The Review of Non-Technical Assumptions in Digital Identity Architectures

Anar Bazarhanova
Department of Computer Science
Aalto University
anar.bazarhanova@aalto.fi

Kari Smolander
School of Engineering Science
LUT University
kari.smolander@lut.fi

Abstract

The literature on digital identity management systems (IdM) is abundant and solutions vary by technology components and non-technical requirements. In the long run, however, there is a need for exchanging identities across domains or even borders, which requires interoperable solutions and flexible architectures. This article aims to give an overview of the current research on digital identity management. We conduct a systematic literature review of digital identity solution architectures and extract their inherent non-technical assumptions. The findings show that solution designs can be based on organizational, business and trust assumptions as well as human-user assumptions. Namely, establishing the trust relationships and collaborations among participating organizations; human-users capability for maintaining private cryptographic material or the assumptions that win-win business models could be easily identified. By reviewing the key findings of solutions proposed and looking at the differences and commonalities of their technical, organizational and social requirements, we discuss their potential real-life inhibitors and identify opportunities for future research in IdM.

1. Introduction

The problem of a global and universally trusted digital identity system – or, more specifically, lack of it – is a well-known problem. Decades of research have built a solid body of knowledge on cryptographic protocols, various architectural designs and functioning, yet, disconnected infrastructures. While the ultimate goal may be to achieve a global internet-based and user-centric digital identity solution, having one unique solution architecture dominating the global market is highly unlikely. This means that there will be a need for inter-domain integrations. Current and future problem in integrating identity management systems is the myriad of service providers (i.e., relying parties) that are not willing (and/or not capable) to implement large modifications in their systems. The future success of an IdM system is dependent on many factors: the solution should be technically sound, scalable, economically viable, convenient for human-users and what is often omitted in many system designs – recognize inter-organizational aspects. While considerable research efforts have been directed towards enabling the interoperability of technical components or accommodating usability factors, the organizational integration aspect is mostly assumed to be achievable and happening in the background. Solutions that span across organizational boundaries usually require changes of various degrees that involve coordinating multiple actors. These inter-organizational aspects range from infrastructural, system-level integrations, to higher-level strategic, business, liability aspects and trust. Therefore, in this research, we set to investigate the current state of IdM research and to elicit implicit architectural assumptions in the proposed designs. To the authors' best knowledge, digital identity architectures have been scarcely investigated from the point of view of non-technical assumptions.

Our research question is *what are the non-technical assumptions in the proposed solutions?* From a theoretical perspective, the analysis was inspired by Lago and Van Vliet [1] that define three types of architectural assumptions: technical, organizational and managerial. The application of their software engineering-specific types of assumptions to our analysis, however, was limited and we employed an inductive approach by deriving the dimensions from the data. The following three dimensions emerged from our data analysis: the extent of infrastructural changes, existence of a trusted party and the responsibility of human-user.

The analysis of sixty-two digital identity designs from literature demonstrates that proposed solutions are based on assumptions of different types. Some are of organizational nature that relate to business strategy or infrastructural concerns, while others are concerning trust and responsibility assumptions that are crucial to the wider adoption of the solution proposed. Full trust in a third party as the main premise is required in nearly half of solution designs. This implies an extensive guardian-

URI: https://hdl.handle.net/10125/64527
978-0-9981331-3-3

ship of a digital identity by the institution. The remaining half of the reviewed articles is based on human accountability assumptions. Infrastructural changes are found to be correlated with either the increased user responsibility or the existence of a trusted institution. Clearly, further research will be needed to investigate the relation between reasonable and, on the other hand, questionable assumptions that in their essence bridge or create the gap between the expected and actual realities.

2. Background

The main concern of this article is consumer Identity Management systems [2], in contrast to enterprise IdM. Organizational needs and requirements in IdM are very different from requirements for a global, more permanent, digital identity system. Enterprise IdM entails a central administrator that manages the needs of an organization, which initiates and provisions users with credentials, and privileges in a company environment. The lack of such a central authority makes the problem of a ubiquitous digital identity at least more challenging.

At a meta-level, digital identity ecosystem consists of three roles: Identity Provider (IDP), human-user, Relying Party (RP), where each actor has their own set of requirements. The RP needs a certain level of assurance to provide the service, the human-users want to be in control of their personal data, and the IDP requires certain diligence in the process of handling the data [3].

The classification of IdM systems has long been adhered to paradigms and models conceptualized in [4]. *Paradigms* refer to implementation and deployment of the system and can be network-, service- or user- centric. *Models* refer to where identity data are stored and delimit the responsibility of each party, such as isolated, centralized and federated models [5]. (For more details on the paradigms and models see [4]). While the research on user-centric designs has attracted much attention from researchers and practitioners, many proprietary solutions are based on service-centric paradigms (e.g., services from Google, Facebook) and with only limited federation of identity data possible (i.e., Single Sign-On (SSO) is possible with e.g., Google, but limited user control on what data is shared). Existing and functioning networks of identity systems (in research, education, companies, countries, etc.) cannot be easily modified [5]. Thus, the digital identity landscape consists of many disintegrated silos of infrastructures and the real challenge is to "connect" them and allow the inter-federation of trust.

