A TAXONOMY OF MODERN USER-CENTRIC IDENTITY MANAGEMENT: FROM THEORY TO PRACTICE

Completed Research Paper

Pol Hölzmer, University of Luxembourg, SnT, Luxembourg, Luxembourg, pol.hoelzmer@uni.lu

Johannes Sedlmeir, University of Luxembourg, SnT, Luxembourg, Luxembourg, johannes.sedlmeir@uni.lu

Adnan Imeri, Luxembourg Institute of Science and Technology, Esch-sur-Alzette, Luxembourg, adnan.imeri@list.lu

Abstract

Modern digital identity management (IdM) systems embrace self-sovereign and decentralised identities as core paradigms following user-centric principles. While the theoretical principles and technical specifications underlying modern IdM systems have converged, corresponding real-world solutions' adherence can be obscured by claims over design principles. To clear the fog, we develop a taxonomy for modern user-centric IdM systems through eight iterations of literature reviews and solution evaluations. To this end, we define the theoretical characteristics to achieve user wholeness, data autonomy, application usability, and the practical characteristics of the technology stack, architecture sharing, and system trust. This taxonomy contributes to a deeper understanding of modern IdM solutions' design and implementation decisions. We demonstrate the taxonomy's usefulness by evaluating five real-world solutions' adherence and capturing the diversity within the evolving digital identity ecosystem. We thereby enable practitioners and researchers to make informed arguments about which IdM characteristics best suit their specific needs and contexts.

Keywords: Self-Sovereign Identity, Decentralized Identity, Identity Wallet, Identity Management.

1 Introduction

Modern information systems require strong identity management (IdM) frameworks that provide effective identification, authentication, and authorisation processes (Rieger et al., 2024). However, digital IdM faces challenges, such as security risks, regulatory compliance requirements, and growing privacy concerns (Sheik et al., 2021). Academic research has become increasingly critical of traditional IdM solutions (Sedlmeir et al., 2021), highlighting conceptual drawbacks and calling for improvements (Abbas & Munoz, 2021). Correspondingly, researchers push towards user-centric and trust-worthy IdM systems that enhance user control while still ensuring verifiability (Babel & Sedlmeir, 2023).

As such, the self-sovereign identity (SSI) paradigm emerged (Allen, 2016) and has been adopted as a modern approach for IdM in both private and public domains (European Commission, 2024a; Jones, 2024). Unlike the traditional IdM models (Rieger et al., 2024), SSI offers a decentralised and user-centric approach that decouples the identity provider (IdP) from the relying party (RP) through digital identity wallets controlled by the user (Bastian et al., 2023). The term SSI is frequently used interchangeably with decentralised, blockchain-based identity models (Kubach et al., 2020), yet its dependency on blockchain technology is contested (Sedlmeir et al., 2021). The initial guiding principles of SSI, defined by Allen (2016), evolved as they were embraced by different domains, reflecting a diversity of stakeholders' needs and requirements (Sedlmeir et al., 2022). Yet, the technical specifications that ensure adherence to these principles in modern IdM are ambiguous, causing confusion in academic and practitioner domains (Smethurst, 2023; Weigl et al., 2023).

Therefore, this paper answers the research question of *what are the dimensions and characteristics of modern user-centric identity management systems* by contributing a multi-layer taxonomy based on iterative literature reviews (theory) and solution evaluations (practice), following the extended taxonomy design process (ETDP) (Kundisch et al., 2022). Our taxonomy provides a holistic overview of modern user-centric IdM systems by synthesising the intersections between different paradigms and implementations. In examining the broad spectrum of these systems' theoretical and practical characteristics, we enrich the discourse on the evolution of motivations for *self-sovereign* identity and whether or not solutions adhere to the theoretical principles (Allen, 2016; Sedlmeir et al., 2022).

The paper is structured as follows: Section 2 introduces essential models and principles of modern user-centric IdM. Section 3 explains our methodology, including the iterative taxonomy design through literature reviews and solution evaluations. Section 4 presents the developed taxonomy's layers, dimensions and characteristics. Section 5 demonstrates the taxonomy by evaluating selected real-world solutions. Finally, Section 6 discusses limitations and highlights future research opportunities.

2 Background

IdM refers to the process of managing users' identity data, encompassing identifiers, attributes, and credentials (Pfitzmann & Hansen, 2010). Traditional IdM models are typically classified as *siloed* (or isolated) with distinct IdM per application, *federated* with centralised IdM for multiple applications, and *user-centric* models where users have greater control over their own identities, deciding what information they share across different applications (Mohammed et al., 2020; Wilson & Hingnikar, 2019). This terminology varies across the literature, reflecting the diverse perspectives on conceptualising models (Rieger et al., 2024) while leading to inconsistencies in their interpretation, as oversimplified terms represent a complex system from different viewpoints (Mohammed et al., 2020), motivating the creating of holistic taxonomy for modern user-centric IdM based on confusions over what self-sovereign, decentralised and wallet-based IdMs characterise, unified or differentiated.

SSI has emerged as a fundamental paradigm for *modern* user-centric IdM in recent years (Allen, 2016). Compared to the traditional user-centric model, SSI ultimately decouples the IdP (i.e., issuer) from the RP (i.e., verifier) and empowers users (i.e., holders) to self-manage their identity data (Weigl et al., 2023). In this model, an IdP issues long-lived attestations of attributes to the identity holder so that RPs can verify their integrity, authenticity, and validity upon presentation by the holder without involving the IdP. Verifiability is ensured through cryptographic mechanisms and (decentralised) trust infrastructures (Sedlmeir et al., 2022). Therefore, in some contexts, SSI is referred to as blockchain-based or wallet-based IdM, exposing similarities but also certain trade-offs (Hoess et al., 2022; Bastian et al., 2023). As such, blockchain-based solutions emphasise the role of distributed ledgers as a trust anchor (Bochnia et al., 2024), while wallet-based solutions focus on user-controlled credentials.

We base our design on the well-established (Čučko et al., 2022; Naik & Jenkins, 2020a) principles by Allen (2016) and Sedlmeir (2022) as the meta-characteristics of our taxonomy. Allen's (2016) ten principles served as guiding tenets for the development and understanding of SSI in the digital identity community (Sedlmeir et al., 2021; Shuaib et al., 2021). *Existence* underscores the need for users to have an independent identity that is not solely digital. *Control* emphasises that users must be the ultimate authority over their identities, including updates and visibility. *Access* specifies that users should be able to retrieve all their identity-related data easily. Transparency demands that the systems and algorithms governing these identities be open and transparent. *Persistence* asserts that identities should be long-lived, even outlasting the services that first generated them. *Portability* ensures identity data isn't limited to a third party, allowing user control and flexibility. *Interoperability* stresses that these identities should be globally usable. *Consent* mandates that data sharing only occurs with the user's explicit agreement. *Minimalisation* recommends keeping data disclosure to a bare minimum. Finally, *protection* declares that user rights must always take precedence.

While these ten principles serve as the theoretical foundation of SSI, the design principles proposed by Sedlmeir et al. (2022) guide the practical implementation and account for industry best practices and use in regulated environments. *Representation* stresses that SSI should be flexible enough to represent

any entity digitally, whether human, legal, or technical. *Control* emphasises that users must actively consent to disclose their digital identity attributes. *Flexibility* is a key principle that prevents vendor lock-in by promoting interoperable standards and open-source projects. *Security* mandates the use of advanced cryptographic techniques and secure, authenticated communications to protect digital identity data. *Privacy* mandates that only essential data is revealed on a need-to-know basis through bilateral communication, consent, and minimisation. *Verifiability* ensures that the validity and timeliness of credentials can be efficiently checked. *Authenticity* establishes that credentials are uniquely bound to their initial bearers, reducing the risk of identity theft and sharing. *Reliability* offers a guidance system for verifiers to determine trustworthy issuers within a resilient infrastructure. Finally, *usability* focuses on the user experience and a system that is efficient, easy to recover, and offers multiple access points.

