Journal of the Association for Information Systems (2024) 25(3), pp. 522-527, doi: 10.17705/1jais.00887

Organizational Identity Management Policies

Alexander Rieger,[1,2] Tamara Roth,[1,2] Johannes Sedlmeir,[2] Gilbert Fridgen,[2] Amber Young

[1]Sam M. Walton College of Business, University of Arkansas, USA

[2]Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg, Luxembourg,

Abstract

Effective identity management is essential for secure organizational processes, but organizations often do not approach it strategically. To break this trajectory, organizational policymakers need to define a clear and sustainable identity management strategy. This paper presents an overview and guidelines to help shape such strategy. It analyzes the key characteristics and trade-offs of today's identity management models. Moreover, it offers practical recommendations for organizational policymakers when choosing among these models.

Keywords: Authentication, Digital Wallets, Identity and Access Management (IAM), Identity Models, Trade-offs

Introduction

Identity management challenges are as old as humankind. In the Book of Genesis, Jacob disguises himself with goat fur to confuse his father and steal his brother Esau's birthright. During the early days of Rome, Carthaginian general Hannibal used a signet ring taken from slain Roman consul Marcellus to deceive Rome's allies (Livius, 1943; Sheldon, 2015). These challenges continue in a digital world where secure but efficient identity management is essential for various organizational processes (Smith & McKeen, 2011; Windley, 2023).

Yet many organizations do not approach identity management strategically. Rather, organizations often purchase pre-packaged software solutions and assign the IT department responsibility for identity management. IT departments may be tempted to focus on security over usability, leading to inconvenient policies, such as rules for long and complex passwords or extensive multifactor authentication. As a result, users may spend more time authenticating or proving their identity than receiving the service.

To break this trajectory, we advocate for a strategic approach to identity management. Specifically, we propose that organizational policymakers define a strategy for managing their users' identity data. In what follows, we outline key policy questions that organizational policymakers should ask as they engage in developing an identity management strategy. We begin with a high-level description of today's dominant models for identity management and their strategic trade-offs in terms of control vs. responsibility and convenience vs. security. We then present recommendations for developing a fitting organizational policy.

Today's Identity Models and Their Trade-Offs

Organizational identity management is typically concerned with user authentication, source verification, and the storage of identity data. *User authentication* describes how users (persons, organizations, or IoT devices) can prove their identity as previously registered. These proofs are typically generated with so-called credentials or authentication factors. These factors can be "something the user knows" (e.g., a password), "something the user is" (e.g., face or fingerprint), or "something the user has" (e.g., an ID card, a temporary code, or a hardware token) (Benantar, 2005; Lacity et al., 2023; Windley, 2023). *Source verification* allows organizations to validate the correctness of identity claims made by a user, such as being a certain age or possessing a valid driver's license.

There are three identity management models available today to realize user authentication, source verification, and the storage of identity data: fragmented, federated, and wallet-based. While the fragmented and federated models are in use worldwide, the wallet-based model is being pushed in Europe, Canada, and a few US states. We describe each model in turn and contrast them in Table 1.

Table 1. Description and Organizational Trade-Offs Associated with the Three Identity Models

	Fragmented Model	**Federated Model**	**Wallet-based Model**
Description	***Enrollment and source verification:*** Users create an account with the organization and fill in a form with required identity attributes. When source verification of identity attributes is required, the organization must employ costly digital or in-person verification processes. ***Identification and authentication:*** Users log in to their account with a username-password combination or passkey as well as additional authentication factors if required.	***Enrollment and source verification:*** Users create an account with the organization and authorize their SSO provider to forward required identity attributes. When SSO providers do not offer source verification, the organization must employ the same processes as in the fragmented model. ***Identification and authentication:*** Users are redirected to their SSO provider, where they log in with a username-password combination or passkey as well as additional authentication factors if required.	***Enrollment and source verification:*** Users create an account with the organization and forward the required identity attributes from a digital wallet. The organization can easily verify the provided attributes using cryptographic checks that are sent together with the identity attributes. ***Identification and authentication:*** Users log in to their account with their digital wallet. Additional authentication factors are limited to those required to log in to the digital wallet app.
Control vs. responsibility	***Control:*** The organization collects and stores users' identity attributes. ***Responsibility:*** The organization is responsible for complying with regulatory requirements for the processing of user identity attributes.	***Control:*** The organization can outsource the collection and storage of identity attributes to SSO providers. ***Responsibility:*** The organization can delegate to the SSO provider some of the responsibility for complying with regulatory requirements for the processing of user identity attributes.	***Control:*** The organization can outsource the collection and storage of identity attributes to users. ***Responsibility:*** Users are responsible for managing their identity attributes and consenting to requests for presentation.
Convenience vs. security	***Convenience:*** Password management is tedious for users. Passkeys are more convenient but require users and the organization to abide by the rules of the passkey ecosystem. In both cases, source verification is slow, costly, and error-prone for the organization. ***Security:*** Security is limited without complex password rules, multifactor authentication, and user compliance with security policies.	***Convenience:*** SSO services are convenient for users and some SSO providers deliver source-verified identity data in a standardized format to the organization. ***Security:*** The likelihood of security incidents is low due to substantial security measures on the SSO provider side, but their impact can be severe.	***Convenience:*** Digital wallet apps are convenient for users and deliver source-verified identity data in a standardized format to the organization. ***Security:*** The likelihood and impact of security incidents are low as individual wallets are relatively unattractive targets for hacks.

