Bus Inf Syst Eng
https://doi.org/10.1007/s12599-023-00830-x

RESEARCH PAPER

A Systematic Review of Identity and Access Management Requirements in Enterprises and Potential Contributions of Self-Sovereign Identity

Jana Glöckler · Johannes Sedlmeir · Muriel Frank · Gilbert Fridgen

Received: 26 September 2022 / Accepted: 11 July 2023
© The Author(s), under exclusive licence to Springer Fachmedien Wiesbaden GmbH 2023

Abstract Digital identity and access management (IAM) poses significant challenges for companies. Cyberattacks and resulting data breaches frequently have their root cause in enterprises' IAM systems. During the COVID-19 pandemic, issues with the remote authentication of employees working from home highlighted the need for better IAM solutions. Using a design science research approach, the paper reviews the requirements for IAM systems from an enterprise perspective and identifies the potential benefits of self-sovereign identity (SSI) – an emerging, password-less paradigm in identity management that provides end users with cryptographic attestations stored in digital wallet apps. To do so, this paper first conducts a systematic literature review followed by an interview study and categorizes IAM system requirements according to security and compliance, operability, technology, and user aspects. In a second step, it presents an SSI-based prototype for IAM, whose suitability for addressing IAM challenges was assessed by twelve domain experts. The results suggest that the SSI-based authentication of employees can address requirements in each of the four IAM requirement categories. SSI can specifically improve manageability and usability aspects and help implement acknowledged best practices such as the principle of least privilege. Nonetheless, the findings also reveal that SSI is not a silver bullet for all of the challenges that today's complex IAM systems face.

Keywords Authentication · Digital wallet · IAM · Security · SSI · Verifiable credential

1 Introduction

Employees' simple and reliable access to digital resources and software applications is one of the essential prerequisites for many organizations' operation (Smith and McKeen 2011). In practice, however, it is difficult for IT managers and users to set up, maintain, and use this access, and it comes at a high cost (Casassa Mont et al. 2003; Sinclair and Smith 2008; Windley 2005), especially when businesses grow and their technology environment becomes increasingly heterogeneous (Bradford et al. 2014). Complexity is also a driver for security incidents like data breaches that can result in unexpected remediation costs and damage to company reputation (Enterprise Management Associates, Inc. 2020), customer churn (Ponemon Institute 2019), and severe fines for violating data protection regulation (LogMeIn 2019; Schlackl et al. 2022). The situation was further aggravated during the COVID-19 pandemic with an estimated 70% of employees working from home (Sadler and Hancock 2020) and a corresponding increase of cyber-attacks; mainly phishing (Naidoo 2020). Several studies found that employees feel more tired, unmotivated, and distracted when working from home (e.g., Velocity Smart Technology 2021). As a result, mistakes and a lack of vigilance appear more frequently (Irwin 2021), and the likelihood of employees

Accepted after 2 revisions by Oscar Pastor.

J. Glöckler
University of Bayreuth, Bayreuth, Germany

J. Sedlmeir
Branch Business and Information Systems Engineering of Fraunhofer FIT, Bayreuth, Germany

J. Sedlmeir (✉) · M. Frank · G. Fridgen
Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg, Luxembourg, Luxembourg
e-mail: johannes.sedlmeir@uni.lu

Published online: 12 September 2023

giving away their passwords in a phishing attempt increases (Sadler and Hancock 2020).

Besides offering better password management for employees, identity and access management (IAM) systems provide enterprises with tools to support them in handling and monitoring a growing number of identities beyond employees, such as external partners, customers, and – driven by the growing relevance of the Internet of Things (IOT) – smart devices (Haber 2020). 77 % of enterprises aim to increase their budget for IAM to mitigate cybersecurity risks (Globenewswire 2020). In contrast, only 38% of companies used dedicated IAM software in 2017 (IDG Business Media GmbH 2017), illustrating the considerable challenges and costs involved with setting up and maintaining these systems. Consequently, enterprises also take complementary approaches, such as raising the awareness of cybersecurity among employees and deploying anti-virus software (Deloitte 2020), or look into new approaches, for instance, zero-trust architectures (Puchta et al. 2019; Buck et al. 2021).

At the same time, the threat of being subject to cybersecurity incidents for companies is increasing. In 2019, the global cost of data breaches alone was $ 2.1 trillion, and it is expected to rise further to $ 5 trillion in 2024, according to Juniper Research (2019). More conservative estimates still suggest that data breaches account for a significant share of the total annual costs of cybercrime of $ 1 trillion (Dyble 2020). 43 % of data breaches involve attacks on web applications, of which more than 80 % can be traced back to brute force attacks on employees' passwords or the use of lost or stolen credentials (Verizon 2020). Consequently, every third data breach can be linked directly to password management. Taking into account that data breaches are only one of the potential consequences of poorly implemented IAM, the need to improve related solutions seems to be widely recognized by researchers and practitioners (Smith and McKeen 2011; Puchta et al. 2019). However, there has been surprisingly little holistic academic research on the requirements of IAM systems, which we deem essential to designing and evaluating new solutions. Consequently, this study seeks to identify and categorize enterprise requirements for employee IAM solutions, leading to our first research question (RQ):

RQ1: What are the requirements of IAM in enterprises?

One of the most prominent new paradigms for digital identity management and in particular authentication is decentralized digital identity management or self-sovereign identity (SSI) (Gartner Inc. 2020; Sedlmeir et al. 2022; Soltani et al. 2021). SSI is not specifically targeting IAM but rather end users', organizations', and smart devices' digital identity management in general. It provides users with digital wallet apps on their mobile phones and empowers them to self-manage digital representations of identity documents such as passports, qualifications, access authorizations, or membership cards (Sartor et al. 2022; Richter et al. 2023). This paradigm, which is often associated with blockchain technology (Mühle et al. 2018; Sedlmeir et al. 2022), has received increasing support from industry consortia and governments in recent years (Kubach and Sellung 2021; Schmidt et al. 2021). Despite these developments, there is still a lack of research in the academic literature on how SSI can improve digital identity management in organizations in general and in IAM in particular. While some research has started investigating different technical aspects of SSI in the context of established IAM standards (Yildiz et al. 2021; Di Francesco Maesa et al. 2023), this study is to the best of our knowledge the first to holistically investigate the extent to which the SSI paradigm in IAM is suitable for meeting IAM system requirements (see RQ1). Our second research question, therefore, is as follows:

RQ2: How can SSI help address the requirements of IAM in enterprises?

To explore the requirements of IAM systems and potential improvements through SSI, we choose a design science research (DSR) approach (Hevner et al. 2004; Peffers et al. 2007). DSR uses scientific methods to design new artifacts or modify existing ones to solve relevant practical problems (Venable and Baskerville 2012; Johannesson and Perjons 2014) and is, therefore, suitable for identifying the challenges of today's IAM in enterprises and designing corresponding solutions. Our study finds that both technical considerations and the role of enterprise IT management and employees as end users are essential for deploying IAM solutions in practice. We first identify four categories of requirements for IAM and use them to discuss how SSI can contribute to creating more secure and manageable IAM solutions.

The remainder of this paper is as follows: Sect. 2 introduces the theoretical background and salient research on identity and access management and SSI. We then describe our DSR approach (Sect. 3), which we use to identify and analyze IAM requirements (Sect. 4). Section 5 presents our SSI-based IAM prototype, followed by its evaluation by experts (Sect. 6) that sheds light on the potential benefits of SSI-based IAM. We also discuss limitations that point to avenues for future research and conclude with Sect. 7.

2 Related Research

2.1 Identity and Access Management

IAM encompasses both "identity management" and "access management" (Thakur and Gaikwad 2015), i.e., it involves the management of identities as well as the processes associated with authentication and authorization processes in organizations. Identities can be claimed by human and non-human entities (Windley 2005). In an enterprise context, the human entities of employees, suppliers, partners, and customers can be distinguished (Mezler-Andelberg 2008). Non-human entities cover organizations, machines, or software applications (Windley 2005).

Authentication is the process of proving control of an identity but does not yet grant access rights (Haber and Rolls 2020). Such proofs of identity involve credentials, sometimes called authenticators, which can be divided into three categories: "what you know" (e.g., a password), "what you have" (e.g., a physical key), and "who you are" (e.g., represented by a fingerprint) (O'Gorman 2003). These credentials can be used also in combination in so called multi-factor authentication (MFA) to increase the level of assurance and, thus, security (Windley 2005). The form of authentication that a system admits generally depends on the type of access and the associated risks (Mezler-Andelberg 2008). In 2019, the use of MFA by companies reached around 57% worldwide, a significant increase from the previous year (LogMeIn 2019). However, MFA not only increases security, it can also increase cost and complexity for organizations and negatively impact user experience (Windley 2005; Yubico and 451 Research 2021; Acemyan et al. 2018).

Once a user is authenticated, access is granted or denied during authorization (Haber and Rolls 2020). An access control list (ACL) of authorized users, i.e., to implement read and write permissions, can be attached to resources (Ferraiolo et al. 2007). By configuring and maintaining such a list, it is easy to keep an overview of which user has which kind of access to the respective resource. However, at the same time it is often difficult to determine to which resources an individual user has access (Ferraiolo et al. 2007), especially in an enterprise with thousands of software applications, some of which are hosted by third parties. As the number of users and resources increases, the costs of managing ACLs hence increase substantially, making the approach inappropriate for larger organizations (Oh and Park 2003). Moreover, while adding permissions is easy, revoking permissions for a particular user is difficult with ACLs (Ferraiolo et al. 2007). Consequently, more common access control models used in enterprises are discretionary access control (DAC), role-based access control (RBAC), and attribute-based access control (ABAC).

DAC allows a resource's owner to decide who is granted access, and entities that have access can in turn delegate, i.e., pass on, this permission (Ferraiolo et al. 2007). In contrast, RBAC assigns roles to specific access rights (Benantar 2006; Mezler-Andelberg 2008). Users can then be assigned one or multiple roles and receive the associated permissions (Ferraiolo et al. 2007). RBAC is the access control model most used by enterprises (IDG Business Media GmbH 2017); yet it causes considerable problems. For instance, when employees change jobs, access rights and roles need to be adjusted, which represents a major administrative burden and cost factor for companies (Kern and Walhorn 2005; Li and Karp 2007; Fuchs and Pernul 2013; Oh and Park 2003; Zhao and Johnson 2010). ABAC aims to address these challenges by granting or denying access based on users' and resources' attributes and environmental conditions. Since attributes can be specified and combined more flexibly than roles, ABAC enables particularly fine-grained access control (Hu et al. 2015). If a change of access rights is necessary, the underlying rules can remain untouched and the modification of a single attribute associated with a user is sufficient (Hu et al. 2015).

Regardless of the choice of access control model, there are generally acknowledged principles that should be applied in IAM systems. The *principle of least privilege* states that users should only possess the minimum rights necessary for their tasks (Ferraiolo et al. 2007). If a user has significantly more rights than necessary, they could cause excessive damage to the system in the event of an attack or misuse (Benantar 2006). Access rights should, therefore, be chosen carefully and reviewed from time to time. A similar guideline is the *principle of least knowledge*, which specifies that users but also IAM system administrators should only see the resources associated with their task (Alsmadi 2019). Moreover, to mitigate fraud, *separation of duties* can be used to ensure that not all steps of a critical operation can be performed by a single user (Ferraiolo et al. 2007).

IAM remains a major challenge for organizations, as attempts to improve the security of their employees' passwords often prove ineffective. When employees are forced to reset their passwords on a regular basis, 49% of employees change only a single digit or character in their old passwords (Jacobson 2020). Employees who find password policies and management onerous also tend to experience security fatigue, making enterprise IT systems even more vulnerable (Cram et al. 2021).