Existing inter-federation architectures – approaches that enable multi-party federations – can be grouped into three types: *hierarchical root of trust, mesh-based and proxy federation* [3]. Root of trust design enables hierarchical services, with the most common examples such as eduroam – international network access for users in research and higher education [6] – and Domain Name Service (DNS) [7] – often criticized for its centralization drawbacks. Second model is a metadata aggregate publication (mesh), where federation participants do not need to negotiate agreements with each other individually but agree on a standard contract. The example of a mesh-based federation is InCommon – a federation of U.S. higher education institutions, which currently has approximately 10 million users and 760 educational institutions. InCommon also has an inter-federation agreement with eduGAIN – the EU higher education federation [3]. Third, proxy federation service is beneficial to RPs and IDPs because it requires only one point of integration but, on the other hand, implies high dependence on the proxy. Here, we refer to the Finnish implementation of a national eID framework as an example, where the role of brokers was introduced as intermediaries between IDPs and RPs [8].

In order to build a large-scale inter-federation employing any of the ecosystem designs above, it takes considerable effort to define legal agreements, federation policies on governance, agree on protocols, data structures and vocabularies. Regardless of the multi-party federation design, the goal is to facilitate and encourage integrations. The challenge of building a global digital identity system, thus, is an interconnection problem that requires more attention focused on business, legal, technical, operational and human linkages of its components.

2.1. Related Literature

Systematic literature reviews in the domain of IdM are very common. Partly, because of the rapid pace of technology innovation in the domain, ever changing regulatory guidelines and the importance of identity management for the functioning of societies. These are exemplified in the following works: classification of authentication systems and their usability and drawbacks [9], survey of existing authentication methods [10], framework for recommendation of authentication schemes [11] and a review of authentication using behavioral biometrics [12]. Literature reviews on identity management have been done from various perspectives, such as surveys in the context of Internet of Things [13], authentication for e-government services [14], on privacy preservation [15] and strategies [16], identity and access management in cloud environments [17]. With regard to more elaborate evaluations, Bonneau et al. [18], for instance, proposed a framework for IdM, using Usability-Deployability-Security as evaluation proper-

ties. Their results and other research on internet password [19] discuss the difficulties of replacing passwords and highlight the research challenges towards designing a password-less authentication scheme. Alternatively, quantitative and qualitative comparison of IdM architectures were performed using Architectural Tradeoff Analysis Method, ATAM [20]. In [20] the authors conclude with pointing out the difficulties in consistent comparison without solid metrics. In recent years, research on federated IdM architectures has been widely investigated, these are federated identity management (FIM) in the cloud [21], FIM challenges [22] and security issues of FIM in the cloud computing [23]. User-centric and self-sovereign identity are thought to be next phases of internet identity development after FIM [24]. Another recent trend in IdM is the application of blockchain [25]. Hence, publications have appeared in recent years e.g., conceptualizing essential components of self-sovereign identity [26], user-centric identity built on blockchain [27] and, counter arguments refuting some of widely-held misconceptions on blockchain as a new trust mechanism [28].

2.2. Architecture and assumptions

Making assumptions is an inevitable part of software development process. Architectural assumption[1] of a software system is defined as a statement about uncertain architectural knowledge [30]. Architectures – high-level conceptions of a system [1] – can be often built on design decisions that are based on some knowledge taken for granted or accepted as true without evidence at the moment. For instance, when a software developer makes an educated guess on the priority of requirements, or a number of potential users of a system per day [30]. These can be the most probable answers that are often automatic, unconscious or deliberately presumed.

Managing architectural assumptions in software development is a critical aspect to the success of any project [30]. When assumptions are not met they are found to be accounted for project failures [31]. For instance, in strategies for tackling assumptions in business plans for new ventures [32] assumptions are shown as impediments in the way of perceiving factual business realities. Lago and Van Vliet [1] define three types of architectural assumptions in software engineering: technical, organizational and managerial. While architectural assumptions have been extensively studied from the perspectives of developers and architects at different levels and throughout software lifecycle [1], more high-level assumptions are also worth to be investigated. In this article, we are particularly interested in assumptions at the ecosystem level: the interplay between technology and business, inter-organizational aspects and governance.

3. Method

This systematic review followed the guidelines for conducting literature reviews in software engineering [33]. The search was conducted in five databases: IEEE Xplorer, ACM Digital Library, Web of Science, Scopus and AIS eLibrary. The search string was as follows: ((*digital* OR *electronic* OR *online* OR *federated* OR *self-sovereign* OR *user-managed*) AND *identity architecture*). Figure 1 illustrates the process of study selection steps according to the PRISMA process [34].

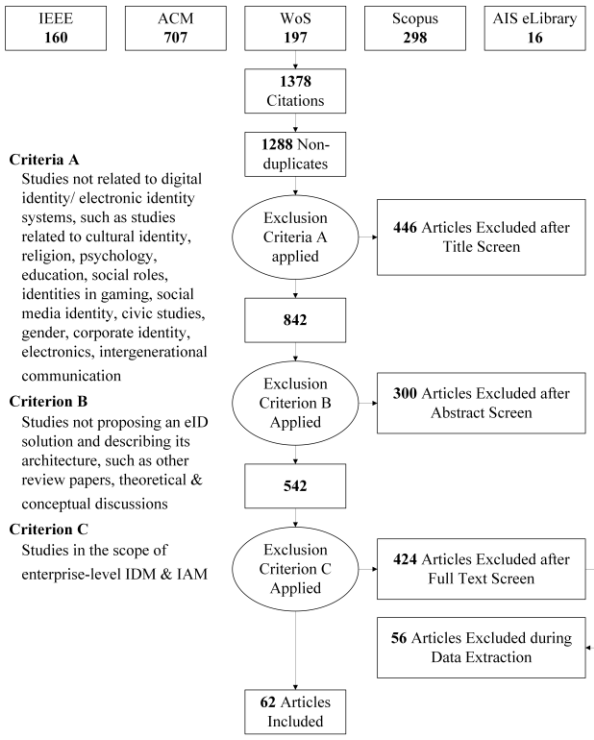

Figure 1. Systematic literature review process applied in this research.