The *fragmented model* describes the familiar experience of having separate accounts with username-password logins for each digital service. This model is easy to set up and gives organizations direct access to a trove of personal data that can be used, e.g., for marketing purposes. However, enrolling new users can be costly—especially when know-your-customer laws require organizations to verify physical identity documents. Moreover, when an organization stores sensitive identity data, securing the data against loss, unauthorized use, and hacks requires significant investment (Windley, 2023). The fragmented model also presents an undesirable trade-off between convenience and security when users need to choose unique and ever stronger passwords to keep up with mounting security threats. Password managers offer some help, but they are honeypots for hackers (Winder, 2023). Furthermore, user experience suffers when additional authentication factors are required and when they differ substantially across organizations. Some of these challenges can be addressed with so-called passkeys that replace username-password logins with cryptographic keys stored on mobile devices. Passkeys are highly secure by design and can be protected, for instance, with biometrics (FIDO Alliance, 2023). However, passkeys do not address costly enrollment and source verification problems (Yeoh et al., 2023).

The *federated model* mitigates these challenges. It limits the use of username-password logins, passkeys, and additional authentication factors to a small number of single sign-on (SSO) services by the likes of companies such as Alphabet, Apple, Meta, and Microsoft. The consistent authentication offered by the federated model makes it convenient for users. The federated model is also convenient for organizations, as they can outsource their responsibility for identity data management to SSO providers. However, ceding control over authentication to SSO providers can be problematic from a compliance and strategy perspective (Smith & McKeen, 2011). Source verification by SSO providers is also often limited, e.g., to phone numbers and driver's licenses. Moreover, cases abound in which SSO providers falsely blocked users and were slow to correct their mistakes (Hill, 2022). Lastly, SSO services are known for tracking user behavior on the web (Zuboff, 2015).

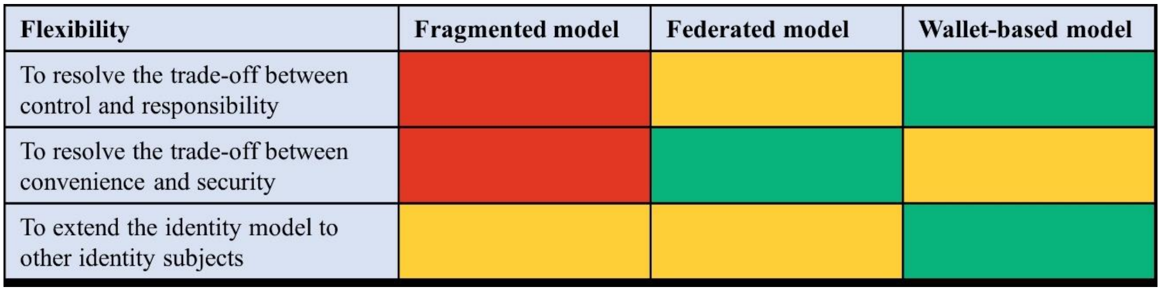
The *wallet-based model* is different in that it puts more control and responsibility for identity management on users. The European Union, along with several Canadian provinces and a few US states, is touting it as the future of identity management (Rieger et al., 2022; Sedlmeir et al., 2021). Under this model, users collect cryptographically verifiable identity attributes from trustworthy issuing organizations. The wallet-based model is convenient for users because digital wallets make passwords and multifactor authentication redundant (Lacity et al., 2023). It can also drastically reduce enrollment, source verification, and authentication costs. The downsides of the wallet-based model are that it is still immature and requires compatibility with identity wallets and solutions for device loss or theft. Moreover, organizations need to define policies for the trustworthiness and acceptance of identity attributes from different issuing organizations.

Three Recommendations for Organizational Policymakers

Identity management seems to be a rather mundane topic to some organizations, but it is a Rosetta Stone for solving many of the challenges organizations face in their processes today. We thus encourage organizational policymakers to take a strategic approach to identity management and carefully choose between the three different models. We next present three recommendations for making this choice.