Besides Allen (2016) and Sedlmeir et al. (2022), related work provides a solid foundation for this study. Naik and Jenkins (2020a) articulate SSI principles, strengthening our theoretical understanding of identity sovereignty and control. Čučko et al. (2022) classify and validate SSI properties through expert evaluation, clarifying user-centric attributes. Schardong and Custódio (2022) bridge conceptual and practical dimensions through a systematic taxonomy of SSI, emphasising blockchain implementation nuances. Similarly, Lesavre et al. (2020) categorise blockchain IdM architectures and governance mechanisms, while Yildiz et al. (2023) define interoperability via a structured reference model. Bastian et al. (2023) categorise wallet security and usability properties, linking theory and practice. Building upon these and the rich body of further research and the analysis of solutions, we synthesise and integrate existing knowledge to provide a holistic taxonomy of modern user-centric identity management.

3 Design Process

Our research follows an iterative design science research (DSR) approach following the extended taxonomy design process (ETDP) (Kundisch et al., 2022). This approach enables the continuous refinement and expansion of our taxonomy to create a holistic overview of modern user-centric IdM systems. We revisit the design and development stages over eight iterations to ensure our taxonomy's relevance, completeness, and usefulness. We cover theoretical concepts and technical solutions to get a complete overview of the characteristics of modern IdM solutions and their trajectory from theory to practice. We adopt the design principles (Allen, 2016; Sedlmeir et al., 2022) as meta-characteristics (Nickerson et al., 2013), representing the foundation of our taxonomy, which we extend and refine with each iteration until the ending conditions are met. We define our ending conditions as the point at which our taxonomy fully encompasses all characteristics of a modern user-centric identity management system, which is determined through iterative literature reviews and evaluations of technical solutions until no further updates to the taxonomy are necessary (Nickerson et al., 2013). We alternated between empirical-to-conceptual design iterations consisting of multiple batches of SLRs following the PRISMA approach (Moher et al., 2009) and conceptual-to-empirical iterations consisting of evaluations of implemented IdM solutions that claim to embrace modern user-centric paradigms, particularly SSI.

3.1 Literature Review

By following the PRISMA guidelines (Moher et al., 2009), we provide structure to our SLR, allowing us to assess the academic discourse on modern user-centric IdM systems. Relevant literature was first identified using targeted search strings across databases and libraries. During screening, irrelevant records were removed. In the eligibility phase, full texts were assessed for relevance. Selected studies were used for the taxonomy design, with further additions through snowballing (Webster & Watson, 2002) and iterative review of three different search strings. This extended SLR ensures broad coverage of nuanced, domain-specific information on which we base the development of our taxonomy. Therefore, with each search string, we follow the PRISMA stages to cover different selections of papers based on a distinct yet overlapping focus and search string to provide us with rich and balanced insights.

Our extended SLR covers three different search strings (*S1*, *S2*, *S3*), each alternating with an ETDP iteration of solution evaluation that complements insights from the literature to support the design of the taxonomy. *S1* ((*self-sovereign identity*) *OR* (*self-sovereignty AND identity*)) aimed to provide an initial

overview of the discourse around the core principles of this rather new paradigm that initiated the push towards modern user-centric IdM (Allen, 2016). *S2* ((*block[-]chain[-based] OR decentral[i[zs]ed]*) *AND* (*identity*)) focuses on works that embrace the ideas of SSI and have been part of the blockchain hype in digital IdM (Hoess et al. 2022). Finally, *S3* ((*digital identity wallet*) *OR* (*digital wallet AND identity*) *OR* (*wallet-based identity*)) allows getting insights into the latest developments in regards to regulatory and business constraints (Sedlmeir et al., 2022) towards a more balanced view of, e.g., the European Union's digital identity wallet (EUDIW) (European Commission, 2020). To identify relevant literature, we queried eight scientific databases: *AISeL*, *ACM DL*, *IEEE Xplore*, *ScienceDirect*, *Springer Link*, and *Scopus.* We saturate the results using *ArXiv*, *Google Scholar*, *Dimensions* and *Elicit*. While we emphasised peer-reviewed literature, we also included grey literature, such as documentation and white papers, during the solution evaluation and final snowballing phase (Webster & Watson, 2002).

To support the development of a holistic taxonomy, our analysis required broad coverage across diverse perspectives within the modern user-centric IdM domain and, therefore, allowed for broad inclusion criteria. Screening was conducted based on titles, abstracts, and other metadata to exclude works that were either unrelated to our search strings or addressed the topic only tangentially. We included papers written in English and published since SSI emerged in 2016 until 2024 Q2 as our measure for *modern* IdM. In the subsequent eligibility phase, we conducted a detailed full-text review to assess the relevance and depth of each work. We included only papers with clear conceptual or technical contributions.

Due to the iterative nature of our research design, we introduced an additional refinement step to the PRISMA process, which we refer to as a *focus* stage. In this step, we temporarily defer eligible papers that are not immediately relevant to the current iteration of the taxonomy-building process. These papers are not excluded but rather held for re-evaluation in future iterations, allowing us to maintain analytical clarity. This is important due to the evolving terminology and conceptual overlap across different phases of modern IdM. Early literature often focused on self-sovereign identity, which later expanded into decentralised and wallet-based identity narratives, each building upon and redefining the former. As these paradigms emerged and shifted over time, so did their associated use cases and terminology. Consequently, some papers are only partially relevant within the scope of a specific iteration. To address this, each iteration of the ETDP follows a chronological and thematic progression, incorporating full-text reviews of both newly selected and previously deferred papers. This is further supported by snowballing to ensure ongoing alignment with the taxonomy's evolving scope and objectives.

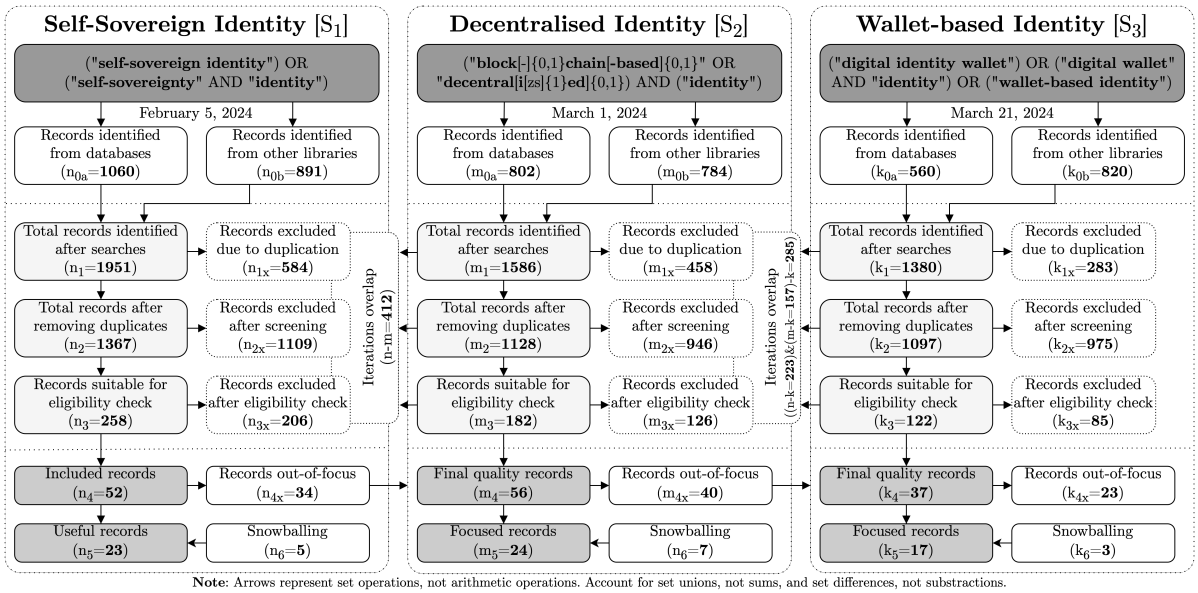

Figure 1. Extended PRISMA flowcharts for the systematic literature review process.