Article selection requirements were the following: central theme is digital/electronic identity management; articles are peer-reviewed and discuss/propose a concrete solution architecture; article is concerned with consumer IdM systems i.e., global, internet scale (not enterprise IdM & IAM systems); articles are in the field of IS, IT, Computer Science research. The scope of the

[1] Assumptions, requirements and constraints are closely related, please refer to [29] for detailed definitions.

review was limited to the period from 2014 to 2019, for a review before 2014 see [35]. Articles describing purely formal cryptographic approaches without any explanations of the implications for governance, processes, or deployment requirements were excluded. Doctoral dissertations, master's theses, textbooks, and non-peer-reviewed papers were also ignored.

3.1. Assumptions extraction and synthesis

We reviewed 62 articles one by one to identify their explicit and implicit assumptions in the designs described. We searched for indications of *assumptions, limitations, constraints, challenges, requirements, and inhibitors* in the articles. We created and followed a review protocol, which ensured that the evaluation of the articles was fair and the methodology is trustworthy, rigorous, and auditable [36].

In software engineering, widely used classes of architectural assumptions [1] are *technical* (the technical environment in which a system is going to run), *organizational* (refers to the company developing the system or using it, its social settings and principles) and *managerial* assumptions (refers to business decisions and strategies to achieve objectives). While using these three categories as the initial schema, the assumptions elicitation process in this study became very soon a bottom-up one, i.e., we identified the assumption categories inductively from the data. Hence, the categories are: (A) the relation to legacy infrastructure, (B) the existence of a trusted third party institution, and (C) the increased human-user's responsibility. The article analysis data can be accessed online[2]. Each article was assessed whether it corresponds to the category in a binary manner: TRUE or FALSE.

For example, the solution in paper *[9] requires integrations with additional backend nodes and push message services (changes to legacy infrastructure –TRUE), implies a greater dependence on Certificate Authorities apart from a trusted IDP (existence of a trusted third party institution – TRUE). The authors also state that, "*The private key SK never leaves the [IdM wallet app]*", which implies an increased user responsibility (TRUE). Another example, the architecture in paper *[20] is based on Namecoin blockchain (TRUE), the proposed scheme is outside the control of any single entity (FALSE) and the InterPlanetary File System (IPFS) is used to publish the user profiles where the ownership is associated with a possession of a corresponding private key (TRUE). The architecture in paper *[39] proposes the use of the Open Algorithms (OPAL) paradigm in federations. This requires that a trust framework, which requires changes to existing operations (TRUE), governs the operational aspects of the federation. The architecture employs a gateway entity that coordinates queries and responses (TRUE) but the architecture has no new specifications for user-side (FALSE), apart from more user control to the execution of trusted algorithms.

4. Results

Assumptions elicitation resulted in the following dimensions. A (blue) – whether the solution requires a change to infrastructural components, and/or a completely new infrastructure; B (pink) – whether the solution implies a trusted third party (trusted intermediary, semi-trusted agents); C (lilac) – whether the solution assumes the users are ready to take more control and responsibility over "something they have", or requiring an increased user understanding and training. Figure 2 demonstrates the articles distribution that belong to dimensions described.

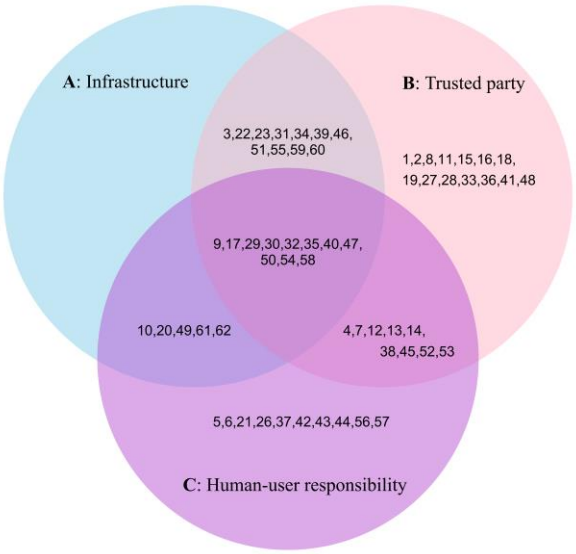

Figure 2. Venn diagram grouping articles according to assumption categories.