Organizational policymakers should first consider the trade-off between control and responsibility. User and usage data can be highly relevant for some organizations, be it for the personalization of services, market segmentation, or the identification of opportunities for cross- and upselling. For these organizations, the costs associated with collecting and storing identity data may be well spent. If the organization is not using this data productively, outsourcing its protection to SSO providers may be wise. Yet, outsourcing identity management to SSO providers introduces strategic dependencies. Alternatively, they can ask their users to assume more responsibility. This can be helpful to reduce the organization's costs for secure storage of identity data and to support users across jurisdictions. However, controlling one's own identity data can be demanding for users. Increased user agency requires educated users (e.g., in terms of how to detect phishing attacks, how to create backups for recovery, etc.), and many users may not be skilled enough to manage their data or willing to tolerate high levels of responsibility.

Second, organizational policymakers should strike a balance between convenience and security. External SSO services may be convenient and more secure than most organizational services but do not always offer the required levels of source verification. For some organizations, the balance will need to be on the side of security. Compromised medical or financial processes, for instance, are not only embarrassing but can have serious consequences for affected users. For these processes, federated or wallet-based models may be the better choice. Where instances of incorrect identity data are inconsequential, policymakers should also consider whether identity data requires costly source verification.



Flexibility	Fragmented model	Federated model	Wallet-based model
To resolve the trade-off between control and responsibility	🟥	🟨	🟩
To resolve the trade-off between convenience and security	🟥	🟩	🟨
To extend the identity model to other identity subjects	🟨	🟨	🟩

Figure 1. Flexibility Associated with the Three Identity Models.

Finally, organizational policymakers should think beyond customer identities before selecting a model. Using the same model to manage identities and access for customers and employees, suppliers, partner organizations, and even IoT devices may substantially reduce complexity and costs (Glöckler et al., 2023; Guggenberger et al., 2023; Sedlmeir et al., 2023). In this regard, the wallet-based model may trump the other two models. Policymakers should also consider the political landscapes in which they operate. In certain industries and certain countries, regulators may mandate certain identity models. The European Union, for instance, will mandate the wallet-based model for customer identity management in various industries (European Commission, 2024). Organizational policymakers should be aware of these mandates and consider adopting the same model for other users to streamline IT processes across the organization.

Figure 1 summarizes these recommendations and offers an indication of the ability of the three identity models to align with them. While the federated and wallet-based models may often provide more flexibility than the fragmented model, it is important to carefully consider their strategic implications. Ultimately, there is no "fire and forget" solution for identity management. Instead, identity management is a challenge that requires organizational policymakers to take stock of their organizations' needs and resources, carefully consider the available models, and adapt to changes in the identity market (Smith & McKeen, 2011). Organizations should regularly revisit their identity management policies to keep up with developments in the digital landscape, including security trends, regulatory changes, and technological advancements.

Acknowledgments

We are grateful to John L. King for his insightful feedback and guidance throughout the process and to the members of the policy posse for their helpful comments that strengthened the paper. This research was funded in part by the Luxembourg National Research Fund (FNR), grant reference 16326754, and PayPal, PEARL grant reference 13342933/Gilbert Fridgen. For the purpose of open access and in fulfillment of the obligations arising from the grant agreements, the authors have applied a Creative Commons Attribution 4.0 International (CC BY 4.0) license to any author-accepted manuscript version arising from this submission.

References

Benantar, M. (2005). *Access control systems: security, identity management and trust models* (2006 edition). Springer.

Council of the European Union. (2024). *European digital identity (eID).* https://www.consilium.europa.eu/en/press/press-releases/2024/03/26/european-digital-identity-eid-council-adopts-legal-framework-on-a-secure-and-trustworthy-digital-wallet-for-all-europeans/

FIDO Alliance. (2023). *Passkeys (Passkey authentication).* https://fidoalliance.org/passkeys/

Glöckler, G., Sedlmeir, J., Frank, M., & Fridgen, G. (2023). A systematic review of identity and access management requirements in enterprises and potential contributions of self-sovereign identity. *Business & Information Systems Engineering*. https://doi.org/10.1007/s12599-023-00830-x

Guggenberger, T., Kühne, D., Schlatt, V., & Urbach, N. (2023). Designing a Cross-organizational Identity Management System: Utilizing SSI for the Certification of Retailer Attributes. *Electronic Markets*, *33*(1). https://doi.org/10.1007/s12525-023-00620-z

Hill, K. (2022). A dad took photos of his naked toddler for the doctor. Google flagged him as a criminal. *The New York Times. https://www.nytimes.com/2022/08/21/technology/google-surveillance-toddler-photo.html*

Lacity, M., Carmel, E., Young, A. G., & Roth, T. (2023). The quiet corner of Web3 that means business. *MIT Sloan Management Review*, *64*(3). https://sloanreview.mit.edu/article/the-quiet-corner-of-web3-that-means-business/

Livius, T. (1943). *Livy: History of Rome, VII, Books 26-27* (F. G. Moore, Trans., Reprint Edition). Harvard University Press.