3.2 Solution Evaluation

In recent years, the user-centric IdM landscape has been replete with an overwhelming variety of components and full-stack solutions. To build and demonstrate our taxonomy across this diverse and evolving IdM solution landscape, we needed a well-founded yet manageable selection of representative solutions. We, therefore, thoroughly assessed the solution landscape and identified different solutions from multiple providers that claim to align with modern user-centric IdM paradigms and advertise to be self-sovereign, blockchain-based, or wallet-centric. These projects range from academic to commercial and open to closed source. We first collected solutions that are referenced at least three times in literature that focuses on conceptualising SSI (e.g., *Helix ID*, *Blockcerts*, *LifeID*, *SelfKey*, *Shocard*, *Sovrin*, *Spherity*, *Trinsic*, *IDchainZ*) (Ahmed et al., 2022; Dib & Rababah, 2020; Kubach & Sellung, 2021; Kuperberg & Klemens, 2022; Nokhbeh Zaeem et al., 2022). We then extended this list through structured web searches, prioritising solutions with visible traction, such as continued development or sustained visibility in media and technical communities. Because of the industry's ongoing evolution, some commonly covered solutions in literature were already outlived (e.g., *uPort*, *Secure ID* by *Civic*) or vanished (e.g., *AuthenteQ*, *Jolocom*, *FinID* by *Fincue*) at that time.

Based on this scoping, we selected 30 diverse candidates based on four indicative factors: (1) relevance across SSI, decentralised, and wallet-centric paradigms, (2) diversity in architectural and functional scope (partial vs. full-stack), (3) presence of publicly available documentation or interfaces enabling technical assessment, and (4) representativeness in terms of maturity, ecosystem role (e.g., issuer, wallet provider), and origin (public, private, open source, etc.). This resulted in the following evaluation set: *Altme* by *Talao*, *BlockID* by *1KOSMOS*, *EASSI* by *TMO*, *ESSIF*, *EUDIW*, *Entra Verified ID* by *Microsoft*, *Grimly ID*, *Hyperledger* (*Aries*, *Fabric*, *Indy*), *Iden3* by *0KIMS*, *Jolocom*, *Lissi* by *neosfer*, *LuxTrust*, *PingID* by *ShoCard*, *Pass* by *Civic*, *SelfKey*, *Sovrin*, *Sphereon*, *Spherity*, *SpruceID*, *Trinsic*, *VIDchain* by *Validated ID*, *VII* by *MATTR*, *Walt.id*, *WorldID*, *_SOWL* by *Esatus*, *cheqd*, and *uPort* and its successors *Serto* and *Verno*. Our preliminary assessment further highlighted the rapid evolution in the IdM landscape and the importance of thorough, empirical analyses to identify the most effective and viable layers, dimensions, and characteristics for evaluating the IdM solution's adherence to core SSI principles and identifying potential reasons for success or failure, calling for future research.

We followed a systematic process for the actual solution evaluation, beginning with the study of the assessed information and documentation. This helped us outline and conceptualise the respective system's architecture and functionalities. We then engaged directly with an instance of the solution through local deployment and/or functionality testing to verify the practical applicability of our findings from the processing empirical-to-conceptual iteration to ensure that all defined characteristics are theoretically sound and practically applicable. We started each deployment and functionality testing process by installing the mobile agent or wallet app when available. If an app was not available, we proceeded with command-line-based agent evaluation. Whenever possible, we locally set up a containerised setup (i.e., Docker) to create a controlled environment, or alternatively (i.e., closed-source), directly used the public service endpoints provided by the vendor. We also thoroughly reviewed any available technical documentation and repositories to understand the code, APIs, and system design.

We curated a heterogeneous selection of notable solutions for the final demonstration of our taxonomy and the evaluation process, reflecting different functionalities, maturity levels, and market relevance. Our selection showcases diverse solutions that illustrate our taxonomy's design, development, and usefulness. These solutions span different domains (public, private, academia) and major paradigms (e.g., SSI-focused and blockchain-focused narratives). We chose *uPort* as an early representative that was strongly influenced by early perceptions of blockchain as a foundation for SSI, *Trinsic* and *Walt.id* as two mature full-stack solutions with a focus on privacy and enterprise compatibility, respectively. These two solutions also reflect both the American and European perspectives. Finally, we included *WorldID* as a somewhat exotic contender and the *EUDIW* as the potential future of digital IdM in Europe in our evaluation. This diverse selection reflects not just the range of functionality and maturity among modern user-centric IdM solutions but also addresses the often narrow and outdated focus found in the existing literature. The details of this preliminary evaluation are subject to future work.

4 Taxonomy

This section presents the details of our holistic taxonomy for modern user-centric IdM, which spans across 6 layers, 22 dimensions and a wide range of theoretical and practical characteristics. We initiated the taxonomy design with principles from Allen (2016) and Sedlmeir et al. (2022) as meta-characteristics (Nickerson et al., 2013), which have been extended and refined along our iterations between SLR and solution evaluation (Kundisch et al., 2022). Following the ETDP, dimensions were iteratively derived through conceptual (deductive) reasoning and empirical (inductive) insights gathered from the literature and evaluation of existing IdM solutions. In turn, each layer captures a distinct abstraction level, allowing us to systematically group related dimensions, ranging from initial identity principles and architecture to governance and adoption factors. The process was guided by objective and subjective ending conditions to ensure comprehensiveness and practical relevance while avoiding redundancy. As many characteristics in our taxonomy can co-exist within a single dimension, we intentionally allow for non-mutually exclusive classifications to reflect the complex and multifaceted nature of real-world IdM systems. By distinguishing between theoretical constructs and practical implementations, our taxonomy addresses the dual nature of characteristics inherent of modern user-centric IdM. It integrates foundational elements, such as identity principles, architectural components, and technical specifications, with applied considerations, including legal, organisational, and governance requirements. This approach ensures that our taxonomy serves as a conceptual framework (theory) and guides system development (practice). Figure 2 features our final taxonomy.

The six layers of our final taxonomy are user wholeness, data autonomy, application usability, technology stack, architecture sharing, and system trust. Together, they offer a comprehensive structure to capture both conceptual foundations and practical design considerations in modern IdM systems. *User wholeness* focuses on maintaining the entirety of a user's digital identity (wholeness) (Pierucci & Cesaroni, 2023), ensuring the existence of a persistent identity representation. *Data autonomy* covers aspects that enable holders to control and verifiably disclose digital attestations in a privacy-preserving way without being controlled by an authority (autonomy) (Cameron, 2005; Pierucci & Cesaroni, 2023; Sovrin Foundation, 2022). *Application usability* (Sedlmeir et al., 2022) revolves around the user-facing domain-specific components and features that potentially boost the acceptance and diffusion of a solution driven by convenience and transparency. It is arguably one of the most important dimensions but also one of the most complex to achieve due to users' biased mental models and challenges in societal acceptance (Khayretdinova et al., 2022; Sartor et al., 2022). Our focus for the *technology stack* (Schmidt et al., 2021) lies in the technical elements that facilitate the functionality of IdM systems. This includes the cryptographic building blocks, protocols, and data structures that together form the technical stack that acts as the foundation of any SSI system (Yildiz et al., 2023). *Architecture sharing* further scrutinises the structural design of modern user-centric IdM systems, emphasising the distribution and collaboration of system components (architecture) that allow for interoperability (sharing) (Yildiz et al., 2023). Finally, the *system trust* includes rather intangible factors that enhance the overall trustworthiness of the system. Quantifying this dimension is challenging but indispensable for establishing the credibility and longevity of real-world solutions (Schwalm et al., 2022). In the following, we present the dimensions and characteristics associated with each layer.

