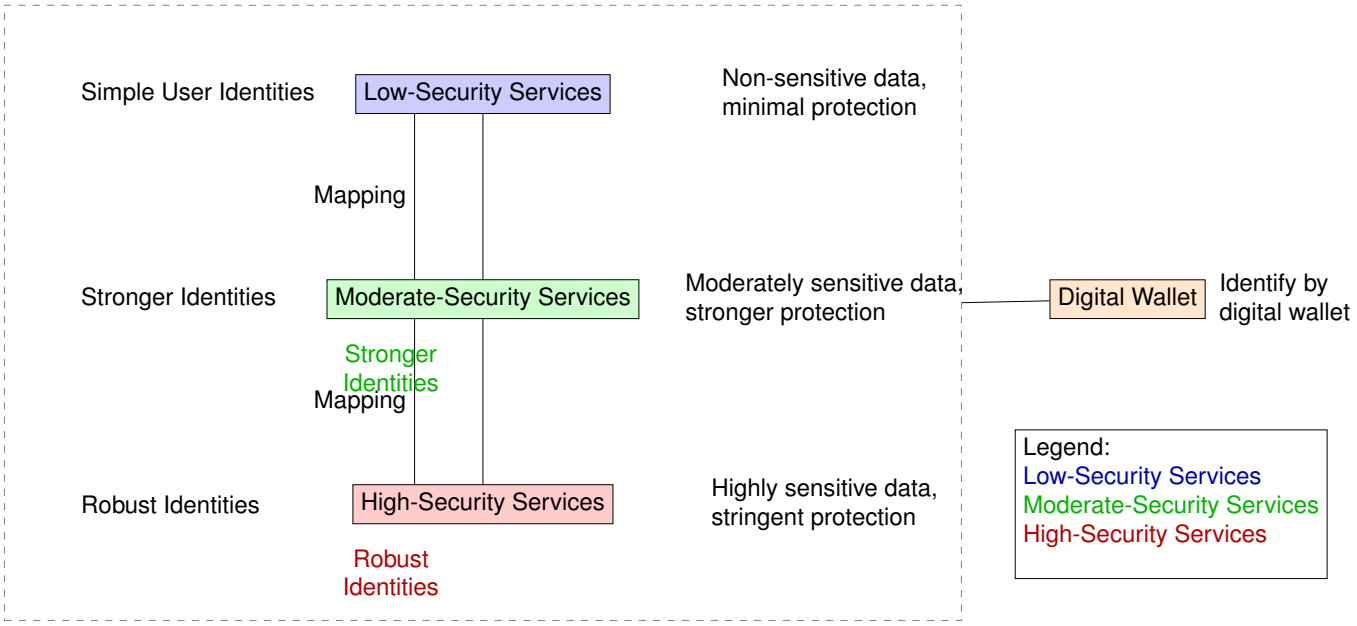

Fig. 1. Categorization of Cloud Services and Identity Types

sensitive data, such as financial records or health information, and demand stringent security measures.

Mapping different types of identities to each category is vital to align the level of security and privacy features with the corresponding cloud service. For low-security services, simple user identities, such as usernames and passwords, may be sufficient for authentication and access control. However, moderate-security services may require stronger authentication mechanisms, such as two-factor authentication or biometrics, to enhance security. High-security services necessitate even more robust identity types, such as digital certificates or hardware tokens, to ensure the highest level of protection and privacy for sensitive data.

To illustrate the practical application of this categorisation scheme, let us consider an example. Suppose a cloud service involves a public-facing web application that provides access to general information about a company. Based on the categorisation scheme, this service would fall under the low-security category. Consequently, a simple user identity, such as a username and password, would be sufficient to authenticate users and manage access to the service. However, if the same company offers a cloud-based Customer Relationship Management (CRM) system that handles customer data, the service would be classified as a moderate-security service. In this case, a stronger identity type, such as two-factor authentication or biometrics, would be necessary to ensure the security and privacy of customer information.

V. Conclusion

In conclusion, digital wallets and federated services offer significant advantages in digital identity management. Digital wallets provide a secure and convenient way for users to store and manage their digital assets, simplifying the management of digital identities while enhancing security and privacy. The emergence of different identity management models, including federated and user-centric approaches, along with advancements like Self-Sovereign Identity (SSI), empower users with greater control over their credentials. Projects like Gaia-X exemplify the aim to give users increased control over their personal information and foster innovation in the digital realm.