General assumptions, i.e., not IdM-specific, that were extracted vary from having no discussions on potential actors involved and their motivations in participating, to the ones that propose involving new agencies that are close to the user, such as insurance companies, banks, postal offices and local shops (e.g., paper *[38]) for identity provisioning. The number of articles that explicitly discuss adoption by providers (e.g., paper *[40]) is low. A viable economic model and considerations on

[2] Article list in ascending numerical order can be found following this link: https://tinyurl.com/y4pa8cvf

the incentives for the participation are crucial in attracting private sector. Table 1 lists the compilation of assumptions found.

Table 1 A list of assumptions.

General Assumptions:	Sources
Uptake and support of the solution by organizations, users and governments.	Nearly all articles
Once adopted in an e-government scenario the same technology will spread to other consumer cases (if the solution is in e-government context).	*[8], *[60], *[16]
Easy and cost-efficient distribution of tokens (if the solution implies tokens).	*[6], *[19]
The process of digital identity provisioning is optimized.	*[11], *[61], *[62]
Necessary inter-organizational collaborations are achievable.	*[53], *[10], *[15]
Sustainable business models exist; new model brings cost savings.	*[14], *[38], *[46]
A: Relation to Legacy Infrastructures:	
It is trivial to make integrations with e.g., IDPs and RPs.	*[50], *[47]
Scalability is achievable.	*[8], *[18], *[20]
The proposed governance structure is feasible.	*[24], *[39]
B: Trusted Institution:	
A Trusted third party (TTP) can be trusted (e.g., unlinkability of identities is guaranteed, key recovery not possible). TTPs are the intermediary institutions, except Identity Provider, such as manufacturers of secure hardware (e.g., Trusted Platform Module (TPM), Trusted Execution Environment (TEE), metadata proxies and other agents).	*[4], *[7], *[30],*[35], *[54], *[58]
C: Human-User's Responsibility:	
Users understand the importance of not compromising the security.	*[6], *[20], *[57]
Users would like to use their smartphones as security tokens.	*[5], *[32], *[43]
Smartphones are secure and used as a single repository for data.	*[7], *[13], *[29]
Users vouch to keep their tokens safe.	*[9], *[12]

The final list of articles consists of journal articles (N=16) and conference publications (N=46). The articles distribution by publication year is 2014 (15%), 2015 (15%), 2016 (19%), 2017 (31%), 2018 (20%). In relation to their contexts, articles could be grouped as e-government (N=18), Federated Identity Management (FIM, N=17), cloud IdM (N=14), smartphone-centric (N=11), blockchain (N=10), self-sovereign identity (SSI, N=6) and TPM or TEE (N=6). Nearly all studies are based on a common set of established technologies such as SAML, OpenID Connect, Web SSO, FIDO. One challenge with this is that FIM frameworks and protocols rely on static trust agreements and do not scale easily. On the other hand, articles within e-government and/or EU scope are mature and tend to investigate the inter-federation prospects. They are, however, limited in their scope to public service use cases. The majority of such works are in EU cross-border context (e.g., STORK project), public services in e-government related services, or specific domain contexts such as academic research collaborations (e.g., eduGAIN).

4.1. Relation to legacy infrastructure

In relation to existing IdM infrastructures, articles can be grouped to those proposing changes of various degrees in legacy infrastructures, such as improvements of PKI, or mechanisms for managing untrusted IDPs such as Google, Facebook, etc. Others propose that there is a need for completely new infrastructures such as private or public blockchains. This is illustrated by paper *[46], which describes an approach of a shared Know Your Customer (KYC) infrastructure among banks and regulators. However, according to previous research [37], such initiatives in making financial institutions work together involve complex and lengthy negotiations. Integration efforts and complexity [38] are addressed explicitly in only few articles. Even though, ultimately, the "winner" models should be integrated into existing infrastructures without significant changes.

Low-level infrastructural aspects such as deployment, storage and performance issues are investigated the most in articles within the domain of distributed cloud computing. Articles that focus on cross-cloud infrastructural interoperability try to address the issues of identity and access management (IAM) and attributes sharing (e.g., paper *[33]). For example, trust negotiation mechanisms was proposed based on reputation (e.g., paper *[48]), but this and related cloud-labeled articles are still based on some kind of pre-existing relationships such as a commercial organization with multiple branches in geographically diverse locations, or assume access to the performance history of a remote IDP. Articles tackling authentication and authorization in cloud environment often try to adapt IdM & IAM from enterprise world. Such solutions, however, require more consolidated approach and cannot be so easily abstracted and implemented in a non-enterprise world.

4.2. Trusted institutions

Articles that belong to this dimension are based on one or more trust anchors. These can be intermediaries that operate federation metadata, proxies, trusted hardware providers or personal data store agents. A trusted third party is an institution that facilities the process; or operates a software service that manages things on behalf of the user (e.g., in paper *[58] Dropbox, and Google Drive are used as personal data stores). Given the involvement of a TTP in an IdM scheme, complex governance techniques, including standards, best practices, and auditing must be managed. Building and operating TTPs is also costly and TTPs are subject to liabilities. Nevertheless, articles especially in the e-governmental context stress the need for operating a governmental TTP. Centralized designs, surprisingly, can also be found in a number of articles (e.g., the design in paper *[45] comprises of one central IDM server, mobile device and a cloud server).

