Universal Identity and Access Management Framework for Future Ecosystems

Daniela Pöhn* and Wolfgang Hommel
Universität der Bundeswehr München, Research Institute CODE, 85579 Neubiberg, Germany
{daniela.poehn, wolfgang.hommel}@unibw.de

Received: December 21, 2020; Accepted: February 18, 2021; Published: March 31, 2021

Abstract

Identity and access management (I&AM) plays a crucial role in today's IT infrastructure. In order to access a service, the user needs to authenticate. I&AM maintains attributes, credentials, roles, and permissions for an identifier, which is, e.g., linked to a human person. The variety of approaches to solve I&AM makes it hard to compare or even combine them. As various protocols are developed to solve real-world problems, it is increasingly difficult to provide secure implementations and configurations. In order to gain an overview and to enable interoperability, this article proposes an identity and access management framework (IAMF). Based on a motivating scenario, different requirements are mapped with identity management models and approaches within. These findings build the foundation for IAMF, consisting of a technical architecture and interfaces for processes. The fundamental difference to existing systems is its integrating, interoperable, and modular approach.

Keywords: Identity Management, Identity Management Framework, Federated Identity Management, Framework

1 Introduction

According to [46], the standard user has 90 online accounts. In the U.S., an average of 130 accounts are assigned to a single email address. These identities are used for work, e-government, and social media for example. Each identity is linked to a specific context and has different user information, called attributes. Providers like Facebook and Google allow users to securely re-use their accounts to authenticate at other services by utilizing the protocols OAuth and OpenID Connect (OIDC). The same principle is used by Security Assertion Markup Language (SAML) in research and education. Even though the re-use is possible in some federated identity management (FIM) scenarios, this is not the case everywhere. The resulting diversity makes it cumbersome for users to get an overview of which services received which personally identifiable information. Additionally, end users tend to insecurely re-use or modify their passwords across providers, as shown by Wang et al. [75]. According to [46], 10.8% users have only one default password, while 49.3% re-use passwords sometimes for unimportant or non-critical accounts.

Besides human users, computers, and servers, also smartphones, other mobile devices, Internet of Things (IoT) devices as well as cooperation partners are added to the identity portfolio of companies. With this multitude of standards, solutions, and identities, it is cumbersome to keep an overview. As identity theft and other attacks targeting accounts are rising, the situation is even more challenging.

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), 12(1):64-84, Mar. 2021
DOI:*10.22667/JOWUA.2021.03.31.064*

[*] Corresponding author: Universität der Bundeswehr München, Research Institute CODE, 85579 Neubiberg, Germany, Tel: +49 89 6004 2495

According to the Identity Defined Security Alliance, 79% of organizations have experienced an identity-related security breach in the last two years [31]. Although FIM allows the secure re-use of account information, the impact of identity theft is higher. A status overview of one's own identity management is crucial for the security and the base for continuous service improvements.

We address these problems by an extensive state of the art analysis in accordance to [54], which is extended by the design of a modular framework, consisting of an architecture and proposed interfaces for business processes. The design tries to achieve interoperability between identity providers (IdPs) and service providers (SPs) for different use cases and standards. Thereby, we investigate on the integration of existing approaches and interfaces for processes into such a framework and analyze required tools. These tools need to be adaptable and modular within the framework. We additionally explore ways to improve the multi-lateral security. This includes an overview of the entity's security of its identity management system, but also interfaces to other entities in case of incidents. Consequently, we enhance [54] by the outline of a framework combining as many approaches as possible while providing additional value in accordance to the stated requirements.

This article contributes the following improvements to the identity management landscape: It designs a generic identity and access management framework (IAMF) as a layer for different identity management use cases. IAMF allows various protocols to interact. It further adds an overview of all identity management systems run within one organization and an integration to security management. Security management, for example according to the norm ISO/IEC 27001 [34], requires an overview as a first step. Then security controls, tests, and incidents can be analyzed in a controlled and structured way. The IAMF overview therefore helps to improve the security of identity management and connected services. IAMF is a work-in-progress approach. An implementation and cross-organizational security incident processes still need to be established.

The rest of the article is organized as follows: Section 2 motivates the work through a chosen scenario, a literature analysis, and a summary of gained requirements. Section 3 introduces the identity models centralized, federated, and user-centric identity management. It further discusses different approaches within and compares them with the gathered requirements [54]. This is followed by an high-level overview of the framework IAMF in Section 4, describing the introduced components. Section 5 discusses the framework based on the motivating scenario and gained requirements, followed by a brief security analysis in Section 6. Section 7 concludes the article and gives future directions.

2 Requirements for Interoperable Identity & Access Management

Before the IAMF can be designed, relevant requirements need to be gathered. We describe shortcomings and already existing possibilities with a motivating scenario from a research cooperation. In a next step, we analyze literature. This is followed by the summarized requirements.