2.2 Self-Sovereign Identity and Digital Wallets

SSI can be considered a paradigm that extends the use of asymmetric cryptography and, in particular, digital signatures beyond the identity management of web servers and makes it accessible to end users via digital wallets (Sedlmeir et al. 2022). Certificate-based identity management has been a backbone of cybersecurity for decades (Lioy et al. 2006), and SSI aims to apply this approach to identity management for end users, smart devices, and organizations (Preukschat and Reed 2021). It is seen as an answer to the security, usability, and efficiency challenges of logging in with usernames and passwords (Bonneau et al. 2012), and as an alternative to the privacy issues and lock-in effects related to the data silos of federated identity providers that offer a convenient single sign-on experience (Kubach et al. 2020; Ehrlich et al. 2021; Sedlmeir et al. 2022).

Certificate-based digital identity management for end users was already widely discussed in the computer science literature as early as the 2000 s (e.g. Backes et al. 2005; Lioy et al. 2006; Jøsang and Pope 2005; Ahn et al. 2009), but did not gain broad awareness or acceptance in practice until recently (Kubach et al. 2020). Potential reasons for the renewed interest in using this paradigm for end users' identity management may be traced back to the increasing availability and capabilities of mobile phones (Sedlmeir et al. 2022). Moreover, it seems that the collaborative spirit in public and private ecosystems in the context of a broad enthusiasm for blockchain technologies, and the corresponding cryptographic key management, may have promoted the interest in identity management through digital wallets (Mühle et al. 2018; Jørgensen and Beck 2022). Although blockchain technology is not required for SSI (Chadwick 2020; Schlatt et al. 2022a), the technologies are strongly connected (Mühle et al. 2018; Čučko and Turkanović 2021), and many SSI frameworks leverage a blockchain for their underlying public key infrastructure (PKI) (Schmidt et al. 2021). In the context of SSI, also a new standard – verifiable credential (VC) – has emerged (Sporny et al. 2021). VCs aim to replace identity documents based on paper or "plastic cards" (Richter et al. 2023) by means of digital attestations and can be thought of as an extension and generalization of traditional, digitally signed documents, such as X.509 certificates that build the identity layer for web servers and JSON Web Tokens that are frequently used in enterprise applications leveraging federated identity management based on protocols like OpenID Connect (OIDC) (Babel and Sedlmeir 2023; Kuperberg and Klemens 2022).

SSI comprises three important roles: Issuers, holders, and verifiers (Soltani et al. 2021). An *issuer* digitally signs VC that contain claims about their subject's attributes and sends them to the holder (Sporny et al. 2021). *Holders* request VC from issuers and store them in their *digital wallets* that often take the form of mobile apps for end users. Since holders store their VC locally, they have control over data disclosure (Sartor et al. 2022). They can then use their VC according to their preferences to create machine-verifiable proofs about claims concerning their identity in a *verifiable presentation (VP)* when interacting with a verifier (Sporny et al. 2021; Feulner et al. 2022). As digital information tends to leave unique traces, an important principle of SSI is that it is possible to reveal only certain parts ("selective disclosure") or only properties derived from it ("predicates"), such as a proof of legal age (Feulner et al. 2022), and to allow the cryptographic verification of the VP's authenticity despite hiding the unique value of the digital signature or the binding public key from the verifier (Babel and Sedlmeir 2023). These privacy-enhancing features are typically based on cryptographic zero-knowledge proof (ZKP) (Backes et al. 2005; Camenisch and Lysyanskaya 2001; Hardman 2020; Di Francesco et al. 2023). A ZKP gives evidence about the correctness of a statement (e.g., the result of a computation) without transferring any knowledge beyond the statement under consideration (Goldwasser et al. 1989).

A VP can involve one or several VC, and the corresponding proof is automatically checked by the verifier upon receipt (Preukschat and Reed 2021; Feulner et al. 2022). Due to the forgery-proofness of digital signatures, there is no need for communication between the issuer and the verifier. However, verifiers will in general only trust a verifiable credential (VC) used in a VP if they trust the corresponding issuer. Communication between parties takes place via end-to-end encrypted messaging between software components, so-called *agents* (Preukschat and Reed 2021; Schlatt et al. 2022b). Agents sometimes integrate a client for a blockchain that is used to store issuers' public signing keys, standards, and revocation information (Schlatt et al. 2022a). The latter is required as VC reside in the holder's wallet, so they can no longer be removed reliably after issuance (Ruff 2018). Revocation is often implemented via revocation registries. For the identity management of servers, there is no big issue with publicly available revocation information; however, from an end user's perspective, this approach poses privacy challenges (Babel and Sedlmeir 2023). For this purpose, some SSI implementations hide credentials' unique identifiers in VPs, proving only set membership or non-membership in the public revocation registry by using a ZKP (Hardman 2020; Schlatt et al. 2022a).

Several businesses and organizations have already started to provide software solutions based on SSI. In particular, companies such as esatus, Evernym (recently acquired by Avast), or Trinsic, as well as public-private initiatives

like IDunion that involve many public and private sector stakeholders, implement digital wallet apps for end users that already offer a decent level of standardization and interoperability (Sartor et al. 2022). The EU has also passed a law that mandates member states to provide their citizens with digital wallets and to enforce their use for login with digital service providers in the course of the revision of the electronic identification, authentication and trust services (eIDAS) regulation (European Commission 2021; Schwalm et al. 2022). The range of SSI use cases and potential benefits covers, for instance, passwordless digital authentication and digital proofs of attributes or permissions through digital ID cards, driver's licenses, credit cards, or COVID-19 vaccination certificates (Sedlmeir et al. 2022). In domains such as access control for web applications (Braun et al. 2023), managing know your customer (KYC) processes (Schlatt et al. 2022a), digital diplomas (Grech et al. 2021), and event tickets (Feulner et al. 2022), researchers have already studied the improvements that SSI can provide for individuals' authentication and authorization processes. On the other hand, businesses such as esatus, IdRamp, MATTR, or Workday advocate the potential benefits of an SSI-based flexible and passwordless digital identity management for enterprise IAM and offer corresponding software solutions. Kuperberg and Klemens (2022) recently surveyed the compatibility of and technical bridges between technical components and protocols associated with legacy IAM and SSI, and Belchior et al. (2020) proposed and implemented an SSI-based identity management across organizations.

3 Research Approach

To determine how SSI can improve enterprise IAM, we follow a DSR approach (Hevner et al. 2004; Peffers et al. 2007). DSR had long a tradition in software engineering before it found its way into the field of information systems (Peffers et al. 2007), combining elements from engineering (Eekels and Roozenburg 1991) and behavioral sciences (Hevner et al. 2004). In general, DSR involves the development of an artifact, such as methods, products, processes, or services, to address a general problem, and an evaluation of the solution's fitness to solve the problem (Venable and Baskerville 2012). DSR therefore aligns with the goals of information systems research, which also employs build-and-evaluate processes to study the interaction of technical and social systems and find solutions to practical challenges (Lee 2001).

Commonly, DSR encompasses three different phases: first, the relevance cycle that identifies the practical problem that needs to be solved and the corresponding requirements for research (Hevner et al. 2004; Hevner 2007; Peffers et al. 2007). The next phase, also known as the design phase, is concerned with building and evaluating the design artifact (Hevner 2007). This is followed by a rigor cycle to ensure that artifacts are useful contributions to research and not routine designs (Hevner et al. 2004; Gregor and Hevner 2013). Since it can be challenging to balance the need for practical contributions in a changing technological environment with generalizing and theory building (Baskerville et al. 2018), an expansion of the knowledge base or the implementation of a novel IT artifact that provides solutions to practical problems can already be an appropriate contribution to research (Beck et al. 2013; Gregor and Hevner 2013; Baskerville et al. 2018). In the following, we will further elaborate on our research design and the involved methods. Figure 1 displays our DSR approach and the involved methods that we will describe in more detail below.

In the relevance phase, we first conducted a systematic literature review (SLR) to identify IAM requirements in enterprises (Levy and Ellis 2006). Next, we coded all publications using Saldaña (2015)'s approach and clustered the requirements using a distance metric derived from related sub-requirements. This generated an initial structured collection of IAM requirements that served as design objectives for the artifact (Peffers et al. 2007). To increase relevance, we then conducted interviews with twelve domain experts with the goal of (1) completing the perspective on IAM requirements and (2) refining the categorization. After examining the state of the art of research on SSI in an enterprise context, we took the results as input for a design cycle in which we conceptualized and instantiated a prototype for SSI-based IAM (Sect. 5). In a subsequent rigor cycle (Hevner et al. 2004), we again used expert interviews to assess whether the implementation sufficiently addresses the previously defined opportunities or problems (Hevner 2007). Furthermore, we present new knowledge generated in our DSR in the form of structured requirements and our prototype to the scientific community (Peffers et al. 2007) and demonstrate how SSI can contribute to improving IAM in enterprises. This involves both the dissemination of this manuscript and the disclosure of our demonstrator's source code.[1]

4 Analysis of IAM Requirements

4.1 Systematic Literature Review

To identify and structure the requirements associated with IAM systems in enterprises (see RQ1), we rely on a SLR consisting of three steps: inputs, processing, and outputs

[1] The code is available at https://github.com/JSedlmeir92/SSI-IAM.

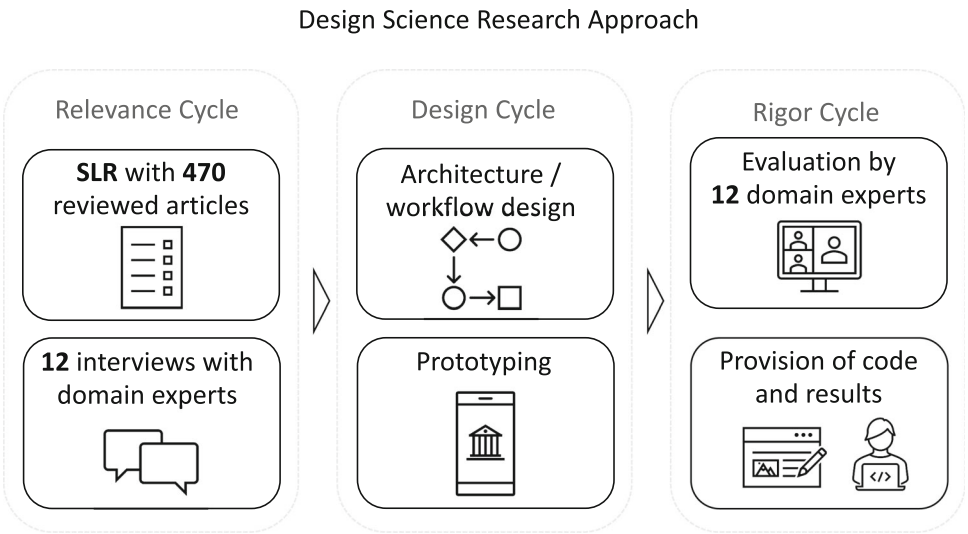


Fig. 1 Phases of the design science research approach

(Levy and Ellis 2006). We then use the results of this analysis as input for the design of our artifact as part of the DSR (as described in Sect. 3). In general, literature reviews support the proposed research question and provide a solid foundation for the research endeavor (Levy and Ellis 2006). The first step is to identify the relevant literature to ensure a certain level of quality of the literature (Levy and Ellis 2006; Kitchenham et al. 2009). This can be achieved through various techniques, such as applying inclusion and exclusion criteria and documenting the search process (Kitchenham et al. 2009). Next, the processing step involves either analyzing, synthesizing, applying, or evaluating the identified literature. The final step is to present the results in a comprehensive and understandable way. We will elaborate more on these steps below.