4.1 User Wholeness

Representation (Sedlmeir et al., 2022) ensures that the system is inclusive, catering to a broad spectrum of entities (Kuperberg, 2020), such as humans (European Commission, 2023), organisations (i.e., legal entities) (European Commission, 2024a; Sedlmeir et al., 2022), technical (e.g., IoT devices) (Naik & Jenkins, 2022), and even animals (e.g. *Althash Breeders*), thereby accommodating the diverse needs of digital interactions and the capacity to handle complex and varied identity attributes seamlessly.

Existence (Allen, 2016) emphasises the necessity for entities to have a unique, verifiable presence that transcends mere digital constructs (Ernstberger et al., 2023). It covers system capabilities for identity federation (Kuperberg, 2020) or to provide identifiers with different privacy properties (e.g., decentralised (DID) (Shuaib et al., 2021), self-issued (OIDC Workgroup, 2023), pairwise

pseudonymous (Shuaib et al., 2021), and single-use (Lesavre et al., 2020)) identifiers and long-lived user-controlled electronic attestations of attributes (European Commission, 2024a). Attestations are often called verifiable credentials (OIDC Consortium, 2022; Sedlmeir et al., 2021) and can refer to any identity attribute, identifier, or credential (Pfitzmann & Hansen, 2010).

Persistence (Allen, 2016) asserts that identities should be (relatively) long-lived (i.e., valid) and independent of the issuer (i.e., issued before and independently of its usage). Identity validity can be verified through revocation registries (active) and attestation timestamping (passive). This includes time revocation (e.g., expiration) (Shuaib et al., 2021) as the generic timestamping of attestations (i.e., *not valid before*, *not valid after*), use-based invalidation (i.e. single-use credential) and remote services (Kuperberg, 2020; Shuaib et al., 2021): Revocation lists (e.g., CRL) return all invalid attestations in bulk, while status lists (e.g., OCSP) reveal a specific attestation's state but risk user profiling. Revocation brokers, while convenient, centralise the task of revocation check mediation and thus may infringe privacy (EBSI, 2023). Non-revocation proofs and cryptographic accumulators protect privacy, but implementations face scalability and complexity issues (Babel & Sedlmeir, 2023).

Protection (Allen, 2016) considers mechanisms that give users a certain degree of control (Devon Loffreto, 2012) over their data and the system. This is closely related to legal compliance requirements for data processors (e.g., the GDPR and eIDAS regulations in the EU) and liability requirements (Pattiyanon & Aoki, 2023). In particular, mechanisms that provide the user with capabilities for data rectification, data erasure (Sim et al., 2019), and consent withdrawal (Schwalm et al., 2022; Tosoni, 2020) may be required. Furthermore, protection requires the assurance that there are no (public) transaction logs that reveal identity usage on an (immutable) ledger. The degree of protection further depends on where the data is stored (distribution) and who controls the data (i.e. (de-) centralised vs. federated authority) (Mohammed et al., 2020).

4.2 Data Autonomy

Control (Allen, 2016; Lesavre et al., 2020; Sedlmeir et al., 2022) captures the essence of sovereign authority (Devon Loffreto, 2012): Users can be their own identity custodians without dependency on external brokers (European Commission, 2024a; Naik & Jenkins, 2020b; Schwalm et al., 2022). The user should have control of their private keys and attestations (Naik et al., 2021). This may be realised by using a wallet and secure element on an edge device or remotely in the cloud using a trusted execution environment (TEE). Users should have full control over their cryptographic keys (i.e., private and public keys) (Babel & Sedlmeir, 2023). Some systems may also allow the sharing of control by assigning trustees (e.g., guardianship) and providing remote wipe functionalities in case of a breach.

Minimisation (Allen, 2016) advocates disclosing only the information necessary for a specific interaction. This underlines the importance of Privacy Enhancing Technologies (PETs) such as selective disclosure, range proofs, further predicate proofs, and general-purpose zero-knowledge proofs (ZKPs) (Babel & Sedlmeir, 2023; Kuperberg, 2020; Lesavre et al., 2020). While selective disclosure should be the baseline (Tosoni, 2020), additional minimisation techniques are appropriate.

Authenticity (Sedlmeir et al., 2022) emphasises the fundamental requirement for identity verification processes of ensuring the secure link to their rightful identity holder and the legitimacy of identity claims. Authenticity can be assured through identification by binding identity to a device or user (Babel & Sedlmeir, 2023; Bastian et al., 2023) and can be further strengthened through wallet authentication (Bastian et al., 2023) and strong multi-factor authentication (MFA) (Kuperberg, 2020). In addition to the previous measures, an immutable ledger listing relying parties (Sim et al., 2019) or legally governed certification schemes can help increase security in wallet-related data processing (Bastian et al., 2023).

Verifiability (Sedlmeir et al., 2022) represents the foundation for establishing trust between entities, ensuring that all parties can confidently rely on the integrity, authenticity and validity of presented information. This encompasses mechanisms like revocation checks (i.e., validity), attestation timestamping (i.e., expiration), attestation schemas (i.e., format), and digital signatures (i.e., integrity and authenticity) (Babel & Sedlmeir, 2023). These mechanisms either work locally using cryptographic metadata (Naik et al., 2021) or remotely through querying trusted registries for metadata.

4.3 Application Usability

Experience emphasises the user interface and experience (UI/X), aiming to streamline and enhance user acceptance and engagement (Khayretdinova et al., 2022). The identity system should provide free basic identity services (e.g., issuance, update, deletion) (Naik & Jenkins, 2020a) but may charge for advanced services (e.g., qualified signatures). The user should not be bound to a specific platform (e.g., software or hardware). Further mechanisms that may improve usability through convenience are self-registration, single-sign-on (SSO), and customer support (Kuperberg, 2020).

Consent emphasises the importance of user engagement in providing permissions for using digital identity data (Naik & Jenkins, 2020a). This includes displaying the requested data to the user and requiring explicit consent for its transfer (Shuaib et al., 2021). Furthermore, authorisation and authentication protocols ensure consent for only deliberately initiating any purposeful action. Finally, consent management interfaces provide the user with an overview of provided consent (e.g., sessions) and integrated features to enforce mechanisms for *protection* and ensure *transparency*.

Access (Allen, 2016) ensures that users can effortlessly retrieve, manage, and interact with their digital identities and associated data. Digital identity wallets are the core component for managing identities in a local and controlled environment (European Commission, 2024a). Naming systems (e.g., DID, PKI) provide information describing public identifiers for stakeholders (e.g., users, issuers, verifiers). Transparency logs (e.g., wallet-based) can offer an auditable trail of interactions only visible to the identity holder. Processor data inspection further empowers data subjects, allowing them to review and understand how the relying party processes their data (Kuperberg, 2020).

Recovery mechanisms (Khayretdinova et al., 2022) allow the regaining of access to digital identities after loss of control. Recovery is essential to mitigate the impact of human errors and ensure that systems remain usable. Different mechanisms exist to restore identity data, including exporting to and importing from local storage and cloud-based backups. The latter is more user-friendly but poses a critical risk if the revocation endpoint is vulnerable, highlighting the security-convenience trade-off. Seed phrases or mnemonics in decentralised key management systems (DKMS) allow users to recover their digital identity without relying on third parties. Systems that (partially) manage data or backups for the user may provide control-recovery mechanisms (e.g., *forgot password*) (Yildiz et al., 2023).

4.4 Technology Stack

The system *layers* are based on the SSI reference model by Yildiz et al. (2023), which is similar to the Trust over IP (ToIP) stack (Davie et al., 2019). The technical trust layer (i.e., anchor) covers components to form trust between stakeholders. The agent layer (i.e., communication, storage, recovery) comprises components for secure communication between actors, such as transport security, cryptographic key management, data portability, and control recovery. The credential layer provides means to issue, store, and present attestations in a verifiable way, including revocation, attestation exchange, binding, format, and proof generation. The application layer covers the domain-specific components (e.g., apps, semantics, and verticals). Finally, cross-layer considerations cover, among others, compliance, privacy, authentication, authorisation, storage, and format that are not exclusive to any layer or system.