Moving forward, future research should focus on integrating emerging technologies such as blockchain and decentralised identity systems to further enhance the security and privacy of digital wallets and federated services. Additionally, exploring the usability and user experience aspects of these solutions can drive their adoption and acceptance among users. Continued efforts in research and development will contribute to addressing the complex challenges of digital identity management and ensure its importance in today's digital era.

Acknowledgement

This research was funded by the Federal Ministry of Education and Research (BMBF) under reference number COSMIC-X 02J21D144, and supervised by Projektträger Karlsruhe (PTKA).

References

[1] P. J. Windley, *Digital Identity: Unmasking identity management architecture (IMA).* " O'Reilly Media, Inc.", 2005.

[2] A. Rashid and A. Chaturvedi, "Cloud computing characteristics and services: a brief review," *International Journal of Computer Sciences and Engineering*, vol. 7, no. 2, pp. 421–426, 2019.

[3] S. Rajamanickam, S. Vollala, R. Amin, and N. Ramasubramanian, "Insider attack protection: Lightweight password-based authentication techniques using ecc," *IEEE Systems Journal*, vol. 14, no. 2, pp. 1972–1983, 2019.

 ISBN: 978-1-68558-043-8

[4] D. R. Malik, D. A. Kataria, and D. N. Nandal, "Analysis of digital wallets for sustainability: A comparative analysis between retailers and customers," *International Journal of Management*, vol. 11, no. 7, 2020.
[5] A. Braud, G. Fromentoux, B. Radier, and O. Le Grand, "The road to european digital sovereignty with gaia-x and idsa," *IEEE network*, vol. 35, no. 2, pp. 4–5, 2021.
[6] B. Otto, "A federated infrastructure for european data spaces," *Communications of the ACM*, vol. 65, no. 4, pp. 44–45, 2022.
[7] M. M. Alam, A. E. Awawdeh, and A. I. B. Muhamad, "Using e-wallet for business process development: Challenges and prospects in malaysia," *Business Process Management Journal*, vol. 27, no. 4, pp. 1142–1162, 2021.
[8] M. A. Hassan and Z. Shukur, "Device identity-based user authentication on electronic payment system for secure e-wallet apps," *Electronics*, vol. 11, no. 1, p. 4, 2022.
[9] 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.
[10] 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.
[11] R. Dhamija and L. Dusseault, "The seven flaws of identity management: Usability and security challenges," *IEEE Security & Privacy*, vol. 6, no. 2, pp. 24–29, 2008.
[12] B. Zwattendorfer, T. Zefferer, and K. Stranacher, "An overview of cloud identity management-models." *WEBIST (1)*, pp. 82–92, 2014.
[13] 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.
[14] N. Selvanathan, D. Jayakody, and V. Damjanovic-Behrendt, "Federated identity management and interoperability for heterogeneous cloud platform ecosystems," in *Proceedings of the 14th international conference on availability, reliability and security*, 2019, pp. 1–7.
[15] C. Cuijpers and J. Schroers, "eidas as guideline for the development of a pan european eid framework in futureid," 2014.
[16] 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.
[17] A. Abraham, C. Schinnerl, and S. More, "Ssi strong authentication using a mobile-phone based identity wallet reaching a high level of assurance." in *SECRYPT*, 2021, pp. 137–148.
[18] D. Du Seuil, "European self sovereign identity framework," 2019.
[19] "Veramo," https://veramo.io/, 2023, accessed: Jun 27, 2023.
[20] T. South and R. Mahari, "Justice in a vaccum?" 2023.
[21] A. Kudra, "Self-sovereign identity (ssi) in deutschland: Projekte mit strahlkraft für die globale community," *Datenschutz und Datensicherheit-DuD*, vol. 46, no. 1, pp. 22–26, 2022.
[22] M. Gaedke, J. Meinecke, and M. Nussbaumer, "A modeling approach to federated identity and access management," in *Special interest tracks and posters of the 14th international conference on World Wide Web*, 2005, pp. 1156–1157.
[23] V. Siska, V. Karagiannis, and M. Drobics, "Building a dataspace: Technical overview," 2023.
[24] K. Bernsmed, M. G. Jaatun, P. H. Meland, and A. Undheim, "Security slas for federated cloud services," in *2011 Sixth International Conference on Availability, Reliability and Security*. IEEE, 2011, pp. 202–209.

 ISBN: 978-1-68558-043-8