4.1.1 Procedure

Following Levy and Ellis (2006), we selected the articles for the SLR using a keyword search, followed by forward and backward searches. To determine a suitable search string that is broad enough to cover existing work on IAM in enterprises but at the same time has a sufficiently high density of relevant hits, we performed a keyword search in several databases with many synonyms for IAM, combined with synonyms for enterprises using the logical operator "AND". We screened the first pages of results and focused on works with many citations or where the abstract matched our research topic. Due to the large number of potentially relevant articles we found in the initial search, we decided to limit our focus to enterprise IAM for employees. The final search string we used for the SLR was

("Identity Management" OR "Access Management" OR "Access Control")
*AND Employe**
AND (Busines OR Compan* OR Enterpris* OR Organi*)*

Table 1 features the databases we searched with this search string and the corresponding numbers of hits. We considered 10 hits as a page. Since many databases still yielded far too many initial hits, we decided to end the search once 20 hits in a row no longer yielded a relevant article after abstract and full-text screening. The decreasing trend of the number of relevant hits per page (see Table 1), as well as the limited number of works that the subsequent backward search (9 new articles) and forward search (no new articles) added, indicate that we were able to cover the field comprehensively with these heuristics. In the course of the search, we screened a total of 5,569 articles. After applying inclusion and exclusion criteria (Kitchenham et al. 2009), 40 articles remained for in-depth full-text analysis (see Table 1 in Appendix A.1; available online via http://link.springer.com). Inclusion criteria included selecting articles or book chapters that address enterprise IAM requirements or improvements for IAM approaches; exclusion criteria, on the other hand, applied to articles written in a language other than English or German and articles with IAM requirements for consumers or other stakeholders. In addition, articles to which the authors did not have access were not considered. These were 45 articles in the keyword search, 164 in the backward search, and 25 in the forward search.

Among these 40 articles, Puchta et al.'s (2019) study is the only one that systematically structures requirements for IAM systems, using a literature review and expert interviews. The authors identify five current challenges for IAM. These are integration of identities beyond the employee level, heterogeneity, data quality and management, the transition from role-based to attribute-based approaches, and privacy. Puchta et al. (2019) also discuss

Table 1 Number of relevant search results per database (keyword search)

	Total Hits	Reviewed Articles	Relevant Articles	
			∑	per Page
ACM	9,963	50	3	
AISeL	800	30	1	
EBSCO	1,014	30	1	
EconBiz	230	40	2	
Emerald Insight	1,743	30	1	
Google Scholar	17,200	90	11	
IEEE Xplore	204	60	4	
JSTOR	1,715	20	0	
Springer Link	17,889	80	10	
Web of Science	275	40	2	
∑	**51,033**	**470**	**35**	
		without Duplicates	**31**	

how visual analytics can address the first three challenges to varying degrees. In contrast, our focus is not only on incremental improvements but on the suitability of an alternative, SSI-based solution for enterprise IAM. Consequently, for identifying comprehensive design objectives of a novel approach, we intend to cover not only current challenges of IAM but also general requirements. We will also see that SSI can contribute to the last two challenges of Puchta et al.'s (2019) study, thus complementing their research.

After screening papers of interest in accordance with RQ1, we continued with the processing step, which included the analysis and evaluation of the works to be reviewed. As proposed by Levy and Ellis (2006), we identified key IAM requirements germane to the research question and categorized thematically similar ones into groups. For generating categories, we used coding (Saldaña 2015). The coding was performed iteratively in MAXQDA by one researcher alone, which is a common procedure for less extensive research projects (Saldaña 2015). To ensure validity, the researcher shared her coding scheme captured in the codebook – a compilation of codes and brief examples – with the other researchers in the team to achieve group consensus (Harry et al. 2005; Saldaña 2015). The first cycle consisted of two steps: (1) the initial coding in which the relevant data were divided into smaller parts (Strauss and Corbin 1998) and (2) subcoding in which the obtained codes were further subdivided and refined (Saldaña 2015). For books, we only coded the relevant sections. During the first cycle, we identified 24 categories corresponding to 280 (sub-)codes. Figure 1 in Appendix A.2 illustrates how often the 24 categories appeared in the 40 articles.

In a second cycle, we relied on pattern coding to identify and group thematically similar codes together (Onwuegbuzie et al. 2016). We performed pattern coding using the unweighted average linkage method in MAXQDA, as it allows to merge the clusters with the highest similarity step by step (Forina et al. 2002). Our computer-assisted, statistical analysis may also allow for more rigorous analysis than human-based merging (Bringer et al. 2004). Structuring the codes from the SLR resulted in eight different requirement clusters that define our design objectives. Figure 2 in Appendix A.3 depicts how often codes from these clusters appeared in the articles overall, while Tables 2, 3, and 4 in Appendix A.4 present the number of overlapping subcodes, used to generate the distance matrix for pattern coding. Figure 3 in Appendix A.4 illustrates the corresponding distances between categories. The colors indicate which of the categories form a cluster. One theme ("control") is missing in the distance matrix because the topic has insufficient links with other codes to calculate a meaningful distance matrix. Therefore, we have kept it as a separate cluster.

4.1.2 Results of the Literature Review

In the following, as part of the final step of the SLR (Levy and Ellis 2006), we present all eight clusters we identified in descending order according to the aggregate frequency of the codes they comprise:

Cluster 1 – Security, Compliance, Integrity, & Auditability: The first cluster consists of requirements associated with security risk avoidance, technical measures to increase security, as well as with auditing and monitoring. Security threats, for instance, should be minimized as far as possible or, if feasible, prevented altogether (Walter et al. 2004).

Frequently, passwords are a root cause for security problems, so the usage of MFA that requires further credentials like biometric data or a physical token is increasing (Theofanos et al. 2016; Keszthelyi and Michelberger 2012). The continuous adaptation of security mechanisms is essential, as the methods used to break into a system are also constantly evolving (D'Costa-Alphonso and Lane 2010). To reduce risks, audits can be conducted (Damon and Coetzee 2018), for instance, to determine overprivileged users (Bradford et al. 2014). Monitoring employees' activities is not only important from a security perspective but also with regard to ensuring integrity and compliance (Haber 2020). For instance, organizations today have to comply with several regulations that mandate the record-keeping and reporting of IAM-related information (e.g. Damon and Coetzee 2018; Hummer et al. 2018; Zhao and Johnson 2010), such as the Sarbances-Oxley Act.

Cluster 2 – Manageability, Efficiency, Automation & Cost: The large number of identities, databases, and applications that today's IAM systems need to handle contribute significantly to obfuscating and ultimately inhibiting a holistic picture of users' permissions, complicating manageability (Puchta et al. 2019; Pöhn and Hommel 2020; Osmanoglu 2014; D'Costa-Alphonso and Lane 2010). Consequently, it is important to track employees' authorizations and activities to some extent to prevent fraud and facilitate audits (Smith and McKeen 2011; Osmanoglu 2014). Automating related processes, such as access reviews, certifications, and password resets, can help reduce the manual effort and increase efficiency (Osmanoglu 2014; Bradford et al. 2014) and reducing costs, for instance, for IT help desks (Osmanoglu 2014; Theofanos et al. 2016; Windley 2005). Other cost factors include modifications to role assignments and access lists – frequent processes that considerably increase the management workload (Kern and Walhorn 2005; Li and Karp 2007).

Cluster 3 – Standardization, Interoperability & Simplicity: Many companies face an organic growth of their digital resources and related IAM tools, without considering standards or interoperability (Bradford et al. 2014; Windley 2005). In addition, there are often differences in processes depending on the location or department (Osmanoglu 2014). The prevailing complexity from the company's point of view is often underestimated and can lead to substantial problems, especially when introducing new IAM systems (Royer 2013). The use of and adherence to established standards can help mitigate these challenges with interoperability and integration as well as simplify IAM systems (Small 2006; Windley 2005). Furthermore, standards can help create a more consistent user experience and make it easier to realize a higher degree of automation (Damon and Coetzee 2013; Osmanoglu 2014; Sinclair and Smith 2008; Windley 2005). Complexity, on the other hand, can negatively impact manageability, security, and efficiency (D'Costa-Alphonso and Lane 2010) and imply high costs (Small 2006; Sinclair and Smith 2008).

Cluster 4 – Privacy & Trust: Employees' personal data must be protected and proper use should be ensured by using data only to the required extent (Windley 2005). Users need to be able to trust identity and service providers as well as devices not to disclose unnecessary information (Bertino and Takahashi 2011; Walter et al. 2004). Concerns about data being accessed and correlated, sold, or misused in some other ways are frequently present (Casassa Mont et al. 2003). Privacy-enhancing mechanisms are also important to comply with data protection regulations (Bertino et al. 2001), for instance, the EU GDPR (Puchta et al. 2019). Owing to the presence of tradeoffs between privacy and accountability, the extent to which data is kept private may depend on the resource that is to be protected (Windley 2005).

Cluster 5 – Flexibility: Flexibility refers to the ability to adapt to the introduction of new IT solutions or security threats that need to be dealt with (Casassa Mont et al. 2003; Keszthelyi and Michelberger 2012). Furthermore, it also includes the capability of an implementation to grow with an increasing number of applications or users (Fairchild and Ribbers 2011).

Cluster 6 – Availability: Beyond a few critical special cases, access to systems and data should not depend on employees' location or device, allowing tasks to be completed at all times (Walter et al. 2004) and from different places. This requirement has become apparent particularly in lockdowns and home office periods during the COVID-19 pandemic (Guggenberger et al. 2021). This means that every employee on site, as well as employees accessing them remotely, should have the necessary access to resources in a timely manner (Damon and Coetzee 2013, 2018; Zhao and Johnson 2010).

Cluster 7 – Control: Employees and users in general often feel that they have limited control over their identity data. While no attributes of their identity should be shared with a service provider without explicit consent (Hoepman et al. 2008), it is unclear how users are able to technically enforce this. Once their data is stored on different, unrelated sites or platforms (silos), they can no longer influence what is shared with whom. Hence, they call for more transparency and selective disclosure that allows only the minimum necessary information to be shared on request (Casassa Mont et al. 2003; Smith 2008).

Cluster 8 – Portability: Portability requirements apply to identities and accounts (Pöhn and Hommel 2020; Smith and McKeen 2011). Their usage should not be restricted to

a single device or system (Hoepman et al. 2008; Smith and McKeen 2011). A lack of portability can be used by IAM service providers as part of their business strategy to increase the cost of switching. This aggravates the negative implications of lock-in effects for enterprises regarding their IAM system (Graef et al. 2013).

4.2 Refinement and Interview-Based Evaluation

We conducted semi-structured interviews with a total of twelve experts to complement and review the identified IAM requirements. The research team approached participants individually because of their expertise in the field of IAM or SSI. Of those who agreed to be interviewed, four work or have worked directly in the field of IAM, and four other experts have a background in IT management. In addition, eight of the twelve experts are working or have worked on novel forms of digital identity management, for example, based on blockchain and SSI. We include more details on the experts' areas of expertise in Table 5 in Appendix B.1. To minimize response bias, we assured all respondents that their participation was voluntary and offered to anonymize their statements (Podsakoff et al. 2003). In addition, all interviews were conducted by the same researcher to ensure consistency in data collection (Brod et al. 2009).

Each interview followed a guideline in a semi-structured format (see Table 6 in Appendix B.2). In the beginning, questions focused on the experts' general interest in IAM and their personal experience in this field. In the second, exploratory part of the interview, we asked the experts to report on what requirements and challenges they can identify in the use of IAM systems in companies, and where they currently see the greatest need to catch up. For instance, we asked "what benefits do you see for an organization by implementing an IAM system?" and "what are the possible drawbacks of such a system?". In the last part of the interview, to avoid bias, we then discussed the design objectives we derived in Sect. 4.1.