There are at least two outlooks on the role of a trusted institution in the functioning of a digital identity. Studies supporting true self-sovereignty reject the involvement of any TTP (as in Pretty Good Privacy, PGP) and their opponents advocate TTP's inevitable need. The latter stance on self-sovereignty permits the use of self-attested attributes such as user preferences, but requires other claims to be verifiable [39]:

"*Trustworthy identity depends on jointly-issued credentials, where credentials and certification must be based on trustworthy assertions by the community of people and institutions in which we live. Identity credentials are […] not self-certifying systems.*"

As discussed elsewhere [40], current attempts at creating self-sovereign identity solutions (e.g., paper *[30] – Sovrin, paper *[58], paper *[61]), while being distributed and resistant to single entity control, are still logically centralized and fail to provide a true autonomy. This indicates that conceptually, some degree of centralization is unavoidable (i.e., IDPs), and the question is how to balance the centralization in the overall architecture.

4.3. Human-user's responsibility

At the other end of trust-in-institution spectrum, there is human-users' readiness and/or willingness to take responsibility over their digital identity. Here, we refer to designs where, for example, smartphones are at the center to operate credential wallets (IdM mobile applications), hardware modules or physical eID cards, for securely storing and accessing sensitive cryptographic key material, and other private data that users must keep secure. Advocacy for full human-user control essentially requires users to understand the importance of, e.g., safekeeping the keys or managing backups.

Nearly all articles emphasize the need for designing human-centric IdM architectures. Selective disclosure and pseudo-anonymization of personal data and design patterns with the master key pair and RP-specific keys are also commonly agreed patterns in the articles reviewed. In pseudonyms use, key management is under control of users to various extents. As articulated in [40], the reliance on a single key-pair in day to day operations is not optimal, there should be something-that-the-user-has, that users should keep safe and use to generate as many other key pairs as needed. This brings human-users full control over their interactions but also highlights the importance of self-accountability.

Furthermore, human-centric digital identity problem becomes a problem of a personal data wallet. Once attestations are in the wallet, the user should be able to use them freely with any RP. As any innovation at an early stage, digital wallets require many iterations of trials and errors. While being an important idea, such capabilities require immense paradigm shifts among organizations that currently operate data in silos. The rationale of cryptographic operations, such as the importance of understanding that the system implies no backdoor access or understanding the consequences of losing hardware security modules, is not easily accessible to ordinary human-users [41].

5. Discussion

Research on identity management today encompasses various forms of identity systems: distributed, decentralized and user-centric, user-managed, human-friendly, self-sovereign. Generally, current research is concerned more on personal data sharing or attribute-based mechanisms rather than traditional authentication problems. This may indicate the interest shift from the area of cryptographic schemes for authentication towards data sharing mechanisms.

By explicating non-technical assumptions from articles, our findings expose some of the fundamental issues potentially inhibiting internet-scale IdM system establishment. The elicitation of assumptions, which go hand in hand with risks, is important because solutions may incorporate design choices that are effective from an engineering viewpoint, but less feasible from a business perspective. General assumptions identified from this review (see Table 1) are the most prevalent and they are not IdM domain-specific, i.e., solution designs for problems in other domains are most likely based on these ge-

neric assumptions. Almost any new solution design proposed aspires to be accepted by experts, adopted by many organizations but only few studies articulate how.

At the high abstraction level, in order to achieve a well-functioning IdM system, human subjects must either trust in institutions such as IDPs, stewards, operators or take more control, and consequently, responsibility over their digital identity. Most designs are based on a trusted third party – excluding a trusted identity or attribute provider – acting on behalf of the human-user. This has considerable implications on human-user autonomy, i.e., what is the trust level of human-users to agents handling their personal data activities? What are the incentives for organizations to give up control?

In contrast, as illustrated by a smaller number of papers that do not rely on a TTP, but instead propose a solution with an increased human-user responsibility, digital identity wallets [42] are thought to be as the next milestone in IdM. Although the PGP approach, where the human-users have full control over the end-to-end interactions, provides and ensures the most security effectiveness when used correctly, the human component integration is usually the weakest link in a security chain [43]. While the interactions between (non tech-expert) human-users and digital artefacts can be made seamless, the fear of the unknown may potentially interfere with the solution acceptance. Especially based on modern offerings from, e.g., Google services where the illusion of human control is given to users, it is important for new truly self-sovereign solutions to help the users to understand the implications. Thus, the goal shall be to increase transparency, make complex cryptographic solutions humane and provide training for ordinary users. For example, it is important to dedicate more research and development effort on how multiple device support and synchronization could work without personal data escrow at providers. Or else, in case of future innovations with personal digital wallets, it is crucial for human-users to understand that the software behind it was built by some entity, but the software instantiation and the collection of data in it remains a personal asset [42].

Relation to legacy infrastructure category of assumptions is of organizational nature and refers to the extent of infrastructural changes in existing IdM systems. Infrastructural changes correlate with either the increased user responsibility or the existence of a trusted institution. In our review, no designs proposing only changes to existing infrastructures were found. Following the success of Bitcoin and alike, many propose to utilize blockchain as a main enabler for digital identity success. However, more research into the usefulness of blockchain in IdM is still necessary before obtaining a definitive answer. For example, research has found that the term blockchain (which is used as a main selling point for trust in many solutions reviewed) can rather be negatively connoted by human-users [44]. Implications can vary based on the criticality level of assumptions. Another way to process the results of this literature review is by interpreting the assumptions as a whole. When the authors of articles make a decision, consciously or unconsciously, in favor of a certain design choice, for example by using an IdM wallet application or introducing new roles, each individual research contributes to the shaping of the discourse and, consequently, failing or pushing the reality of IdM industry to change.