Rieger, A., Roth, T., Sedlmeir, J., Weigl, L., & Fridgen, G. (2022). Not yet another digital identity. *Nature Human Behaviour*, *6*, Article 3. https://doi.org/10.1038/s41562-021-01243-0

Sedlmeir, J., Rieger, A., Roth, T., & Fridgen, G. (2023). Battling disinformation with cryptography. *Nature Machine Intelligence*, *5*, 1056-1057. https://doi.org/10.1038/s42256-023-00733-2

Sedlmeir, J., Smethurst, R., Rieger, A., & Fridgen, G. (2021). Digital identities and verifiable credentials. *Business & Information Systems Engineering*, *63*(5), 603-613. https://doi.org/10.1007/s12599-021-00722-y

Sheldon, R. M. (2015). Hannibal as spy chief. Een Geschiedenis van Spionage En Inlichtingendiensten, *Leidschrift: Kennis Is Macht, 30*, 25–46.

Smith, H. A., & McKeen, J. (2011). The identity management challenge. *Communications of the Association for Information Systems*, *28*, 169-180. https://doi.org/10.17705/1CAIS.02811

Winder, D. (2023). Why you should stop using Lastpass after new hack method update. *Forbes.* https://www.forbes.com/sites/daveywinder/2023/03/03/why-you-should-stop-using-lastpass-after-new-hack-method-update/?sh=5b6d7db28fc9

Windley, P. J. (2023). *Learning digital identity: design, deploy, and manage identity architectures*. O’Reilly Media.

Yeoh, W.-Z., Kepkowski, M., Heide, G., Kaafar, D., & Hanzlik, L. (2023). Fast IDentity Online with Anonymous Credentials (FIDO-AC). *Proceedings of the 32nd USENIX Security Symposium*. https://www.usenix.org/system/files/usenixsecurity23-yeoh.pdf

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, *30*(1), 75–89. https://doi.org/10.1057/jit.2015.5

About the Authors

Alexander Rieger is an assistant professor of information systems at the Sam M. Walton College of Business at the University of Arkansas. His research focuses on innovation with emerging technologies in highly structured environments. His work has appeared in *Nature Human Behavior*, *Nature Machine Intelligence, Information & Organization*, *International Journal of Information Management*, and *MIS Quarterly Executive*. He has several years of experience working in industry and consulting for the European Commission as well as various public and private sector organizations in Germany and Luxembourg. He holds a master's degree and a PhD in information systems.

Tamara Roth is an assistant professor of information systems at the Sam M. Walton College of Business at the University of Arkansas. Her research explores how emerging technologies can be leveraged to promote social good and achieve positive organizational change. She combines theories and methods from neurobiology, psychology, social sciences, and management. Tamara's work has appeared in *MIT Sloan Management Review*, *International Journal of Information Management, Nature Human Behavior,* and *Nature Machine Intelligence.* She has an interdisciplinary education with master's degrees in biology and education, a PhD in educational psychology, and is currently finalizing her PhD in information systems.

Johannes Sedlmeir is a postdoctoral researcher at the Interdisciplinary Centre for Security, Reliability, and Trust (SnT), University of Luxembourg. In his research, he focuses on the effective use of emerging digital technologies in organizations by designing and evaluating innovative IT artifacts based on, e.g., distributed ledgers, digital identity attestations, and zero-knowledge proofs. His research has appeared in *Business & Information Systems Engineering, Electronic Markets, Information & Management,* and the *Journal of Network and Computer Applications*. He holds a master's degree in theoretical and mathematical physics and a PhD in information systems.

Gilbert Fridgen is a full professor and PayPal-FNR PEARL Chair in Digital Financial Services at the Interdisciplinary Centre for Security, Reliability, and Trust (SnT), University of Luxembourg, and coordinator of the National Centre of Excellence in Research on Financial Technologies. In his research, he analyses the transformative effects of digital technologies on individual organizations and on the relationship between organizations. He addresses especially emerging technologies like distributed ledgers, digital identities, machine learning, and the internet-of-things.

Amber Young is an associate professor of information systems at the Sam M. Walton College of Business at the University of Arkansas. Her research focuses on how information systems can promote social good and positive organizational outcomes. Amber serves as an associate editor for *MIS Quarterly*. Her research has appeared in *MIS Quarterly*, *Journal of Management Information Systems*, *Journal of the AIS*, *Information Systems Journal*, *Information & Organization*, *MIT Sloan Management Review*, *International Journal of Information Management, AIS Transactions on Replication Research*, and *Communications of the Association for Information Systems*.