We transcribed and coded the interviews as we did for our literature review. In the first cycle, we performed a structural coding to break down the data into segments (Saldaña 2015). We chose the segments based on our interview guidelines, resulting in 10 codes. Following Saldaña (2015)'s recommendation to use other first cycle methods as the next step (Saldaña 2015), we continued with an initial coding as a starting point for further analysis. In a second cycle, we then used axial coding to define the dimensions of a category, as categories are linked to subcategories (Saldaña 2015; Charmaz 2014; Strauss and Corbin 1998). At the end of this cycle, we had a total of 213 codes. We present the results according to the structure defined in the structural coding.

4.2.1 *Open Collection of IAM Challenges*

To compare the experts' assessments of IAM system requirements with the result of our SLR, a researcher with knowledge in the field of IAM first coded the experts' responses along the original 24 categories we derived from the literature review. We illustrate the frequency of appearances in Figure 4 (Appendix B.4). The in-depth analysis of the interviews reveals that the experts most frequently addressed topics from the cluster *"Security, Compliance, Integrity, & Auditability"*. From their perspective, organizations need IAM to better control access to resources from both a security and a governance perspective, addressing auditing and risk issues (Experts 1, 4, 5 & 12). They also mentioned that monitoring user rights is often a compliance issue, especially for insurance companies and banks:

> *"They [A/N: banks and insurance companies] are already required by their compliance frameworks, whether it's COBIT or the Basel standards and anything else that's out there, to clarify who has which authorization, and they have to fully delineate that."* (Expert 8)

The experts also see a substantial risk of security breaches when IAM systems are poorly implemented, as the following statement indicates:

> *"So if it's poorly implemented [...], then under certain circumstances [...] you have the problem that the identity can be stolen [...]."* (Expert 6)

Overall, the experts still see a great need to catch up in terms of the implementation of IAM systems, especially among medium-sized companies. During the interviews, some of them mentioned that enterprises' IT departments often lack incentives to implement such a complex system, and the benefits are often not yet fully recognized, especially if IT is not part of the business model (Experts 9 & 10).

The second cluster most frequently addressed by experts was *"Manageability, Efficiency, Automation & Cost"*. The experts agree that IAM systems offer considerable advantages for overseeing systems and employees and their authorizations (Experts 1, 2, 6 & 10). When the size of a company reaches a certain threshold, they consider an IAM system indispensable (Experts 10 & 12). However, the experts note that managing an IAM system also involves increased effort, including costs (Experts 2, 3, 6, 9, and 10). With regard to efficiency, the experts contended that authorizations should be assigned as efficiently and quickly as possible to new employees to achieve first-day readiness. On the other hand, they also emphasized the importance of being able to revoke authorizations quickly

(Expert 8). Some of the interview participants emphasized how a high degree of automation in IAM systems can help prevent unwanted access:

> *"It helps [...] to have strict identity and access management [...] so that [...] I can automate things and then no users [...] that have been retired for ten years have access to any systems."* (Expert 1)

As there are usually many different systems in large companies (Bradford et al. 2014), the effort required to maintain the IAM system increases and IAM staff can lose the global perspective (Experts 1, 6 & 10). When each system has its own independent process and assigns permissions individually, there is no longer a single comprehensive history of permission granting and revoking processes (Expert 10). Expert 8 noted that IAM systems can assist with these issues by mapping the organizational structure and managing employees' permissions and roles.

Topics from the cluster *"Standardization, Interoperability & Simplicity"* were third-most mentioned. The experts see particular challenges when integrating a new IAM solution into existing systems. One of the experts pointed out:

> *"It's [...] always difficult when you want to migrate from one system to another, and there's kind of a [system] landscape already in place."* (Expert 1)

One expert also mentioned that businesses often avoid implementing IAM systems because they fear the corresponding complexity. The following statement addresses the potential hassle due to overlaps with other systems:

> *"Our whole structure is not designed for that at all. [...] We have the file server where all kinds of data converge, and to separate that [...], [everything] would have to be completely redone."* (Expert 4)

The experts also see room for improvement in terms of standardization and usability; for instance, to prevent the need for several roles across different systems (Expert 12). According to the experts, the heterogeneity and the number of isolated solutions affect not only security but also have substantial implications, as the following statement reasons:

> *"For the individual user, I would say, it [A/N: the implementation of an IAM] is certainly associated with certain fears because it of course makes it quite transparent who has access to what, and things that work in a shadow IT environment, like when users somehow book an app service or a cloud service themselves [...], are no longer that simple [...]."* (Expert 1)

Besides these three clusters, the experts also referred to each of the clusters *"Privacy & Trust"* and *"Flexibility"*. Overall, the distribution of the experts' responses is quite similar to the findings of the SLR, indicating that our findings are consistent. However, comparing the individual categories that they named, we notice some differences compared to related work (cf. Figures 1, 2, and 4 in the Appendix). The topic of security, which was one of the most mentioned in our SLR, was also mentioned several times by the experts, but not quite as frequently. A potential reason is that the security requirement is so obvious that the experts did not consider it worth discussing as much. The topic of manageability, by contrast, was mentioned considerably more often in interviews than in the literature, indicating that this is where current IAM solutions cause substantial difficulties for IT departments.

4.2.2 Refinement of the Clustering

After the initial discussion of requirements for IAM, we confronted the experts with the requirements we had identified in Sect. 4.1 through our SLR. For the most part, the experts agreed with the requirements and also found the scope and structure comprehensive and useful. In the following, we will present their remaining suggestions for improvement, which included merging and splitting some clusters and adding new topics. In addition, we will present the final structuring of our IAM requirements (see Fig. 2).

When asked what changes they thought were needed, the expert frequently suggested merging the "Privacy & Trust" and "Control" clusters, as indicated in the following statement:

> *"Privacy protection is always divided into two parts: On the one hand, there is the protection of privacy as ensured by governance frameworks [...] but on the other hand, there is also the issue of self-data protection. Do I have a way of exercising control over it?"* (Expert 8)

Moreover, the experts suggested combining "Standardization, Interoperability & Simplicity" and "Portability" (Experts 6 & 8). One expert suggested that "Manageability, Efficiency, Automation & Cost" and "Availability" should either be merged or more clearly separated:

> *"In a way, automation [and] efficiency also means availability."* (Expert 6)

When asked about which topics need to be rearranged or removed from clusters, the experts mainly discussed the role of "Simplicity" in Cluster 3. In particular, they expressed concerns about the relationship between simplicity and the other two subcategories, "standardization"

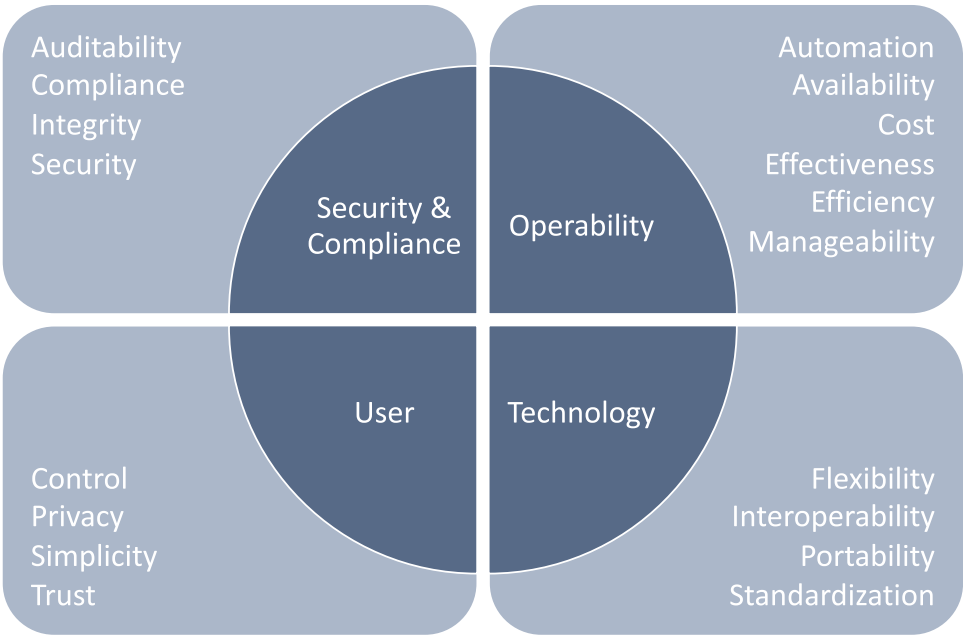


Fig. 2 Requirements for an enterprise IAM system: consolidated results after the SLR and the evaluation with experts

and "interoperability." The following statement reflects their doubts:

> *"Whether, for example, standardization, interoperability, and simplicity, i.e., Cluster 3, fit together so well, I don't know. [...] Standardization is a topic that does not necessarily have anything to do with simplicity."* (Expert 2)

When we asked the experts whether or not they see any topics that should be added to the clusters, they came up with several ideas. One of the experts, for instance, brought up future readiness, which describes the extent to which the requirements leave room for potential adjustments in the future. The following statement reflects his thoughts:

> *"For us what is always important is [...] the adoption somehow happening, [...] and is it future proof, so I can somehow adapt it in the future for things, but maybe that is also covered with [the cluster] flexibility."* (Expert 10)

Another expert suggested adding "effectiveness" to Cluster 2 (Manageability, Efficiency, Automation & Cost) but had to admit that it is probably already covered by manageability and automation (Expert 8). Finally, one expert recommended attaching concise labels to each cluster (Expert 7).

Drawing on the experts' suggestions on the composition of the clusters, we made some adjustments: We combined "Privacy & Trust" with "Control", we combined "Standardization, Interoperability & Simplicity" with "Portability", and we added "Availability" to "Manageability, Efficiency, Automation & Cost". Furthermore, based on the discussion above, we decided to split the category "Simplicity" from Cluster 3 ("Standardization, Interoperability & Simplicity") and combine it with the new cluster "Control, Privacy & Trust", as these all relate closely to the user perspective. As proposed by Expert 8, we added the aspect of "Effectiveness" to the second new cluster. We also added "Flexibility" to this cluster, as it concerns the design of the system. To make the newly formed clusters easier to understand and put the topics within the clusters into the right context, we gave them concise labels following Expert 7's recommendation. Ultimately, our changes led to the following four clusters: "Security & Compliance", "Operability", "Technology", and "User". We illustrate the final structuring of IAM requirements in Fig. 2.