5.1. Non-academic solution designs

Here, we include a brief overview of non-academic solution architectures that were outside the scope of the literature review. We select solutions that, in our perspective, represent the contemporary industry development to provide a bit more complete perspective on the state-of-the-art of IdM. First, it is essential to discuss the evaluative study of the Distributed Ledger Technology based IdM schemes by Dunphy & Petitcolas [25], where they evaluate three representative proposals of decentralized trusted identity and SSI solutions – uPort, ShoCard and Sovrin. The full description and detailed comparison of solutions can be found in [25].

We now discuss their design choices along the three assumption categories we identified. While ShoCard solution can be bootstrapped with existing identity documents, the relying parties must make integrations with ShoCard's centralized servers (Category A – TRUE) – intermediary for storing encrypted attributes (Category B – TRUE). Human-users are offered to control the creation and disclosure of their ShoCardIDs via a mobile application (Category C – TRUE). However, there is an "unclear usability and user understanding of ShoCard privacy implications" [25]. uPort is built on Ethereum DLT and uses smart contracts to regulate the data operations and to hold the mapping of uPort identifiers with the data itself stored on IPFS infrastructure (TRUE). Its key design choice is the lack of a central authority (FALSE), but the secret key, for example, that is under full control of human-users is kept only on the user's mobile device (TRUE), it supports the social recovery protocol (i.e., users must nominate the trustees who can vote to replace the public key). Sovrin is an open-source solution built on a permissioned DLT and Linux Foundation's Hyperledger Indy project codebase (TRUE). Stewards are the trust anchors that govern the infrastructure and take part in consensus protocols (TRUE). Human integration in Sovrin is reported to be remain an open issue as the system is at the early development phase [25]. Human-users can choose whether to use the storage capabilities of their endpoints or, otherwise,

must rely on agencies that will act on their behalf (TRUE or FALSE).

Dunphy & Petitcolas [25] conclude that there is an inevitable need for some centralization in IdM architectures. This includes the process of identity provisioning, backup & recovery of cryptographic keys and secure lookup of entities and services. Moreover, our findings resonate with their conclusion on the existence of the widespread assumption that users are naturally equipped with skills to conduct effective cryptographic key management and understand the implications of distributed/decentralized/DLT-based data management:

"*Approaches to digital identity that remove central authorities and depend upon effective key management strategies from its users create the risk that non-technical users will be alienated by the technology"* [25].

Another example of privacy-enhancing credentials implementation is IBM's Identity Mixer [45] – a protocol suite that provides strong authentication with privacy-preserving features: anonymity and unlinkability. Although the building blocks for Identity Mixer have been based on the advanced and mature cryptographic schemes (such as selective disclosure by Camenisch & Lysyanskaya [46]), the technology was not widely adopted due to the deployment complexities (TRUE). Although the solution architecture eliminates the need for any additional TTPs (FALSE), and hands in a full control to the human-user (TRUE), the intricacies of the reference implementation required specialized knowledge and understanding of technology (e.g., developers and implementers need to learn the specific data formats) that hindered the adoption [47]. The experiments with real-world infrastructures as part of EU ABC4Trust project revealed the challenges that could be grouped into two categories [47]:

- challenges to enable users to manage their identities and the identity management process;
- challenges to encourage the (commercial) usage of privacy preserving credentials by relying parties and service providers.

These challenges are in line with the two assumption categories we identified: human-user integration and the degree of infrastructural changes.

Among other examples from the industry are the new digital ID from MasterCard[3] and Sign in with Apple[4] that put strong emphasis on privacy of personal information but have inherent design limitation that puts these entities at the center managing the digital identity network.

While every non-substantiated assumption should be considered as vulnerability, it does not mean that assumptions need to be avoided. Rather, they ought to be recognized and explicitly stated. In conclusion, our high-level review of various IdM architectures designs shows that solution designs can be based on trust in an institution or human-user responsibility along with infrastructural deployability assumptions. These assumptions have their own implications, and, more importantly, they manifest the research gap. For instance, the concept of human-user's readiness to take responsibility is more than user experience; or that the role of various institutions and businesses in IdM is not entirely understood.

5.2 Limitations

Our research has limitations. *First*, our study was limited to the research published in the most common Information technology (IT) outlets, and does not include all publication forums (we did not look into professional sources, only academic publications). Our overview of non-academic solutions in Discussion section is rather superficial and was included in an attempt to provide pointers for further research. Furthermore, we did not perform backward and forward searches as part of the snowballing technique. *Second*, we did not differentiate between different purposes of identity management. It is important to note that we employ the digital identity solution in its broad scope. This includes strong user authentication as well as and single sign-on and sharing of attributes in a privacy-friendly way. There was neither a differentiation on the security achieved, the privacy provided, nor the technology employed. We hope that these factors could be taken into account in the future work. *Third*, in present review we focused on non-technical assumptions based on the information provided in the articles only. In [31], the authors indicate the challenges in assumptions recovery from a system without having a thorough understanding of the system. Therefore, we make a call for future research that may entail a deeper inquiry involving interviews of key people and stakeholders, and the analysis of documentation. *Fourth*, the generalizability of our findings needs to be investigated in future research due to a small sample of articles in the analysis. In this study, we focused on three types of assumptions. The list is possibly not yet complete, and we hope that the future work may extend it.