2.1 Research Cooperation Scenario

In the chosen scenario, a university cooperates with two commercial companies in a research project. All entities use different local identity management systems for the users of their own systems. This may result in several accounts for the end user when accessing external services. Like most organizations, the university runs a local Identity & Access Management (I&AM) to provide several services, e.g., email and web conferencing, to students, staff, and professors alike. The I&AM is based on the protocol Lightweight Directory Access Protocol (LDAP). The university is part of national and international research and education federations, such as DFN-AAI and eduGAIN. These federations use SAML to provide an authentication and authorization infrastructure for their members. As a result, the university runs SAML software, e.g., Shibboleth, on top of LDAP. With a collaboration outside of these federations, the university has to find other means, especially if the partners do not use SAML.

The I&AM at the company *A* is based on Active Directory (AD). In order to allow Web Single Sign On (SSO) for other services, the component Federation Services (AD FS) is deployed. AD FS can make use of several protocols, like OAuth and SAML. The company operates a private cloud for data storage, which suppliers and project partners can access with OAuth and a variant of OIDC. As both partners do not apply the same protocol, a proxy or bridge is needed. On account of running Shibboleth as SAML implementation, the university is able to integrate and configure an OIDC extension. Company *B* is a startup without I&AM. They use Internet of Things (IoT) devices in a testing environment with local accounts. In order to participate, either company *A* needs to set up local accounts for the cloud or company *B* needs a guideline to decide and configure the best fitting I&AM software. As prerequisite, the I&AM software should enable FIM and suit IoT. Since company *B* is into blockchains, user-centric approaches, i.e., User Managed Access and Self-Sovereign Identities (SSIs), are evaluated as well.

2.2 Literature Analysis

Several approaches already gathered requirements for identity management. Torres et al. [71] concluded that Usability, Interoperability, Functionality, Trustworthiness, Security, Mobility, Privacy, Law Enforcement, and Affordability are the main requirements. These are used as bases for IoT by Boujezza et al. [14]. The requirements excluding Mobility are stated by Ferdous and Poet [18]. The newest direction of identity management is SSIs. According to El Haddouti and El Kettani [25], SSIs have the requirements User Control and Consent, Minimal Disclosure for a Constrained Use, Justifiable Parties, Directed Identities, Design for a Pluralism of Operators and Technology, Human Integration, and Consistent Experience across Contexts.

2.3 Summary of the Requirements

The requirements gathered by Torres et al. [71] are used as foundation, incorporating requirements for SSIs, shown in [54]. Since further functionalities for integration of other approaches and protocols might be needed, the requirement *Functionality* is split into *Management* of identities and further *Functionality*. The General Data Protection Regulation (GDPR) gives users the right to get an export of their account as well as porting their data to another SP. As a result, the requirement *Location* of the user data is changed to *Portability*. This includes pluralism of operators and technology. With ever evolving protocols, it is important to be able to integrate them into existing infrastructures. Hence, the requirement *Affordability* is divided into *Integration* and *Scalability*, a main drawback of large-scale SAML infrastructures with central trusted third parties (TTPs). Additionally, more and more devices and identities are added, giving increasing importance to scalability. As a result, the following requirements, shown in Table 1, are used to evaluate different approaches. They extend the requirements gathered by Torres et al., taking SSIs and the evolving ecosystem into account, and build the base for IAMF.

3 Overview of Identity Management Models

According to Yuan Cao and Lin Yang [79], identity management can be characterized by three models, which include different approaches.

- Centralized / Network-centric Identity Management.
- Federated / Application-centric Identity Management.

Table 1: Requirements for Universal Identity Management according to [54]

No.	Name	Description
REQ1	Management	This requirement describes the management of identities, e.g., human, IoT, computers, and the automation of it.
REQ2	Usability	This requirement comprises user interface, reduced complexity, and consistent experience across platforms.
REQ3	Interoperability	With this requirement, the interoperability between protocols, models, and silos including protocol variants is described.
REQ4	Scalability	The requirement scalability details the mobility of the environment. The environment should be scalable for an increasing amount of identities, devices, and protocols.
REQ5	Functionality	The requirement represents needed functionality for universal identity management. This includes services, like translation services, proxies and bridges between for interoperability as well as group management.
REQ6	Trustworthiness	Trust need to be established and estimated between involved entities. In order to facilitate trustworthiness, trust management, segregation of power, and policies for automated trust estimation are required.
REQ7	Security	This requirement describes basic, i.e., single-entity, and multi-lateral security. Security can be enhanced by security management.
REQ8	Portability	In accordance to GDPR, the requirement details the portability of accounts and systems.
REQ9	Privacy	The requirement represents the aspects anonymity, pseudonymity, transparency, controlability, consent, and data minimization.
REQ10	Liability	Liability and accountability are relevant for law-enforcement, digital evidence, and data retention. Accountability is required for paid services, but also for security. Logged data is on the other hand in contrast with privacy. Therefore, it has to be in accordance to law.
REQ11	Integration	The requirement describes affordability of the solution including needed efforts for the integration into processes and existing infrastructure.

- Decentralized / User-centric Identity Management.

Although centralized identity management was the first evolutionary step after isolated services, it is still used as a base. In the following, protocols, approaches, and new directions within these three models are analyzed regarding the stated requirements [54].