5 Prototype

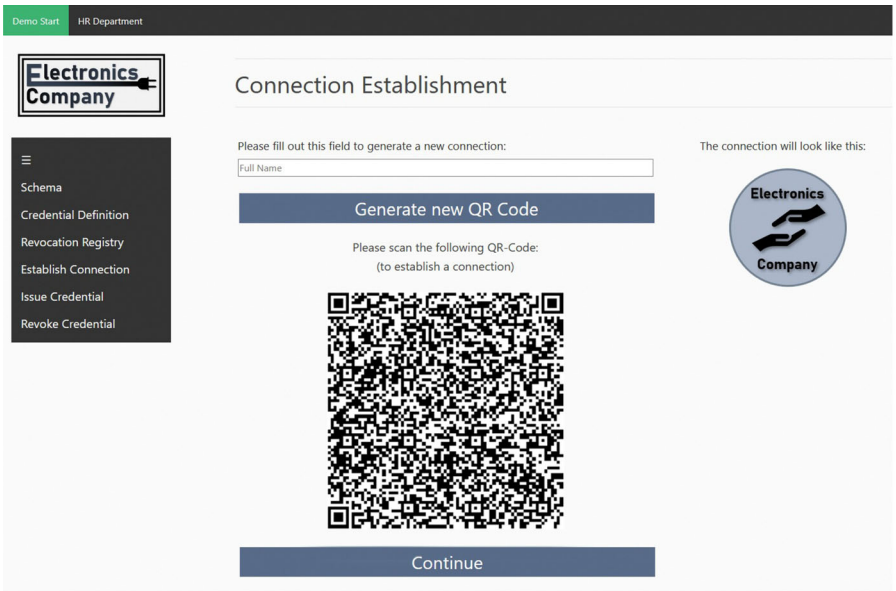
In this section, we present the SSI-based prototype that we developed based on the requirements identified in Sect. 4. Our prototype allows an employee VC to be issued, used, and revoked as part of a simulated intranet login. There are three parties involved in the process: The human resources (HR) department, which issues and revokes VC, the employee, who receives and holds the VC and uses it to prove authorization for logging in, and the intranet login manager or gateway that ensures that only authorized users gain access. Both the HR department and the intranet login operate "institutional agents", i.e., independent instances

of the *Hyperledger Aries Cloud Agent in Python (ACA-Py)*, as a microservice. ACA-Py is suitable for non-mobile environments and can be used to build decentralized identity applications (Linux Foundation 2020). It implements a RESTful API that allows an admin to manage cryptographic keys and VC in an SQLite database, integrates client functionalities to communicate with a public permissioned Hyperledger Indy blockchain, and provides an endpoint for standardized and encrypted peer-to-peer messaging (Schlatt et al. 2022b). As this messaging is often asynchronous (e.g., because a user's confirmation is required to continue a credential issuance or VP process), ACA-Py also provides webhooks to notify an application's controller about corresponding events.

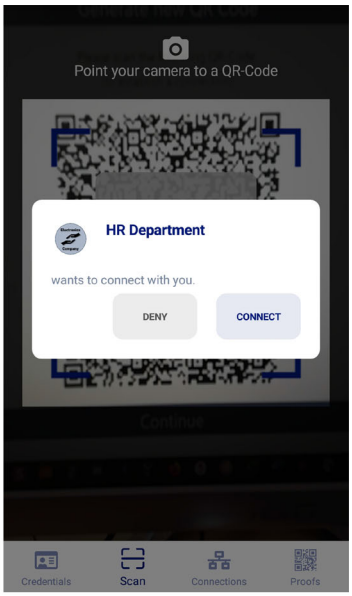
The two ACA-Py agents for the HR department and the intranet login never communicate with each other in our prototype and do not use a shared directory. The employee runs an SSI wallet app on a smartphone that can generate and use cryptographic keys, receive and manage VC, and interact with verifiers in VPs (Schlatt et al. 2022a; Sartor et al. 2022). The wallet app can be thought of as having a subset of the ACA-Py's functionalities. As such, the wallet also requires client capabilities for the Hyperledger Indy blockchain, so a user must currently choose the same blockchain that the other two agents are connected to within their digital wallet app. No other customizations of the mobile wallet were required for our prototype. We chose the *esatus* wallet, but there are other, compatible digital wallet apps such as *Trinsic*'s or *Lissi*'s that we could have used equivalently. We also built a web interface to run the demo using *Django*.

5.1 Connection Establishment

Establishing an initial connection between two agents is necessary for them to exchange information over a secure, end-to-end encrypted channel (Mühle et al. 2018). In this scenario, the employee's wallet app requires a connection with the HR department's agent (issuer) and with the intranet login manager's agent (verifier). The procedures to establish these connections are almost identical: in both cases, the institutional agent creates a personalized invitation link that resolves to an endpoint of the agent that serves the agent organization's name and public key for encrypted and authenticated messaging. Employees can either scan a quick response (QR) code that represents this link with their wallet app, or they can access it via a deep link that directly opens the payload in their digital wallet. As we illustrate in Fig. 3, the HR department can also personalize the invitation with an icon. To date, the QR code needs to be delivered through a trustworthy communication channel, like a personalized email or the company's authentic website, secured by traditional website certificates: Manipulating the QR code by inserting another endpoint that serves another public key but the same organization name and icon would enable man-in-the-



(a) Generating a QR code on the "connection" page.



(b) Scanning the QR code with the wallet app.

Fig. 3 Establishing a connection between the HR department and the employee

middle attacks (Babel and Sedlmeir 2023). This topic has been extensively discussed in the context of the German ID wallet (Lissi 2021; Schellinger et al. 2022). The corresponding vulnerability is currently being addressed by verifying that the connection's service endpoint corresponds to the referenced public key and organization name, either via using existing public key certificates for web servers or via a lookup on the permissioned Hyperledger Indy blockchain (Lissi 2021; Schellinger et al. 2022).

If the employee then scans the QR code, the employee's wallet creates a cryptographic key pair for this connection and asks the user whether he or she would like to accept the invitation. By accepting the invitation, the wallet sends a response to the HR department's or intranet login manager's agent respectively, i.e., to the service endpoint specified in the invitation, encrypted with the agent's public key referenced in the connection invitation. After a standardized initial message and key exchange, there is now an active connection between the two parties. The wallet sends messages directly to the agent; in the opposite direction, the wallet app provider runs a so-called mediation service that collects messages and provides them to the wallet when it is online. Fundamentally, such a mediator agent could be provided by any party and does not need to be trusted concerning confidentiality owing to end-to-end encryption. Yet, switching to a custom mediation agent is not yet supported by the wallet, and implementations of mediation agents usually rely on the push notification services of Apple and Google to avoid periodic polling.

5.2 Credential Issuance

To issue VC representing attested attributes to employees, the HR department has to make some preparations to bootstrap their agent for issuance. The agent first needs to register its endpoint and public key on the Hyperledger Indy blockchain. After that, it may have to publish a new schema. The schema contains, among other things, the type of attributes that are to be issued to the employee, i.e., it can be regarded a template or standard for a VC type in a specific context. In our prototype, the schema references the attributes "employee name", "company name", "division", and "job title". After publishing the schema or deciding to use an existing one, an issuer-specific credential definition must be derived from it. This determines the issuer's signing public key (more precisely, one key for each attribute) that is referred to in later proofs. If the agent is to revoke VC, it must also create and upload a revocation registry, which refers to a specific credential definition, to the Hyperledger Indy blockchain, and publish tails files – a list of public random numbers that the wallet needs for later ZKPs of non-revocation yet is too large to be uploaded to a blockchain (Babel and Sedlmeir 2023) – to a public repository, for which we chose GitHub.

Once the HR department has bootstrapped a credential definition and revocation registry, it can issue VC to employees. To do so, the process is initiated by the HR department which uses a web interface to define which values the attributes should have for the respective employee. We illustrate the form to enter the values in Figure 5 in Appendix C.1. In practice, HR departments would likely automate this by retrieving the attributes from an existing employee database. Next, the HR department's agent creates a credential offer with these attributes and sends it to the respective employee via an existing connection. The mediation agent associated with employees' wallets then pushes a notification on the smartphone, and employees can view and accept or reject the offer. If they accept the VC offer and respond with their binding public key to be included in the VC, the HR department agent creates and signs the VC and sends it to the employee's wallet app, where the VC is stored. Now the employee is ready to use the VC for future VPs.

5.3 Credential Usage for a Verifiable Presentation

If employees want to log in to the intranet with their mobile wallet, they need a credential issued by the HR department and an active connection with the intranet login manager. The view of the login page differs depending on whether users are new or returning: By using a session key to recognize a user's repeated logins, the intranet login manager can use a previously set-up communication channel instead of initializing a new connection through a QR code or deep link. We present both views in Figure 6 in Appendix C.2. After establishing a new connection or clicking the login button in the case of an existing one, employees automatically receive a proof request on their mobile wallet. The proof request asks for selected attributes from their employee VC. A proof request contains a random challenge ("noce") to prevent replay attacks and "restrictions", i.e., the VC must follow a specific schema or be issued by an issuer from a specific trusted list. Employees' digital wallets automatically create a dropdown list of VC that include the required attribute and that satisfy the corresponding restriction for every attribute requested and preselect one. In our case, the only choice is the VC that the HR department has previously issued. We illustrate the corresponding view in the wallet app in Figure 7 in Appendix C.3. Employees can change the selection of VC (if applicable) and give consent to answer the request. Their wallet then queries the current state of the revocation registry on the Hyperledger Indy blockchain and uses it to create a cryptographic proof. This proof corresponds to a ZKP that – simplified – asserts that:

- One of the issuers specified in the proof request's restrictions digitally signed the VC used to generate the proof.
- The user knows the private key associated with the (undisclosed) binding public key referenced in the VC.
- The attributes requested have the values revealed in the proof.
- The VC is not expired and not revoked.

Through the ZKP, as opposed to certificates based on conventional digital signatures that are used for authentication in some organizations, no additional information like the full VC including the value of the signature or the public binding key, is given to the verifier (Babel and Sedlmeir 2023). Moreover, it is possible to reveal attributes selectively, and verifiers cannot correlate them beyond the equality of the revealed attributes in repeated VPs that use the same VC (Hardman 2020). The wallet also supports predicates, e.g., it proves that the VC's expiration date (as UNIX timestamp) is larger than a specific timestamp (e.g., the current time) specified in the verifier's proof request, without disclosing the potentially correlated expiration dates themselves. Likewise, the ZKP proves set membership of the VC's revocation ID in the revocation registry without revealing the revocation ID. The digital wallet then sends the cryptographic proof to the intranet login's agent, which checks the status of the revocation registry and cryptographically verifies the proof accordingly. Afterward, the agent sends the proof verification result to the intranet controller – the core backend of an application that implements the overall process logic and potentially coordinates additional microservices, including databases – via a webhook. Only if the proof is valid, the employee can access the web application (intranet) based on the value of the revealed attributes. The sequence diagram for the verifiable presentation is depicted in Figure 8 in Appendix C.4.

5.4 Credential Revocation

If an employee retires, resigns, or changes the department in the organization (or other attributes), it may be necessary to revoke a VC to ensure access is no longer granted or to revoke and re-issue when attributes need to be updated. For this, an employee in the HR department can select the VC to be revoked. Automation would also be conceivable, for example, by revoking and re-issuing the VC after changes in the personnel database. The HR department's agent performs the revocation itself by creating an update for the revocation registry on the blockchain and publishing it there. To do this, it must authenticate with the same cryptographic key that was used for creating the revocation registry in the bootstrapping process. If the employee wants to use a revoked VC, it is recognized as invalid: The state of the revocation registry no longer allows the creation of a ZKP of non-revocation for a current timestamp, making it impossible to log in to the intranet. For the purpose of the demo, the agent immediately publishes the update to the revocation registry, so that the VC is effectively revoked after a few seconds. In a real-life enterprise context, it would be more practical to publish aggregate changes to the revocation registry state on the blockchain in larger intervals, e.g., once a day: Writing data to distributed ledgers is costly in general owing to redundancy, and Hyperledger Indy in particular has considerable performance limitations when it comes to write throughput (Sedlmeir et al. 2021).

6 Discussion

6.1 Prototype Evaluation

To evaluate the potential contributions of SSI to improve enterprise IAM solutions, we presented our prototype to the same twelve experts who had already evaluated the IAM requirements in Sect. 4.2. The researcher introduced the prototype to the participants and walked them through its features and functionalities. To illustrate this, the experts were presented with the case of Alice, a new hire, who receives a VC from the HR department. The VC is stored in a digital wallet on her cell phone and is used to create a VP when she wants to log in to the company's intranet. The login backend ensures that only authorized users have access. The interviewer explained all the roles (issuer, holder, and verifier) and also demonstrated how revocation works (for more details see Sect. 5). Participants were then asked to evaluate first the strengths and weaknesses of the prototype and then those of SSI-based solutions in general in a semi-structured way. We included the interview guideline in Table 6 in Appendix B.2. All interviews were recorded and transcribed with the consent of the participants. Again, one researcher coded the interviews along the coding dimensions identified in Sect. 4.2 (Saldaña 2015). Table 7 in Appendix B.3 displays an excerpt from the codebook with codes, subcodes, and brief explanations. Figure 4 in Appendix B.4 illustrates how often codes from the clusters were mentioned in these interviews.