The list of system *components* is similar to system *layers* but stretches vertically through the system architecture rather than horizontally. Hence, it covers key software components provided to and by different stakeholders, such as agents in the form of mobile apps or command-line, wallets (local, edge, or cloud), as well as issuance, verification, and trust anchor components (Schmidt et al., 2021). This provides a clear view of the system's operational dynamics and interdependencies. In this context, interoperable systems can share or exchange components.

Decentralisation mechanisms define the shift from centralised authority towards distributed trust anchors and registries (Sim et al., 2019). This covers DLTs such as blockchain, distributed filesystems (DFSs), and distributed hash tables (DHT) for a resilient and transparent trust infrastructure (Čučko & Turkanović, 2021). Yet, not all IdM systems use DLT; they may also fully or partially rely on public key infrastructures (PKI), centralised web services, or be fully self-contained (Hoops et al., 2023).

Participation explores the extent to which entities can engage with and contribute to the trust infrastructure (Kuperberg, 2020). Trust infrastructures may be public permissionless, public permissioned, and private permissioned (Schmidt et al., 2021). While this classification is commonly applied to DLT solutions (Beck et al., 2018), it can be transferred to other types of registries. In this sense, a centralised web service may be public permissioned by exposing an API endpoint for reading data (e.g., certificate transparency logs) while only the central authority has write access or is completely hidden from the user (e.g., only revocation brokers get read access), and, therefore, private permissioned.

4.5 Architecture Sharing

Functionality describes operational capabilities and the range of actions a system can perform or has been designed for. It encompasses essential identity services such as identification, authentication, and authorisation. Beyond these foundational services, it extends to the attestation of identity data to the holder and its subsequent verification by the verifier. Additionally, it addresses specialised applications such as verifiable data storage and data exchange, along with the generation of (qualified) electronic signatures for documents (Kubach & Sellung, 2021; Schmidt et al., 2021).

Interoperability (Allen, 2016) emphasises the capacity of systems to (inter)operate across platforms and ecosystems (Grüner et al., 2021; Sovrin Foundation, 2022). It highlights the role of common protocols and data formats through which identities are portable across different systems (Lesavre et al., 2020). *Technical* interoperability requires machines to communicate using common protocols (e.g., OpenID4VCI, SIOP) and infrastructures. *Syntactical* interoperability requires common data formats (e.g., SD-JWT and mDOC). *Semantic* interoperability requires a shared understanding of exchanged information (e.g., ISO/IEC 18013-5) between sender and receiver. *Organisational* interoperability requires data to be exchangeable between diverse systems (Yildiz et al., 2023).

Portability (Allen, 2016; Kubach et al., 2020) allows for the flexible use of identity data that is not bound to a single platform or service. This ensures users can maintain control over their identity across systems through user-agent and wallet agnosticism, adherence to open standards and specifications, or support for universal wallets (e.g., W3C) (Grüner et al., 2021; Yildiz et al., 2023). Differential credentialing describes an approach where attestations with a low level of assurance (LoA) may be portable. This is impossible for attestations with LoA high (e.g., eID). Application and service provider interfaces (API/SPI) facilitate the migration and interoperability of identities (Kuperberg, 2020).

4.6 System Trust

Transparency (Allen, 2016; Kubach et al., 2020) addresses means for openness towards mechanisms and processes. This can be accomplished through open-sourcing employed code (Pattiyanon & Aoki, 2023). Open governance ensures decision-making processes are inclusive and accountable. Community engagement allows externals to influence the system's evolution. Comprehensive documentation and clear process notices can provide insights into operational procedures, while audit trails ensure actions within the system are traceable and accountable. Finally, establishing a clear trust hierarchy can facilitate more transparency and trust (Kuperberg, 2020).

Reliability (Sedlmeir et al., 2022) describes different types of (decentralised/distributed) trust anchors (Podgorelec et al., 2022). These include public institution registries (i.e., trustworthy issuers and verifiers), trusted schemas registries (i.e., semantics), status registries (i.e., validity checks), DID registries (i.e., public identity lookups), identifier-attribute registries (i.e., locations for off-chain storage), and blockchain anchors (i.e., on-chain hash-based evidence) (Čučko et al., 2023).

Finally, *security and privacy* (Sedlmeir et al., 2022) are usually intangible yet come at the cost of convenience and usability. Most characteristics presented in this section so far contribute to security and privacy. This final layer adds characteristics required for secure system basis, such as transport security (e.g., TLS), end-to-end encryption, post-quantum safety, and secure hardware to be future-proof (Babel & Sedlmeir, 2023; Naik et al., 2021). The employment of PETs (e.g., ZKPs) should provide the highest level of unlinkability. Certifications (e.g., EUDIW certified wallet) and independently verified (e.g., by the BSI or NIST) compliance can further increase trust (Ernstberger et al., 2023; Kubach et al., 2020).

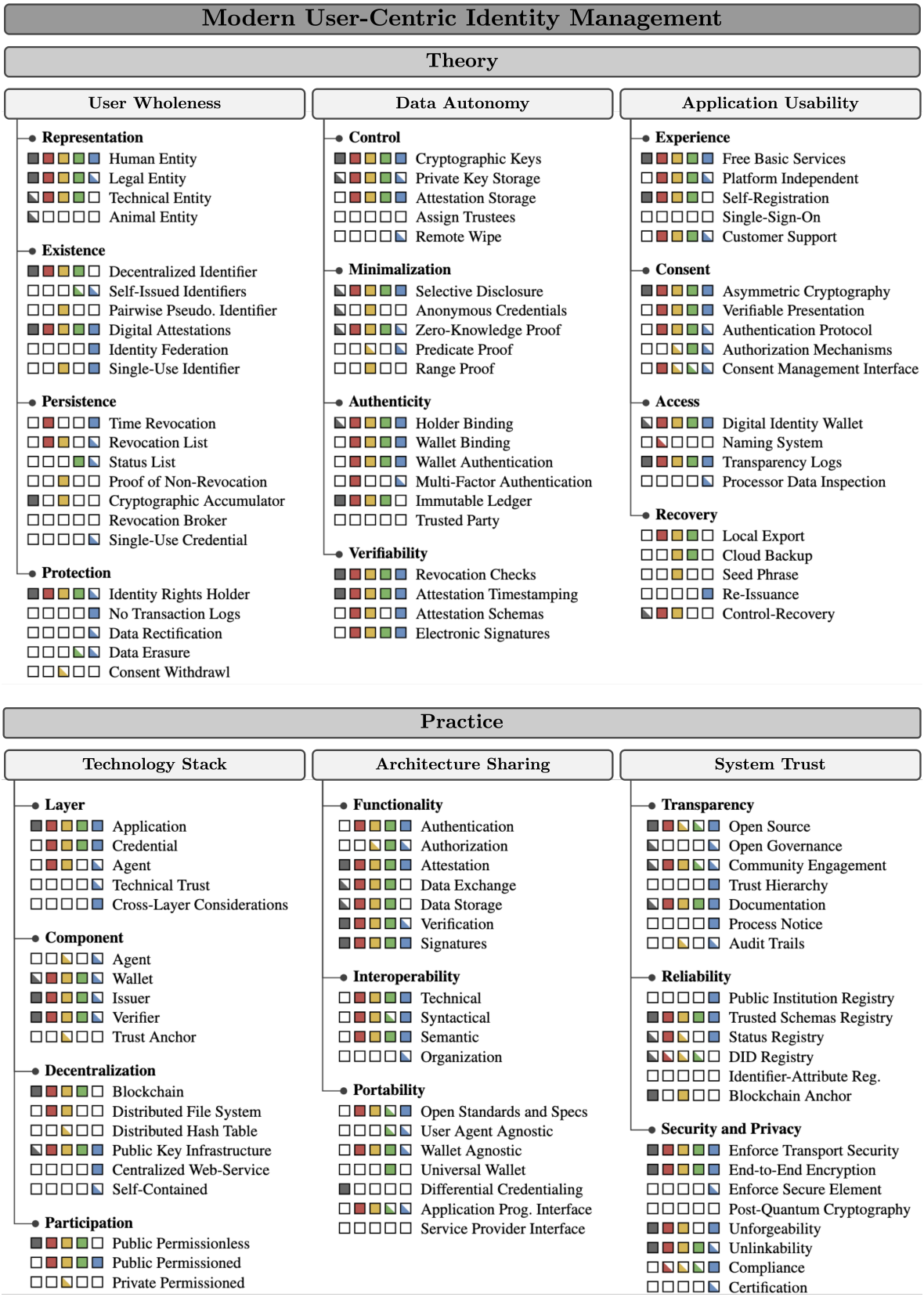

Figure 2. Taxonomy to evaluate full-■, conditional-◪, or non-adherence □ to core principles of user-centric identity management, exemplified using uPort ■, Walt.id ■, Trinsic ■, WorldID ■ and the European Digital Identity Wallet (EUDIW) ■.