6. Conclusion

It is widely acknowledged that trust establishment plays a key role in scalability of IdM solutions. There is a clear need for consolidation of distributed and fragmented, currently ongoing and future IdM initiatives. In

[3] https://www.wired.com/story/mastercard-digital-id/

[4] https://www.evernym.com/blog/login-with-apple/

this article, we observe that inter-organizational integrations can be the background problem of a ubiquitous IdM establishment. Our findings show that various IdM designs proposed are in the spectrum of either trust in a third-party institution, or full control by the human-user. In addition, infrastructural changes proposed also depend on these two assumptions, or a combination of both. This indicates that even self-sovereign identity designs, or the use of blockchain in IdM still require some kind of trusted agent or the trust in human subject's responsibility. We call for future research to bear in mind non-technical assumptions and to address their implications explicitly. For instance, what are the roles in the proposed solution? What are the potential organizations, and what are the incentives for their participation? Specifically, what innovative business models are required? Why should organizations collaborate and what is the extent of infrastructural changes in participating organizations?

7. Acknowledgments

We thank the mini-track chairs and anonymous reviewers whose comments have greatly improved this manuscript.

8. References

[1] P. Lago and H. van Vliet, "Explicit Assumptions Enrich Architectural Models," in *Proceedings of the 27th International Conference on Software Engineering*, New York, NY, USA, 2005, pp. 206–214.

[2] T. Hardjono and A. Pentland, "Open Algorithms for Identity Federation," in *Advances in Information and Communication Networks*, 2019, pp. 24–42.

[3] M. Schwartz and M. Machulak, *Securing the Perimeter - Deploying Identity and Access Management with Free Open Source Software*. 2018.

[4] Y. Cao and L. Yang, "A survey of Identity Management technology," in *2010 IEEE International Conference on Information Theory and Information Security*, 2010, pp. 287–293.

[5] J. Carretero, G. Izquierdo-Moreno, M. Vasile-Cabezas, and J. Garcia-Blas, "Federated identity architecture of the European eID System," *IEEE Access*, vol. 6, pp. 75302–75326, 2018.

[6] "eduroam – World Wide Education Roaming for Research & Education." [Online]. Available: https://www.eduroam.org/. [Accessed: 26-Aug-2019].

[7] P. Mockapetris and K. J. Dunlap, "Development of the Domain Name System," in *Symposium Proceedings on Communications Architectures and Protocols*, New York, NY, USA, 1988, pp. 123–133.

[8] Finnish Transport and Communications Agency (Traficom), "Electronic identification and trust services," 30-Aug-2019. [Online]. Available: https://www.kyberturvallisuuskeskus.fi/en/electronic-identification. [Accessed: 02-Sep-2019].

[9] M. H. Barkadehi, M. Nilashi, O. Ibrahim, A. Zakeri Fardi, and S. Samad, "Authentication systems: A literature review and classification," *Telematics and Informatics*, vol. 35, no. 5, pp. 1491–1511, Aug. 2018.

[10] K. Halunen, J. Häikiö, and V. Vallivaara, "Evaluation of user authentication methods in the gadget-free world," *Pervasive and Mobile Computing*, vol. 40, pp. 220–241, Sep. 2017.

[11] I. Velásquez, A. Caro, and A. Rodríguez, "Kontun: A Framework for recommendation of authentication schemes and methods," *Information and Software Technology*, vol. 96, pp. 27–37, Apr. 2018.

[12] I. C. Stylios, O. Thanou, I. Androulidakis, and E. Zaitseva, "A review of continuous authentication using behavioral biometrics," in *ACM International Conference Proceeding Series*, 2016, vol. 25-27-September-2016, pp. 72–79.

[13] S. Pal, M. Hitchens, and V. Varadharajan, "Modeling Identity for the Internet of Things: Survey, Classification and Trends," in *2018 12th International Conference on Sensing Technology (ICST)*, 2018, pp. 45–51.

[14] A. Dubey, Z. Saquib, and S. Dwivedi, "Electronic authentication for e-Government services — A survey," in *10th IET System Safety and Cyber-Security Conference 2015*, 2015, pp. 1–5.

[15] U. A. Khan and K. Mustafa, "Survey on Privacy Preservation and Identity Management Systems," *Computer Science and Engineering*, vol. 6, no. 9, p. 9, 2017.

[16] J. Werner, C. M. Westphall, and C. B. Westphall, "Cloud identity management: A survey on privacy strategies," *Computer Networks*, vol. 122, pp. 29–42, Jul. 2017.

[17] I. Indu, P. M. R. Anand, and V. Bhaskar, "Identity and access management in cloud environment: Mechanisms and challenges," *Engineering Science and Technology, an International Journal*, vol. 21, no. 4, pp. 574–588, Aug. 2018.

[18] J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano, "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes," 2012, pp. 553–567.

[19] D. Florencio and C. Herley, "An Administrator's Guide to Internet Password Research∗," p. 18.

[20] C. Staite and R. Bahsoon, "Evaluating identity management architectures," in *Proceedings of the 3rd international ACM SIGSOFT symposium on Architecting Critical Systems - ISARCS '12*, Bertinoro, Italy, 2012, p. 11.