Throughout the interviews, the experts agreed that our prototype suggests that SSI integrates very well with existing IAM systems. They, for instance, mentioned its strong similarity with OIDC-based solutions (Kuperberg and Klemens 2022), and that verifiable attributes retrieved from the VP can be used as part of a JSON web token for OAuth-based protocols. The following statement stresses these findings:

> *"[One] can make a gradual transition without hurting anyone, [...]. Otherwise, you would have to throw away all the investments you may have made, and of course no one in a large company makes that decision."* (Expert 10)

The experts, however, also noted that some of the technical wording in the frontend and wallet might be difficult for users to understand. Users who are not yet familiar with SSI may feel insecure because of the unfamiliar workflow and terminology, as the following statement suggests:

> *"I would like it to be a bit more user friendly, [...] [because] I wouldn't understand anything at first, although I think I'm already halfway living in today's time. Everything is very, I would say, technically formulated."* (Expert 4)

This perspective is also in line with the results of first user experience studies (Sartor et al. 2022; Guggenberger et al. 2023; Khayretdinova et al. 2022) that indicate usability challenges but also promising solution approaches. Other experts pointed out that it is important to delete also sessions to make revocation effective. In line with this, one of the experts suggested the following procedure:

> *"And when the credential is revoked, you can flag that right there [A/N] in the user database] and just delete the session. Then the session is basically sent there and the website realizes, oh, this one doesn't exist anymore, and then you're automatically redirected back to the login and can't get in."* (Expert 6)

However, when the selective disclosure capabilities of SSI-based authentication prevent a direct mapping of a session to an employee and their VC, it may be necessary to delete all sessions periodically (e.g., once a day) or a subset of potentially matching sessions when revoking a VC.

Expert 11 suggested that a less similar layout for the two pages (issuance and verification) could help to visually make clear the separation of the HR department page and the intranet pages in the architecture for the end user. Expert 12 noted that if the credential contains only the four attributes "employee name", "company", "department" and "job title", it may happen that two employees have the same name. He, therefore, suggested that a unique employee identifier be added as an attribute to overcome this problem, which also resonates with enterprises' current management of employees in databases. We subsequently incorporated these changes into our prototype.

6.2 Benefits and Challenges of SSI-Based Solutions for IAM

In the following, we highlight the experts' opinions on the hurdles and benefits of SSI-based solutions for IAM. The experts identified many benefits of SSI in terms of integration with existing IAM systems. They emphasized that SSI-based IAM solutions offer fine-granular access control and support the use of ABAC through the verifiable disclosure of identity attributes in VPs. Particularly the positive contribution of revocation to security was emphasized:

> *"And then if they [A/N: employees] resign or leave or are fired, then blocking them in the systems [...] is also faster. I think the technology stack [A/N: SSI], even if it still has weaknesses [...] is strong. With the revocation of keys, the technology stack generally resolves this tension between usability and security quite well." (Expert 7)*

The experts also highlighted the benefits of SSI-based solutions in terms of speed, as the following statement reflects:

> *"On the one hand, you can integrate your new employees into the systems much faster, or rather you grant them access to the systems more quickly. And then when they resign or leave or are laid off, they're also locked out of the systems faster."* (Expert 7)

However, one of the experts mentioned that providers of conventional IAM services are not yet showing much interest in the technology. This perception is supported by Glaude and Kudra (2021), who hypothesize that maintaining the existing complex and often non-interoperable landscapes is in the interest of IAM software providers as they want to secure their business models.

During the interviews, experts also discussed how SSI balances privacy and auditability features. They agreed that security is enhanced by passwordless authentication and native two-factor authentication, as VC are stored only on employees' mobile phones and unlocking the digital wallet for a VP requires a valid PIN or biometric unlock. Some of the experts pointed to benefits of SSI in terms of usability and user-friendliness:

> *"The fact that you don't have to come up with a different password for each system, or any password at all, but have the password in your wallet that you need to unlock your smartphone, or the biometric feature, makes it convenient."* (Expert 3)

In addition to increased usability, the experts considered improved privacy and control over information disclosure the main benefit for the user, especially as identity

attributes only need to be stored in employees' digital wallets. One of the experts stated:

> *"What I think is an advantage [...] is that I actually have full transparency in this wallet at all times [...] about who has somehow already queried my credentials then perhaps I could also somehow consolidate the whole thing at once and in principle say [...] I somehow don't want to use them anymore [...]."* (Expert 1)

In summary, the experts see several positive contributions that SSI can provide for IAM in all four clusters (please see Table 8 in Appendix B.5 for additional direct quotes from the experts indicating that they see potential improvements that SSI can provide for IAM systems in all four sets of requirements that we identified in Sect. 4). Nonetheless, the experts also pointed out some issues that need to be addressed in the future in order for such a solution to become established. These include, for example, the network connection that is required for checking (non-)revocation, standards that are still evolving, and the lack of availability of credential chaining, which is still a limitation for large-scale adoption from a technical point of view (Schlatt et al. 2022b; Babel and Sedlmeir 2023). Notably, the lack of maturity that is hard to deny after having implemented the prototype was not criticized by the majority of experts, as they consider a gradual introduction of SSI in IAM possible.

6.3 Limitations and Future Work

As with any research endeavor, our study comes with limitations that point to avenues for future research. First, we limited our literature review to employees in the enterprise context only. However, the perspectives and requirements of customers, suppliers, and partners could be also considered to further explore the potential benefits of SSI in an enterprise context. Another perspective we did not consider relates to the ongoing trend of IOT. First research in this domain has already appeared (Bartolomeu et al. 2019), but implementing SSI wallets on embedded devices is still an underexplored topic beyond working groups in SSI-related foundations like Sovrin and Trust over IP.

The second limitation concerns the prototype. Even though we have tried to develop an application that is as close to reality as possible, some of the processes involved that promise to improve IAM have not yet been implemented in practice. One example is the automatic issuance of a credential based on identity information stored in the companies' existing employee management system, or the distribution of a credential offer and the ensuing issuance to an employee who is not on-site, e.g., via e-mail.

Lastly, it is worth mentioning that our research focused on the authentication of employees, providing machine-verifiable attributes for ABAC, and managing the issuance and revocation of VC and the verification of VPs. Yet, some of the challenges of IAM systems as pointed out by Puchta et al. (2019), such as detecting entities with an unusual number of entitlements, might constitute a separate issue that can be addressed through complementary approaches like visual or automated data analytics. Future research could therefore investigate the additional adaptations that IAM software needs to monitor activities and manage access policies to resources based on verifiable attributes.

Another fruitful avenue for future work is a comparative analysis of our prototype with existing solutions such as Keycloak, as this would improve our understanding of which technology can best meet the IAM requirements and also identify more narrowly the potential for improvement of existing solutions.

Enterprise IAM is only one of many proposed applications of SSI. We believe that shedding light on where SSI can reduce complexities, increase security, and save costs is an interesting area for more interdisciplinary research, particularly in combination with other novel paradigms for enterprises' IT security like zero trust (Buck et al. 2021) and the integration of smart devices. For example, researchers could study how the introduction of passwordless authentication affects technology adoption and user security behavior. With regard to the latter, they could investigate whether digital wallets mitigate security-related stress – a phenomenon that employees often experience when complex security measures are involved (Frank and Kohn 2021).

7 Conclusion

The goal of this study was to identify IAM requirements in enterprises and investigate the extent to which SSI is able to address and fulfill these requirements. Using a SLR refined by twelve domain experts, we were able to cluster IAM requirements into four categories: "Security & Compliance" covering the subcategories security, compliance, integrity, and auditability, "Operability" covering the subcategories manageability, efficiency, effectiveness, automation, cost, and availability, "Technology" covering the subcategories standardization, interoperability, flexibility, and portability, and "User" covering the subcategories simplicity, privacy, trust, and control. Building on these requirement categories and the new paradigm of decentralized identity management called SSI, we developed a prototype and had it evaluated by the twelve domain experts. Our prototype and the evaluation process suggest

that integrating SSI into IAM systems can offer advantages in each of the four requirements categories. We conclude that SSI can indeed help improve IAM systems. These improvements encompass, for example, the possibility of selective disclosure, the fast onboarding and off-boarding of employees (revocation), consideration of the principle of least privilege, and the possibility of a higher degree of automation to improve efficiency and manageability.

Supplementary Information The online version contains supplementary material available at https://doi.org/10.1007/s12599-023-00830-x.

Acknowledgements This research was funded in part by the Luxembourg National Research Fund (FNR) through the FiReSPArX (grant reference 14783405) and PABLO (grant reference 16326754) projects and by PayPal, grant reference "P17/IS/13342933/PayPal-FNR/Chair in DFS/Gilbert Fridgen" (PEARL). We also gratefully acknowledge the support of the Bavarian Ministry of Economic Affairs, Regional Development and Energy in form of their funding of the project "Fraunhofer Blockchain Center (20-3066-2-6-14)" that made this paper possible. We further thank the editor and the anonymous reviewers for their highly valuable and constructive feedback. For the purpose of open access, 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

Acemyan CZ, Kortum P, Xiong J, Wallach DS (2018) 2FA might be secure, but it's not usable: a summative usability assessment of Google's two-factor authentication (2FA) methods. Proc Human Factors Ergon Soc Annu Meeting SAGE 62:1141–1145. https://doi.org/10.1177/1541931218621262

Ahn GJ, Ko M, Shehab M (2009) Privacy-enhanced user-centric identity management. In: Proceedings of the international conference on communications, IEEE, https://doi.org/10.1109/ICC.2009.5199363

Alsmadi I (2019) Identity management. In: The NICE cyber security framework, Springer, Heidelberg, chap 12, pp 313–329

Babel M, Sedlmeir J (2023) Bringing data minimization to digital wallets at scale with general-purpose zero-knowledge proofs. arXiv:2301.00823. Accessed 9 Aug 2023

Backes M, Camenisch J, Sommer D (2005) Anonymous yet accountable access control. In: Proceedings of the ACM workshop on privacy in the electronic society, ACM, pp 40–46, https://doi.org/10.1145/1102199.1102208

Bartolomeu PC, Vieira E, Hosseini SM, Ferreira J (2019) Self-sovereign identity: use-cases, technologies, and challenges for industrial IoT. In: Proceedings of the 24th international conference on emerging technologies and factory automation, IEEE, pp 1173–1180, https://doi.org/10.1109/ETFA.2019.8869262

Baskerville R, Baiyere A, Gregor S, Hevner A, Rossi M (2018) Design science research contributions: finding a balance between artifact and theory. J AIS 19:358–376. https://doi.org/10.17705/1jais.00495

Beck R, Weber S, Gregory RW (2013) Theory-generating design science research. Inf Syst Front 15:637–651. https://doi.org/10.1007/s10796-012-9342-4

Belchior R, Putz B, Pernul G, Correia M, Vasconcelos A, Guerreiro S (2020) SSIBAC: self-sovereign identity based access control. In: Proceedings of the 19th international conference on trust, security and privacy in computing and communications, IEEE, pp 1935–1943, https://doi.org/10.1109/TrustCom50675.2020.00264

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

Bertino E, Takahashi K (2011) Identity management: concepts, technologies, and systems. Artech House, London

Bertino E, Bonatti PA, Ferrari E (2001) TRBAC: a temporal role-based access control model. ACM Transact Inf Syst Secur (TISSEC) 4:191–233. https://doi.org/10.1145/501978.501979