5 Demonstration

Our developed taxonomy, featured in Figure 2, provides a structured framework to assess modern user-centric IdM solutions combined with some illustrative evaluation results. As such, it allows us to evaluate the degree of adherence to these principles layer-wise. We distinguish between full, conditional, and non-adherence. We have applied this final taxonomy to a set of five solutions for demonstration, revealing varying degrees of adherence to diverse sets of characteristics. Each solution provided valuable insights into implementing user-centric principles' practical challenges and successes, which helped us continuously refine our taxonomy. We chose *uPort*, *Trinsic*, *Walt.id*, *WorldID*, and the *EUDIW* as candidates in the final iteration to demonstrate the diversity within the IdM landscape, encompassing a mix of early and mature solutions that stretch between the discussed definitions of modern user-centric IdM, thus showcasing the flexibility and applicability of our taxonomy.

After evaluating the original uPort solution using our taxonomy, it appears that while uPort was once an innovative and prominent solution in the early decentralised IdM landscape, it exhibits a substantial set of drawbacks. Specifically, uPort lacks *interoperability* and *portability*, as it is strongly bound to the Ethereum blockchain with reliance on, e.g., the non-standardized Ethr-DID protocol. *Control* is also a concern, as the solution lacks user-controlled key storage, which conflicts with the principle of user autonomy. This resonates with the lack of support for *data minimisation*, as uPort does not support PETs. Yet, selective disclosure is partially supported in Varamo. The system's approach to *revocation* via smart contracts and to *recovery* via delegation to trusted entities (i.e., family and friends) is also unusual. These methods further raise concerns about governance, ownership, and disclosure control, as well as the risk of identity manipulation or *blocklisting* (i.e., loss of availability), undermining user trust.

As we navigate the evolution of IdM, the EUDIW serves as a relevant case (Giannopoulou, 2023) that marks the future of digital identity for European citizens "*to have a secure, authentic and verifiable digital identity with a user-centric approach and full protection of citizens' personal data*" (POTENTIAL Consortium, 2023). The EUDIW has reached an important milestone at the time of this writing. The legislative revisited eIDAS (2.0) regulation (EU/2024/1183) has been published recently (European Parliament and Council, 2024), the technical architecture reference framework (ARF) (v1.4) has been released (European Commission, 2024c), and an initial demonstration for the EUDIW reference implementation (RI) has been published (European Commission, 2024b). The EUDIW is on the way to its full adoption in 2026 when several important public and private services have to accept the EUDIW, and wallets must be available in all member states (European Commission, 2024d).

At this point, it should be reiterated that the EUDIW is not yet in production. Our evaluation reflects this milestone state of the EUDIW. It features some conditional adherence due to uncertainty on the realisation of some features or potential later changes in the ARF or RI. As the certification of a self-implemented or third-party wallet is left to member states, a diverse landscape of wallet solutions can be expected (Degen and Teubner, 2024). However, several open questions remain. For instance, revocation and status lists are not yet fully deployed due to uncertainties about the trust infrastructure. Thus far, it also remains unclear how to achieve a high level of assurance (LoA) in the fragmented landscape of secure elements (SE), smart cards (SC), or (remote) hardware security modules (HSMs).

Moreover, while both standards for electronic attestations provide selective disclosure, how to achieve unlinkability has not been specified, as corresponding ZKPs are not sufficiently standardised (Fernández, 2024). Lastly, no *recovery* mechanism has been implemented besides *re-issuance*. The recovery mechanism, if any, must be selected with the highest risk evaluation. Overall, our evaluation of the EUDIW underlines a strong focus on user control and system trust while recognising the system's pragmatic approach to combining user-centric principles with the requirements of national identity management within a regulated, federated structure without any decentralised trust anchor and somewhat centralised authority. Transparency and interoperability between member states are especially important. Centralised services substitute complex security and privacy-related questions under the state authority as trust anchors.

6 Discussion

The IdM landscape is complex and constantly evolving, particularly with the rise of solutions following the self-sovereign, blockchain-based, and wallet-based paradigms. We show they share common values that emphasise user-centricity, and many solutions are converging towards digital wallets for identity storage and transactions. This convergence is not merely semantic; our taxonomy highlights the overlapping characteristics, suggesting a direction in the *modern user-centric* digital identity evolution. It highlights a practical realisation of IdM principles supporting and transcending theoretical constructs.

We exemplify this observation based on the evaluation of the EUDIW. The EUDIW is described in eIDAS as "*a trusted, voluntary, user-controlled digital identity that is recognised throughout the Union and allows every user to control their data in online interactions*". The EUDIW does not claim to comply with the SSI principles nor foresee the use of DLT. Instead, the EC focuses on the features of a wallet for the EUDIW for this rather special example evolving around citizens' legal identity, which has stronger implications on security and privacy, but arguably also the necessity for a central (trust-worthy) authority for government and identity federation and as the authentic source. Nevertheless, the EUDIW demonstrates alignment with characteristics of modern user-centric IdM, particularly regarding the *trust* and *control* layers. However, it rather operates a federated model between MS as an identity provider and trust anchors, adapting to the demands of secure and usable *verified legal* identities within the EU.

Our final taxonomy still entails some complexities. For instance, it does not contain any mutually exclusive characteristics. This is due to the nature of complex IdM systems, where we could almost always identify circumstances where either exception (especially considering sub-systems) could be found or characteristics were too narrow or relative (e.g., adherence). Instead, we focused on components that could be freely combined. Mutual exclusiveness still applies, but inter-dimension, as, e.g., solutions that do not rely on ZKP for data minimisation, cannot provide proof of non-revocation. We further introduced the degrees of adherence that include a conditional state highlighting scenarios in which strong statements cannot be made, e.g., if the solution uses ZKPs in a single specific scenario (e.g., a range proof for age), it would be too strong of a statement to claim full- or non-adherence.

There are also several socio-technical challenges and gaps for modern IdM solutions (Giannopoulou, 2023). Privacy- and verifiability-enhancing technologies are a central part of the user-centric model but are often either not mature enough or not widely adopted (Sedlmeir et al., 2021). Recovery is vital in user-friendly models that account for human error and nature but often represents a risk to user wholeness if any vulnerability arises (Pierucci & Cesaroni, 2023). Similarly, hardware components for protecting cryptographic keys present unique challenges, as diversity can lead to inconsistencies and make the system vulnerable (Bastian et al., 2023). Thus, performing operations securely in cloud-based HSMs may be crucial in aligning security and convenience. Interoperability and portability are paramount for widespread adoption (Schmidt et al., 2021). Regulations and policies affect standardisation and adoption, and there is a need for technical standards (Yildiz et al., 2023).