[21] R. Shere, S. Srivastava, and R. K. Pateriya, "A review of federated identity management of OpenStack cloud," in *2017 International Conference on Recent Innovations in Signal processing and Embedded Systems (RISE)*, 2017, pp. 516–520.

[22] J. Jensen, "Federated Identity Management Challenges," in *2012 Seventh International Conference on Availability, Reliability and Security*, 2012, pp. 230–235.

[23] E. Ghazizadeh, M. Zamani, J. A. Manan, and A. Pashang, "A survey on security issues of federated identity in the cloud computing," in *4th IEEE International Conference on Cloud Computing Technology and Science Proceedings*, 2012, pp. 532–565.

[24] C. Allen, "The Path to Self-Sovereign Identity," 2016. [Online]. Available: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html.

[25] P. Dunphy and F. A. P. Petitcolas, "A First Look at Identity Management Schemes on the Blockchain," *IEEE Security & Privacy*, vol. 16, no. 4, pp. 20–29, Jul. 2018.

[26] A. Muehle, A. Gruener, T. Gayvoronskaya, and C. Meinel, "A survey on essential components of a self-sovereign identity," *Computer Science Review*, vol. 30, pp. 80–86, Nov. 2018.

[27] D. Augot, H. Chabanne, T. Chenevier, W. George, and L. Lamber, "A User-Centric System for Verified Identities on the Bitcoin Blockchain," *arXiv:1710.02019 [cs, math]*, Oct. 2017.

[28] A. Auinger and R. Riedl, "Blockchain and Trust: Refuting Some Widely-held Misconceptions," in *Proceedings of International Conference on Information Systems*, 2018, p. 9.

[29] R. Roeller, P. Lago, and H. van Vliet, "Recovering architectural assumptions," *Journal of Systems and Software*, vol. 79, no. 4, pp. 552–573, Apr. 2006.

[30] C. Yang, P. Liang, and P. Avgeriou, "A survey on software architectural assumptions," *Journal of Systems and Software*, vol. 113, pp. 362–380, Mar. 2016.

[31] A. A. Mamun and J. Hansson, "Review and Challenges of Assumptions in Software Development," *Second Analytic Virtual Integration of Cyber-Physical Systems Workshop (AVICPS)*, p. 8, 2011.

[32] Z. Block and I. C. MacMillan, "Milestones for Successful Venture Planning," *Harvard Business Review*, no. September 1985, 01-Sep-1985.

[33] B. Kitchenham, O. Pearl Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, "Systematic literature reviews in software engineering – A systematic literature review," *Information and Software Technology*, vol. 51, no. 1, pp. 7–15, Jan. 2009.

[34] D. Moher, A. Liberati, J. Tetzlaff, D. G. Altman, and T. P. Group, "Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement," *PLOS Medicine*, vol. 6, no. 7, 2009.

[35] A. Alkhalifah and J. D'Ambra, "Identity Management Systems Research: Frameworks, Emergence, and Future Opportunities," p. 17, 2015.

[36] S. Keele, "Guidelines for performing systematic literature reviews in software engineering," Technical report, Ver. 2.3 EBSE Technical Report, 2007.

[37] A. Bazarhanova, J. Yli-Huumo, and K. Smolander, "From platform dominance to weakened ownership: how external regulation changed Finnish e-identification," *Electronic Markets*, 2019.

[38] D. Slamanig, K. Stranacher, and B. Zwattendorfer, "User-centric identity as a service-architecture for eIDs with selective attribute disclosure," in *Proceedings of ACM Symposium on Access Control Models and Technologies, SACMAT*, 2014, pp. 153–163.

[39] A. Pentland and T. Hardjono, "Digital Identity Is Broken. Here's a Way to Fix It," *WSJ*, 03-Apr-2018. .

[40] G. Linklater, C. Smith, A. Herbert, and B. Irwin, "Toward Distributed Key Management for Offline Authentication," in *Proceedings of the Annual Conference of the South African Institute of Computer Scientists and Information Technologists*, New York, NY, USA, 2018, pp. 10–19.

[41] K. Halunen and Outi-Marja Latvala, "Cryptography for Human Senses," *IACR Cryptology ePrint Archive*, p. 757, 2018.

[42] D. O'Donnell, "The Current and Future State of Digital Wallets," *Continuum Loop Inc.*, p. 83, 2019.

[43] A. Whitten and J. D. Tygar, "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0," in *USENIX Security Symposium*, 1999, vol. 348, pp. 169–184.

[44] N. Ostern and J. Cabinakova, "Pre-Prototype Testing: Empirical Insights on the Expected Usefulness of Decentralized Identity Management Systems," in *Proceedings of the 52nd Hawaii International Conference on System Sciences*, 2019, p. 10.

[45] J. Camenisch, S. Mödersheim, and D. Sommer, "A Formal Model of Identity Mixer," in *Formal Methods for Industrial Critical Systems*, 2010, pp. 198–214.

[46] J. Camenisch and A. Lysyanskaya, "An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation," in *Advances in Cryptology — EUROCRYPT 2001*, 2001, pp. 93–118.

[47] K. Rannenberg, J. Camenisch, and A. Sabouri, "Attribute-based Credentials for Trust," *Identity in the Information Society, Springer*, 2015.