Bonneau J, Herley C, Van Oorschot PC, Stajano F (2012) The quest to replace passwords: a framework for comparative evaluation of web authentication schemes. In: Symposium on security and privacy, IEEE, pp 553–567, https://doi.org/10.1109/SP.2012.44

Bradford M, Earp JB, Grabski S (2014) Centralized end-to-end identity and access management and ERP systems: a multi-case analysis using the technology organization environment framework. Int J Account Inf Syst 15:149–165. https://doi.org/10.1016/j.accinf.2014.01.003

Braun CHJ, Papanchev V, Käfer T (2023) SISSI: an architecture for semantic interoperable self-sovereign identity-based access control on the web. In: Proceedings of the ACM web conference 2023, pp 3011–3021. https://doi.org/10.1145/3543507.3583409

Bringer JD, Johnston LH, Brackenridge CH (2004) Maximizing transparency in a doctoral thesis 1: the complexities of writing about the use of QSR*NVIVO within a grounded theory study. Qual Res 4:247–265. https://doi.org/10.1177/1468794104044434

Brod M, Tesler LE, Christensen TL (2009) Qualitative research and content validity: developing best practices based on science and experience. Qual Life Res 18:1263–1278. https://doi.org/10.1007/s11136-009-9540-9

Buck C, Olenberger C, Schweizer A, Völter F, Eymann T (2021) Never trust, always verify: a multivocal literature review on current knowledge and research gaps of zero-trust. Comput Secur 110(102):436. https://doi.org/10.1016/j.cose.2021.102436

Camenisch J, Lysyanskaya A (2001) An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In: Proceedings of the international conference on the theory and applications of cryptographic techniques, Springer, Heidelberg, pp 93–118, https://doi.org/10.1007/3-540-44987-6_7

Casassa Mont M, Bramhall P, Pato J (2003) On adaptive identity management: the next generation of identity management technologies. https://www.hpl.hp.com/techreports/2003/HPL-2003-149.pdf. Accessed 9 Aug 2023

Chadwick DW (2020) Why I do NOT need DIDs or a DLT for VCs and SSI. https://verifiablecredentials.info/contact-us. Accessed 9 Aug 2023

Charmaz K (2014) Constructing grounded theory. Sage, Thousand Oaks

Cram WA, Proudfoot JG, D'Arcy J (2021) When enough is enough: investigating the antecedents and consequences of information security fatigue. Inf Syst J 31:521–549. https://doi.org/10.1111/isj.12319

Čučko Š, Turkanović M (2021) Decentralized and self-sovereign identity: systematic mapping study. IEEE Access 9:139,009-139,027. https://doi.org/10.1109/ACCESS.2021.3117588

Damon F, Coetzee M (2013) Towards a generic identity and access assurance model by component analysis – a conceptual review. In: Proceedings of the first international conference on enterprise systems, IEEE, https://doi.org/10.1109/ES.2013.6690086

Damon F, Coetzee M (2018) The design of an identity and access management assurance dashboard model. In: Proceedings of the international conference on research and practical issues of

enterprise information systems, Springer, Heidelberg, pp 123–133, https://doi.org/10.1007/978-3-319-99040-8_10
D'Costa-Alphonso MM, Lane M (2010) The adoption of single sign-on and multifactor authentication in organisations: a critical evaluation using TOE framework. Issues Inform Sci Inf Technol 7:161–189. https://doi.org/10.28945/1199
Deloitte (2020) Impact of COVID-19 on cybersecurity. https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html. Accessed 9 Aug 2023
Di Francesco Maesa D, Lisi A, Mori P, Ricci L, Boschi G (2023) Self sovereign and blockchain based access control: supporting attributes privacy with zero knowledge. J Netw Comput Appl 212(103):577. https://doi.org/10.1016/j.jnca.2022.103577
Dyble J (2020) McAfee: cybercrime costs the global economy $600bn annually. https://technologymagazine.com/data-and-data-analytics/mcafee-cybercrime-costs-global-economy-dollar600bn-annually,. Accessed 9 Aug 2023
Eekels J, Roozenburg NF (1991) A methodological comparison of the structures of scientific research and engineering design: their similarities and differences. Design Stud 12:197–203. https://doi.org/10.1016/0142-694X(91)90031-Q
Ehrlich T, Richter D, Meisel M, Anke J (2021) Self-Sovereign identity als Grundlage für universell einsetzbare digitale Identitäten. HMD Prax Wirtschaftsinform 58:247–270. https://doi.org/10.1365/s40702-021-00711-5
Enterprise Management Associates, Inc (2020) Contextual awareness: advancing identity and access management to the next level of security effectiveness. https://www.enzoic.com/wp-content/uploads/EMA-Contextual-Awareness-Report-03.2020-ENZOIC-SUMMARY.pdf. Accessed 9 Aug 2023
European Commission (2021) Commission proposes a trusted and secure digital identity for all Europeans. https://ec.europa.eu/commission/presscorner/detail/en/IP_21_2663. Accessed 9 Aug 2023
Fairchild A, Ribbers P (2011) Privacy-enhancing identity management in business. In: Camenisch J, Leenes R, Sommer D (eds) Digital Privacy. Springer, Heidelberg, pp 107–129. https://doi.org/10.1007/978-3-642-19050-6_7
Ferraiolo DF, Chandramouli R, Kuhn DR (2007) Role-based access control, 2nd edn. Artech House, London
Feulner S, Sedlmeir J, Schlatt V, Urbach N (2022) Exploring the use of self-sovereign identity for event ticketing systems. Electron Market 32:1759–1777. https://doi.org/10.1007/s12525-022-00573-9
Forina M, Armanino C, Raggio V (2002) Clustering with dendrograms on interpretation variables. Analytica Chimica Acta 454:13–19. https://doi.org/10.1016/S0003-2670(01)01517-3
Frank M, Kohn V (2021) How to mitigate security-related stress: the role of psychological capital. In: Proceedings of the 55th Hawaii international conference on system sciences, pp 4538–4547. https://doi.org/10.24251/HICSS.2021.550
Fuchs L, Pernul G (2013) Qualitätssicherung im Identity-und Access Management. HMD Prax Wirtschaftsinform 50:88–97
Gartner Inc (2020) Hype cycle for identity and access management technologies. https://www.gartner.com/en/documents/4004062. Accessed 9 Aug 2023
Glaude M, Kudra A (2021) SSI for identity & access management (IAM). https://northernblock.io/ssi-for-identity-access-management-iam/. Accessed 9 Aug 2023
Globenewswire (2020) New ESG & JumpCloud study uncovers IT's biggest identity and security challenges due to COVID-19. https://www.globenewswire.com/news-release/2020/10/02/2102941/0/en/New-ESG-JumpCloud-Study-Uncovers-IT-s-Biggest-Identity-and-Security-Challenges-Due-to-COVID-19.html. Accessed 9 Aug 2023
Goldwasser S, Micali S, Rackoff C (1989) The knowledge complexity of interactive proof systems. SIAM J Comput 18:186–208. https://doi.org/10.1137/0218012
Graef I, Verschakelen J, Valcke P (2013) Putting the right to data portability into a competition law perspective. Law J High School Econ Annu Rev pp 53–63
Grech A, Sood I, Ariño L (2021) Blockchain, self-sovereign identity and digital credentials: promise versus praxis in education. Front Blockchain 4:7. https://doi.org/10.3389/fbloc.2021.616779
Gregor S, Hevner AR (2013) Positioning and presenting design science research for maximum impact. MIS Q 37:337–355. https://doi.org/10.25300/misq/2013/37.2.01
Guggenberger T, Lockl J, Röglinger M, Schlatt V, Sedlmeir J, Stoetzer JC, Urbach N, Völter F (2021) Emerging digital technologies to combat future crises: learnings from COVID-19 to be prepared for the future. Int J Innov Technol Manag 18:2140,002. https://doi.org/10.1142/S0219877021400022
Guggenberger T, Neubauer L, Stramm J, Völter F, Zwede T (2023) Accept me as I am or see me go: a qualitative analysis of user acceptance of self-sovereign identity applications. In: Proceedings of the 56th Hawaii international conference on system sciences, pp 6560–6569. https://hdl.handle.net/10125/103427
Haber MJ (2020) Privileged access management. In: Privileged attack vectors, Springer, Heidelberg, pp 151–171, https://doi.org/10.1007/978-1-4842-5914-6_11
Haber MJ, Rolls D (2020) Identity attack vectors: implementing an effective identity and access management solution. Apress, New York
Hardman D (2020) No paradox here: ZKPs deliver savvy trust. https://www.evernym.com/blog/no-paradox-here-zkps-deliver-savvy-trust/. Accessed 9 Aug 2023
Harry B, Sturges KM, Klingner JK (2005) Mapping the process: an exemplar of process and challenge in grounded theory analysis. Edu Res 34:3–13. https://doi.org/10.3102/0013189X034002003
Hevner AR (2007) A three cycle view of design science research. Scand J Inf Syst 19, http://aisel.aisnet.org/sjis/vol19/iss2/4
Hevner AR, March ST, Park J, Ram S (2004) Design science in information systems research. MIS Q 28:75–105. https://doi.org/10.2307/25148625
Hoepman JH, Joosten R, Siljee J (2008) Comparing identity management frameworks in a business context. In: IFIP summer school on the future of identity in the information society, Springer, Heidelberg, pp 184–196, https://doi.org/10.1007/978-3-642-03315-5_14
Hu VC, Kuhn DR, Ferraiolo DF, Voas J (2015) Attribute-based access control. Comput 48:85–88. https://doi.org/10.1109/MC.2015.33
Hummer M, Groll S, Kunz M, Fuchs L, Pernul G (2018) Measuring identity and access management performance – an expert survey on possible performance indicators. In: Proceedings of the international conference on information systems security and privacy, pp 233–240, https://doi.org/10.5220/0006557702330240
IDG Business Media GmbH (2017) Studie Identity- & Access-Management 2017. https://www.airlock.com/fileadmin/content/07_Airlock-PDFs/Studie_Identity-_und_Access_Management_2017.pdf. Accessed 9 Aug 2023
Irwin L (2021) The cyber security risks of working from home. https://www.itgovernance.co.uk/blog/the-cyber-security-risks-of-working-from-home. Accessed 9 Aug 2023
Jacobson K (2020) 8 scary statistics about the password reuse problem. https://securityboulevard.com/2020/04/8-scary-statistics-about-the-password-reuse-problem/. Accessed 9 Aug 2023
Johannesson P, Perjons E (2014) An introduction to design science, vol 10. Springer, Heidelberg

Jørgensen KP, Beck R (2022) Universal wallets. Bus Inf Syst Eng pp 115–125, https://doi.org/10.1007/s12599-021-00736-6

Jøsang A, Pope S (2005) User centric identity management. In: Proceedings of the AUSCERT Asia Pacific information technology security conference, Citeseer, pp 77–89. https://citeseerx.ist.psu.edu/document?repid=rep1 &type=pdf &doi=6bf895c183de4673085f556b2d89043a95a21759

Juniper Research (2019) Business losses to cybercrime data breaches to exceed $5 trillion by 2024. https://www.juniperresearch.com/press/business-losses-cybercrime-data-breaches. Accessed 9 Aug 2023

Kern A, Walhorn C (2005) Rule support for role-based access control. In: Proceedings of the tenth symposium on access control models and technologies, ACM, pp 130–138. https://doi.org/10.1145/1063979.1064002

Keszthelyi A, Michelberger P (2012) From the IT authorisation to the role- and identity management. In: 4th international symposium on logistics and industrial informatics, IEEE, pp 173–178. https://doi.org/10.1109/LINDI.2012.6319483