While our taxonomy is grounded in iterative literature analysis and solution evaluation, some limitations remain. Although the taxonomy fulfils the objective and subjective ending conditions proposed by Nickerson et al. (2013), further empirical grounding through structured interviews and broader application will enhance its validation. In line with Kundisch et al. (2022), future work will extend the evaluation across a broader range of identity management solutions and engage in more diverse stakeholder perspectives and trade-offs to improve generalisability, relevance, and theoretical depth.

7 Conclusion

In this paper, we analysed the principles and characteristics of modern user-centric IdM systems and present a multi-layered taxonomy covering the dimensions of *user wholeness*, *data autonomy*, *application usability*, *technology stacks*, *architecture sharing*, and *system trust*. We ground our research on theoretical principles moving towards practical solutions and real-world implementations, accounting for the economic and legal impact. We showcase our taxonomy's utility by evaluating solutions' adherence to principles and identifying areas for improvement.

Our taxonomy provides a practical and extendable framework for navigating the complex and evolving landscape of modern user-centric identity management. Bridging theoretical principles with real-world implementations enables researchers and practitioners to systematically evaluate and compare IdM solutions based on their adherence to characteristics of modern user-centric IdM systems. Importantly, the taxonomy allows looking beyond abstract principles or specific paradigms like self-sovereign, decentralised, or wallet-based identities. As the digital identity ecosystem continues to diversify, this taxonomy offers a common language and structured lens for assessing existing and designing new systems and aligning technological choices with broader requirements of information systems.

Acknowledgements

This work was funded by Luxembourg's National Research Fund (FNR) and PayPal (PEARL grant ref. 13342933/Gilbert Fridgen, and PABLO grant ref. 1632675), and supported by Luxembourg's Ministry for Digitalisation. For open access purposes, the authors have applied a CC BY 4.0 license to any Author Accepted Manuscript arising from this submission.

References

Abbas, R., & Munoz, A. (2021). Designing antifragile social-technical information systems in an era of big data. *Information Technology & People*, 34(6). https://doi.org/10.1108/itp-09-2020-0673

M. R. Ahmed, A. K. M. M. Islam, S. Shatabda and S. Islam, "Blockchain-Based Identity Management System and Self-Sovereign Identity Ecosystem: A Comprehensive Survey," in IEEE Access, vol. 10, pp. 113436-113481, 2022, doi: 10.1109/ACCESS.2022.3216643.

Allen, C. (2016). *The Path to Self-Sovereign Identity*. Retrieved June 27, 2023 from https://github.com/WebOfTrustInfo/self-sovereign-identity

Babel, M., & Sedlmeir, J. (2023). *Bringing data minimization to digital wallets at scale with general-purpose zero-knowledge proofs*. https://arxiv.org/abs/2301.00823

Bastian, P., Kraus, M., & Fischer, J. (2023). Concepts for Secure Wallets in Decentralized Identity Ecosystems. *HMD Praxis der Wirtschaftsinformatik*. doi.org/10.1365/s40702-023-00954-4

Beck, R., Müller-Bloch, C., & King, J. L. (2018). Governance in the Blockchain Economy: A Framework and Research Agenda. *Journal of the Association for Information System*s, 19(10).

Bochnia, R., Richter, D., & Anke, J. (2024). Self-Sovereign Identity for Organizations: Requirements for Enterprise Software. *IEEE Access*. https://doi.org/10.1109/ACCESS.2023.3349095

Cameron, K. (2005). *Laws of Identity*. Retrieved Aug. 30, 2023 from https:// identityblog.com/?p=353

Čučko, Š., Keršič, V., & Turkanović, M. (2023). Towards a Catalogue of Self-Sovereign Identity Design Patterns. *Applied Sciences*, 13(9), 5395. https://doi.org/10.3390/app13095395

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

Davie, M., Gisolfi, D., Hardman, D., Jordan, J., O'Donnell, D., & Reed, D. (2019). The trust over ip stack. *IEEE Communications Standards*. https://doi.org/10.1109/MCOMSTD.001.1900029

Degen, K., & Teubner, T. (2024). Wallet wars or digital public infrastructure? Orchestrating a digital identity data ecosystem from a government perspective. *Electronic Markets*, *34*(1). https://doi.org/10.1007/s12525-024-00731-1

Devon Loffreto. (2012). *What is 'Sovereign Source Authority'?* Retrieved March 13, 2024 from https://www.moxytongue.com/2012/02/what-is-sovereign-source-authority.html

Dib, O., & Rababah, B. (2020). Decentralized identity systems: Architecture, challenges, solutions and future directions. *Annals of Emerging Technologies in Computing (AETiC)*, *4*(5), 19-40. https://doi.org/10.33166/AETiC.2020.05.002

EBSI. (2023). *EBSI's Credential Status Framework and how to choose a revocation method when using W3C Verifiable Credentials*. Retrieved Oct. 10, 2023 from https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/What+to+do+when+good+Verifiable+Credentials+go+bad

Ernstberger, J., Lauinger, J., Elsheimy, F., Zhou, L., Steinhorst, S., Canetti, R., Miller, A., Gervais, A., & Song, D. (2023). *SoK: Data Sovereignty*. https://doi.org/10.1109/EuroSP57164.2023.00017

European Commission. (2020). *Digital Identity for all Europeans*. Retrieved August 24, 2023, from https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en

European Commission. (2023). *EU Digital Identity Wallet Toolbox Process*. Retrieved March 15, 2024 from https://digital-strategy.ec.europa.eu/en/policies/eudi-wallet-toolbox

European Parliament and Council. (2024) Regulation (EU) 2024/1183 of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework *Official Journal of the European Union*. https://eur-lex.europa.eu/eli/reg/2024/1183/oj

European Commission. (2024a). *EU Digital Identity Wallet (EUDIW)*. Retrieved March 27, 2024 from https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/

European Commission. (2024b). *EUDIW Reference Implementation*. Retrieved March 14, 2024 from https://github.com/eu-digital-identity-wallet/profile/reference-implementation.md

European Commission. (2024c). *EUDIW Architecture Reference Model (ARF)* (Version 1.4). Retrieved May 14, 2024 from https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/arf.md

European Commission. (2024d). *EU Digital Identity Wallet Home*. Retrieved 25 June, 2024 from https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET

Fernández, R. R. (2024). Evaluation of trust service and software product regimes for zero-knowledge proof development under eIDAS 2.0. *Computer Law & Security Review*, 53, 105968. https://doi.org/10.1016/j.clsr.2024.105968

Giannopoulou, A. (2023). Digital identity infrastructures: a critical approach of self-sovereign identity. *Digital Society*, *2*(2), 18. https://doi.org/10.1007/s44206-023-00049-z

Grüner, A., Mühle, A., & Meinel, C. (2021). Analyzing Interoperability and Portability Concepts for Self-Sovereign Identity. *IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications*. https://doi.org/10.1109/TrustCom53373.2021.00089

Hoess, A., Roth, T., Sedlmeir, J., Fridgen, G., & Rieger, A. (2022). With or without Blockchain? Towards a decentralized, SSI-based eRoaming architecture. *In 55th Hawaii International Conference on System Sciences (HICSS)*. https://doi.org/10.24251/hicss.2022.562

Hoops, F., Mühle, A., Matthes, F., & Meinel, C. (2023). A Taxonomy of Decentralized Identifier Methods for Practitioners. *2023 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS)*, 57–65. https://doi.org/10.1109/DAPPS57946.2023.00017

Jones, Z. (2024). *Reusable Identity Product Market Map*. Trinsic. Retrieved March 17, 2024 from https://trinsic.id/reusable-identity-product-market-map/

Khayretdinova, A., Kubach, M., Sellung, R., & Roßnagel, H. (2022). Conducting a Usability Evaluation of Decentralized Identity Management Solutions. *Selbstbestimmung, Privatheit und Datenschutz: Gestaltungsoptionen für einen europäischen Weg*.