Khayretdinova A, Kubach M, Sellung R, Roßnagel H (2022) Conducting a usability evaluation of decentralized identity management solutions. In: Selbstbestimmung, Privatheit und Datenschutz: Gestaltungsoptionen für einen europäischen Weg, Springer, Heidelberg, pp 389–406, https://doi.org/10.1007/978-3-658-33306-5_19

Kitchenham B, Pearl Brereton O, Budgen D, Turner M, Bailey J, Linkman S (2009) Systematic literature reviews in software engineering - a systematic literature review. Inf Softw Technol 51:7–15. https://doi.org/10.1016/j.infsof.2008.09.009

Kubach M, Sellung R (2021) On the market for self-sovereign identity: structure and stakeholders. In: Open Identity Summit, pp 143–154. https://dl.gi.de/handle/20.500.12116/36488

Kubach M, Schunck CH, Sellung R, Roßnagel H (2020) Self-sovereign and decentralized identity as the future of identity management? Open Identity Summit, pp 35–47, https://doi.org/10.18420/ois2020_03

Kuperberg M, Klemens R (2022) Integration of self-sovereign identity into conventional software using established IAM protocols: a survey. In: Open Identity Summit, pp 51–60. https://doi.org/10.18420/OID2022_04

Lee AS (2001) Editor's comments. MIS Q 25:iii–vii, https://www.jstor.org/stable/3250954

Levy Y, Ellis TJ (2006) A systems approach to conduct an effective literature review in support of information systems research. Inform Sci J 9:181–212. https://doi.org/10.28945/479

Li J, Karp AH (2007) Access control for the services oriented architecture. In: Proceedings of the workshop on secure web services, ACM, pp 9–17. https://doi.org/10.1145/1314418.1314421

Linux Foundation (2020) Hyperledger Aries Cloud Agent – Python. https://github.com/hyperledger/aries-cloudagent-python. Accessed 9 Aug 2023

Lioy A, Marian M, Moltchanova N, Pala M (2006) PKI past, present and future. Int J Inf Secur 5:18–29. https://doi.org/10.1007/s10207-005-0077-9

Lissi (2021) Diskussion über die Sicherheit von Wallets für digitale Identitäten. https://lissi-id.medium.com/diskussion-%C3%BCber-die-sicherheit-von-wallets-f%C3%BCr-digitalen-identit%C3%A4ten-d1c6218fef66. Accessed 9 Aug 2023

LogMeIn (2019) Der dritte jährliche globale Passwort-Sicherheitsreport. https://www.lastpass.com/de/business/articles/password-benchmark-report. Accessed 9 Aug 2023

Mezler-Andelberg C (2008) Identity Management - eine Einführung: Grundlagen, Technik, wirtschaftlicher Nutzen. Dpunkt, Heidelberg

Mühle A, Grüner A, Gayvoronskaya T, Meinel C (2018) A survey on essential components of a self-sovereign identity. Comput Sci Rev 30:80–86. https://doi.org/10.1016/j.cosrev.2018.10.002

Naidoo R (2020) A multi-level influence model of COVID-19 themed cybercrime. Europ J Inf Syst 29:306–321. https://doi.org/10.1080/0960085X.2020.1771222

O'Gorman L (2003) Comparing passwords, tokens, and biometrics for user authentication. Proc IEEE 91:2021–2040. https://doi.org/10.1109/JPROC.2003.819611

Oh S, Park S (2003) Task-role-based access control model. Inf Syst 28:533–562. https://doi.org/10.1016/S0306-4379(02)00029-7

Onwuegbuzie AJ, Frels RK, Hwang E (2016) Mapping Saldaña's coding methods onto the literature review process. J Edu Issues 2:130–150

Osmanoglu E (2014) Identity and access management: business performance through connected intelligence. Elsevier, Amsterdam

Peffers K, Tuunanen T, Rothenberger MA, Chatterjee S (2007) A design science research methodology for information systems research. J Manag Inf Syst 24:45–77. https://doi.org/10.2753/mis0742-1222240302

Podsakoff PM, MacKenzie SB, Lee JY, Podsakoff NP (2003) Common method biases in behavioral research: a critical review of the literature and recommended remedies. J Appl Psychol 88:879–903. https://doi.org/10.1037/0021-9010.88.5.879

Pöhn D, Hommel W (2020) An overview of limitations and approaches in identity management. In: Proceedings of the 15th international conference on availability, reliability and security, https://doi.org/10.1145/3407023.3407026

Ponemon Institute (2019) Cost of a data breach report. https://www.ibm.com/downloads/cas/RDEQK07R. Accessed 9 Aug 2023

Preukschat A, Reed D (2021) Self-sovereign identity: decentralized digital identity and verifiable credentials. Manning, Shelter Island, NY

Puchta A, Böhm F, Pernul G (2019) Contributing to current challenges in identity and access management with visual analytics. In: IFIP annual conference on data and applications security and privacy, Springer, Heidelberg, pp 221–239, https://doi.org/10.1007/978-3-030-22479-0_12

Richter D, Praas CR, Anke J (2023) Beyond paper and plastic: a meta-model for credential use and governance. In: Proceedings of the 31st European conference on information systems. https://aisel.aisnet.org/ecis2023_rp/371/. Accessed 9 Aug 2023

Royer D (2013) EIdM: concepts, technologies, and application fields. In: Enterprise Identity Management, Springer, Heidelberg, pp 27–56, https://doi.org/10.1007/978-3-642-35040-5_3

Ruff T (2018) The three models of digital identity relationships. https://medium.com/evernym/the-three-models-of-digital-identity-relationships-ca0727cb5186. Accessed 9 Aug 2023

Sadler T, Hancock J (2020) A Stanford deception expert and cybersecurity CEO explain why people fall for online scams. https://www.fastcompany.com/90542273/a-stanford-deception-expert-explains-why-people-fall-for-online-scams. Accessed 9 Aug 2023

Saldaña J (2015) The coding manual for qualitative researchers. Sage, Thousand Oaks

Sartor S, Sedlmeir J, Rieger A, Roth T (2022) Love at first sight? A user experience study of self-sovereign identity wallets. In: Proceedings of the 30th European conference on information systems, AIS. https://aisel.aisnet.org/ecis2022_rp/46/. Accessed 9 Aug 2023

Schellinger B, Sedlmeir J, Willburger L, Strüker J, Urbach N (2022) Mythbusting self-sovereign identity (SSI): discussion paper on user-centric identities. https://www.fim-rc.de/Paperbibliothek/Veroeffentlicht/1426/wi-1426.pdf. Accessed 9 Aug 2023

Schlackl F, Link N, Hoehle H (2022) Antecedents and consequences of data breaches: a systematic review. Inf Manag 59(103):638. https://doi.org/10.1016/j.im.2022.103638

Schlatt V, Sedlmeir J, Feulner S, Urbach N (2022) Designing a framework for digital KYC processes built on blockchain-based self-sovereign identity. Inf Manag 59(103):553. https://doi.org/10.1016/j.im.2021.103553

Schlatt V, Sedlmeir J, Traue J, Völter F (2022) Harmonizing sensitive data exchange and double-spending prevention through blockchain and digital wallets: the case of e-prescription management. Distrib Ledger Technol Res Pract 2. https://doi.org/10.1145/3571509

Schmidt K, Mühle A, Grüner A, Meinel C (2021) Clear the fog: Towards a taxonomy of self-sovereign identity ecosystem members. In: Proceedings of the 18th international conference on privacy, security and trust, IEEE, https://doi.org/10.1109/PST52912.2021.9647797

Schwalm S, Albrecht D, Alamillo I (2022) eIDAS 2.0: challenges, perspectives and proposals to avoid contradictions between eIDAS 2.0 and SSI. In: Open Identity Summit, pp 63–74. https://doi.org/10.18420/OID2022_05

Sedlmeir J, Ross P, Luckow A, Lockl J, Miehle D, Fridgen G (2021) The DLPS: a new framework for benchmarking blockchains. In: Proceedings of the 54th Hawaii international conference on system sciences, pp 6855–6864. https://doi.org/10.24251/hicss.2021.822

Sedlmeir J, Barbereau T, Huber J, Weigl L, Roth T (2022) Transition pathways towards design principles of self-sovereign identity. In: Proceedings of the 43rd international conference on information systems, AIS. https://aisel.aisnet.org/icis2022/is_implement/is_implement/4/. Accessed 9 Aug 2023

Sinclair S, Smith SW (2008) Preventative directions for insider threat mitigation via access control. In: Stolfo SJ, Bellovin SM, Keromytis AD, Hershkop S, Smith SW, Sinclair S (eds) Insider Attack and Cyber Security. Springer, Heidelberg, pp 165–194. https://doi.org/10.1007/978-0-387-77322-3_10

Small M (2006) Unify and simplify: Re-thinking identity management. Netw Secur 2006:11–14. https://doi.org/10.1016/S1353-4858(06)70411-1

Smith D (2008) The challenge of federated identity management. Netw Secur 2008:7–9. https://doi.org/10.1016/S1353-4858(08)70051-5

Smith HA, McKeen JD (2011) The identity management challenge. Commun AIS 28, https://doi.org/10.17705/1CAIS.02811

Soltani R, Nguyen UT, An A (2021) A survey of self-sovereign identity ecosystem. Secur Commun Netw 2021:1–26. https://doi.org/10.1155/2021/8873429

Sporny M, Longley D, Chadwick D (2021) Verifiable credentials data model 1.1: expressing verifiable information on the Web. https://www.w3.org/TR/vc-data-model/. Accessed 9 Aug 2023

Strauss A, Corbin J (1998) Basics of qualitative research: techniques and procedures for developing grounded theory. Sage, Thousand Oaks

Thakur MA, Gaikwad R (2015) User identity and access management trends in IT infrastructure – an overview. In: Proceedings of the international conference on pervasive computing, IEEE, https://doi.org/10.1109/PERVASIVE.2015.7086972

Theofanos M, Garfinkel S, Choong YY (2016) Secure and usable enterprise authentication: lessons from the field. IEEE Secur Priv 14:14–21. https://doi.org/10.1109/MSP.2016.96

Velocity Smart Technology (2021) Velocity smart market research report 2021. https://www.velocity-smart.com/en-gb/velocity-smart-technology-market-research-report-2021. Accessed 9 Aug 2023

Venable J, Baskerville R (2012) Eating our own cooking: toward a more rigorous design science of research methods. Electron J Bus Res Method 10:141–153

Verizon (2020) 2020 Data breach investigations report. https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf,. Accessed 9 Aug 2023

Walter T, Bussard L, Robinson P, Roudier Y (2004) Security and trust issues in ubiquitous environments – the business-to-employee dimension. In: International symposium on applications and the internet workshops, IEEE, pp 696–701, https://doi.org/10.1109/SAINTW.2004.1268723

Windley PJ (2005) Digital Identity: unmasking identity management architecture (IMA). O'Reilly, Sebastopol

Yildiz H, Ritter C, Nguyen LT, Frech B, Martinez MM, Küpper A (2021) Connecting self-sovereign identity with federated and user-centric identities via SAML integration. In: Symposium on computers and communications, IEEE, https://doi.org/10.1109/ISCC53001.2021.9631453

Yubico, 451 Research (2021) Work-from-home policies driving MFA adoption, but still work to be done. https://resources.yubico.com/53ZDUYE6/at/kxjzxgg79h94js67jt8mnv/451_Advisory_BW_Yubico_v2.pdf. Accessed 9 Aug 2023

Zhao X, Johnson ME (2010) Managing information access in data-rich enterprises with escalation and incentives. Int J Electron Commer 15:79–112. https://doi.org/10.2753/JEC1086-4415150104

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.