Kubach, M., Schunck, C. H., Sellung, R., & Roßnagel, H. (2020). Self-sovereign and Decentralized identity as the future of identity management? https://dl.gi.de/handle/20.500.12116/33180

Kubach, M., & Sellung, R. (2021). On the Market for Self-Sovereign Identity: Structure and Stakeholders. *Open Identity Summit 2021*. https://dl.gi.de/handle/20.500.12116/36488

Kundisch, D., Muntermann, J., Oberländer, A. M., Rau, D., Röglinger, M., Schoormann, T., & Szopinski, D. (2022). An Update for Taxonomy Designers: Methodological Guidance from Information Systems Research. *Business & Information Systems Engineering*, 64(4).

Kuperberg, M. (2020). Blockchain-Based Identity Management: A Survey From the Enterprise and Ecosystem Perspective. *IEEE Transactions on Engineering Management*, 67(4).

Kuperberg, M., & Klemens, R. (2022). Integration of Self-Sovereign Identity into Conventional Software using Established IAM Protocols. https://dl.gi.de/handle/20.500.12116/38704

Lesavre, L., Varin, P., Mell, P., Davidson, M., & Shook, J. (2020). A Taxonomic Approach to Understanding Emerging Blockchain Identity Management. https://arxiv.org/pdf/1908.00929

Mohammed, A. B., Lu, Q., Zhang, F., Wan, Y., Zhang, T., & Ning, H. (2020). Distributed Ledger Technology for eHealth Identity Privacy: State of The Art and Future Perspective. *Sensors*.

Moher, D., Liberati, A., Tetzlaff, J., Altman, D. G., & Prisma Group. (2010). Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. *International journal of surgery*, *8*(5), 336-341. https://doi.org/10.1136/bmj.b2535

Naik, N., Grace, P., & Jenkins, P. (2021). An Attack Tree Based Risk Analysis Method for Investigating Attacks and Facilitating Their Mitigations in Self-Sovereign Identity. *IEEE Symposium Series on Computational Intelligence*. https://doi.org/10.1109/SSCI50451.2021.9659929

Naik, N., & Jenkins, P. (2020a). Governing Principles of Self-Sovereign Identity Applied to Blockchain Enabled Privacy Preserving Identity Management Systems. *2020 IEEE International Symposium on Systems Engineering (ISSE)*. https://doi.org/10.1109/ISSE49799.2020.9272212

Naik, N., & Jenkins, P. (2020b). Your Identity is Yours: Take Back Control of Your Identity Using GDPR Compatible Self-Sovereign Identity. *2020 7th International Conference on Behavioural and Social Computing (BESC)*. https://doi.org/10.1109/BESC51023.2020.9348298

Naik, N., & Jenkins, P. (2022). Is Self-Sovereign Identity Really Sovereign? 2022 IEEE International Symposium on Systems Engineering. https://doi.org/10.1109/ISSE54508.2022.10005404

Nickerson, R. C., Varshney, U., & Muntermann, J. (2013). A method for taxonomy development and its application in information systems. *European Journal of Information Systems*, *22*(3), 336-359. https://doi.org/10.1057/ejis.2012.26

Nokhbeh Zaeem, R., Chang, K. C., Huang, T.-C., Liau, D., Song, W., Tyagi, A., Khalil, M., Lamison, M., Pandey, S., & Barber, K. S. (2022). Blockchain-Based Self-Sovereign Identity: Survey, Requirements, Use-Cases, and Comparative Study. *International Conference on Web Intelligence and Intelligent Agent Technology*. https://doi.org/10.1145/3486622.3493917

OIDC Consortium. (2022). *Verifiable Credentials Data Model*. Retrieved February 3, 2024 from https://www.w3.org/TR/vc-data-model/

OIDC Workgroup. (2023). *Self-Issued OpenID Provider v2*. Retrieved February 3, 2024 from https://openid.net/specs/openid-connect-self-issued-v2-1_0.html

Pattiyanon, C., & Aoki, T. (2023). Analysis and Enhancement of Self-sovereign Identity System Properties Compiling Standards and Regulations. *ICISSP '22. 8th International Conference on Information Systems Security and Privacy*. https://doi.org/10.5220/0010877300003120

Pfitzmann, A., & Hansen, M. (2010). *A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management*. Retrieved Nov. 11, 2024 from dud.inf.tu-dresden.de/Anon_Terminology.shtml

Pierucci, F., & Cesaroni, V. (2023). Data Subjectivation—Self-sovereign Identity and Digital Self-Determination. *Digital Society*, 2(2). https://doi.org/10.1007/s44206-023-00048-0

Podgorelec, B., Alber, L., & Zefferer, T. (2022, June). What is a (digital) identity wallet? a systematic literature review. In *2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC)* (pp. 809-818). IEEE. https://doi.org/10.1109/COMPSAC54236.2022.00131

POTENTIAL Consortium. (2023). *Potential — For European Digital Identity*. Retrieved March 27, 2024 from https://www.digital-identity-wallet.eu/

Rieger, A., Roth, T., Sedlmeir, J., Fridgen, G., & Young, A. (2024). Organizational Identity Management Policies. *JAIS*, 25(3), 522-527. https://doi.org/10.17705/1jais.00887

Sartor, S., Sedlmeir, J., Rieger, A., & Roth, T. (2022). Love at First Sight? A User Experience Study of Self-Sovereign Identity Wallets. ECIS 2022. https://aisel.aisnet.org/ecis2022_rp/46

Schmidt, K., Mühle, A., Grüner, A., & Meinel, C. (2021). Clear the fog: Towards a taxonomy of self-sovereign identity ecosystem members. In *2021 18th International Conference on Privacy, Security and Trust (PST)*. 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 2022* (pp. 63-74).

Sedlmeir, J., Huber, J., Barbereau, T. 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 (ICIS)*. Copenhagen. https://hdl.handle.net/10993/52350

Sedlmeir, J., Smethurst, R., Rieger, A., & Fridgen, G. (2021). Digital identities and verifiable credentials. *Business & Information Systems Engineering*, *63*(5), 603-613.

Sheik, A. T., Maple, C., Epiphaniou, G., & Atmaca, U. I. (2021). A Comparative Study of Cyber Threats on Evolving Digital Identity Systems. CADE 2021. https://doi.org/10.1049/icp.2021.2428

Shuaib, M., Daud, S. M., & Alam, S. (2021). Self-sovereign Identity framework development in compliance with Self sovereign Identity principles using components. *IJMA*, 10(2).

Sim, W. L., Chua, H. N., & Tahir, M. (2019). Blockchain for Identity Management: The Implications to Personal Data Protection. *IEEE Conference: Application, Information and Network Security*.

Smethurst, R. (2023). Digital identity wallets and their semantic contradictions. In *Thirty-first European Conference on Information Systems (ECIS)*. https://aisel.aisnet.org/ecis2023_rp/288

Sovrin Foundation. (2022). *Principles of SSI*. Retrieved Oct. 23, 2024 from sovrin.org/principles-of-ssi

Tosoni, L. (2020). Article 5. Principles relating to processing of personal data. In C. Kuner, L. A. Bygrave, C. Docksey, & L. Drechsler, The EU General Data Protection Regulation (GDPR).

Webster, J., & Watson, R. T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MIS Quarterly*, 26(2). https://www.jstor.org/stable/4132319

Weigl, L., Barbereau, T., & Fridgen, G. (2023). The construction of self-sovereign identity: Extending the interpretive flexibility of technology towards institutions. *Government Information Quarterly*, *40*(4), 101873. https://doi.org/10.1016/j.giq.2023.101873

Wilson, Y., & Hingnikar, A. (2019). Solving Identity Management in Modern Applications: Demystifying OAuth 2.0, OpenID Connect, and SAML 2.0. *Apress*.

Yildiz, H., Küpper, A., Thatmann, D., Göndör, S., & Herbke, P. (2023). Toward Interoperable Self-Sovereign Identities. *IEEE Access*, 11. https://doi.org/10.1109/ACCESS.2023.3313723