3.1 Centralized Identity Management

Centralized identity management is typically based on LDAP, e.g., with OpenLDAP or AD. As directory service for Windows domain networks, AD additionally uses Kerberos and Domain Name System (DNS). DNS as hierarchical decentralized naming system translates memorable domains to numeric internet protocol (IP) addresses. In order to locate the correct IdP of the user, SAML utilizes a list of entity information, called metadata. Other methods exist for OAuth and OIDC. The EU project LIGHTest [59, 58] suggests an extension of DNS as method for discovery and trust. Since it is bound to certificates, it requires eIDAS, resulting in fixed Level of Assurance (LoA) and centralized structure. It is further adapted for IoT. Additional approaches propose DNS for IoT [77, 45, 81, 49], with efficiency and life cycle as drawbacks. Florea et al. [20] provide an overview of different protocols used for IoT, while Belran and Skarmeta [7] describe the protocol Authentication and Authorization for Constrained Environments (ACE) [63].

Protocols specify the technical requirements, but not aspects of the business process, e.g., life cycle. As a result, many approaches are not (REQ3) interoperable, which is comprehensible. Nevertheless, even centralized I&AM can integrate IoT and business decisions might lead to joint ventures and other agreements. Other drawbacks are (REQ6) trust, (REQ1) management, and (REQ11) integration, while (REQ8) portability is difficult to estimate. An overview of the requirements is given in Table 2.

Table 2: Analysis of Centralized Identity Management based on Requirements

No.	Name	Description
REQ1	Management	Software fulfills management. Otherwise it is mainly out of scope.
REQ2	Usability	Single Sign On allows usability locally. Otherwise it is out of scope.
REQ3	Interoperability	Some implementations include several protocols, otherwise this requirement is not fulfilled.
REQ4	Scalability	With centralized identity management, the scalability issue should be less prominent.
REQ5	Functionality	Software includes several functionalities. Otherwise it is out of scope.
REQ6	Trustworthiness	As centralized identity management is within one organization, it is out of scope.
REQ7	Security	This is mainly out of scope, though most software has security implemented.
REQ8	Portability	This is mainly out of scope.
REQ9	Privacy	This is mainly out of scope.
REQ10	Liability	Software has logging mechanisms, otherwise it is out of scope.
REQ11	Integration	For software, integration guides are typically available. Otherwise it is out of scope.

3.2 Federated Identity Management

FIM consists of several IdPs and SPs, which have a common goal and technical setup. The predominant protocols are SAML and OAuth with its authentication layer OIDC. As TTPs are involved in SAML federations, scalability is a drawback [6]. Even though some implementations allow both protocols, interoperability is a general problem between them. Caused by real-world problems, new protocols and extensions are evolving. Different research approaches [4, 19, 55, 39, 16, 33] try to tackle specific issues. Similarly to centralized identity management, DNS is utilized for technical trust establishment [66, 29]. Due to advances in lawmaking and regulations, [36, 11, 27, 56, 12, 13] describe eIDAS, which is based on SAML, and show the combination with other federations. One drawback is the lack of integration into eduGAIN, the de-facto standard federation for research and education. Alonso et al. [3] present a solution for the specific use case FIWARE. Federation as a service, a service offered to customers related to identity management, is apprehended in research [82, 80] with drawbacks i.a. in trust.

To sum up, these approaches in FIM have several drawbacks, ranging from (REQ3) interoperability, to (REQ5) functionality, and (REQ10) liability. With additional policies and agreements, liability is often set up. For interoperability, additional tools, like proxies, are introduced. The protocols themselves are silos. SAML has the further drawbacks regarding (REQ4) scalability and (REQ8) portability. The research approaches lack (REQ3) interoperability, (REQ6) trustworthiness, and (REQ11) integration. (REQ10) Liability depends on the implementation and established processes. This results in Table 3.

Table 3: Analysis of Federated Identity Management based on Requirements

No.	Name	Description
REQ1	Management	All approaches allow federations. The management of identities and policies is thus out of scope.
REQ2	Usability	This is out of scope.
REQ3	Interoperability	Some actual implementations provide interoperability by extensions, e.g., AD and Shibboleth.
REQ4	Scalability	The scalability is a drawback of SAML [6]. This may be the case with the DNS extension as well.
REQ5	Functionality	Translation and group management are out of scope.
REQ6	Trustworthiness	LIGHTest uses DNS and eIDAS, but does not allow other methods. Other approaches tackle trust with non-practical proposals. Otherwise, it is out of scope.
REQ7	Security	This is mainly out of scope.
REQ8	Portability	This is out of scope.
REQ9	Privacy	Besides user consent, it is out of scope.
REQ10	Liability	This is out of scope.
REQ11	Integration	This is out of scope.

3.3 User-Centric Identity Management

Kumar et al. [44] and Slomovic [65] show that although pseudonymity and anonymity are important, identities from different social networks can be merged and lead to one specific person. User-centric identity management evolved in parallel to FIM [73], but is not yet relevant in practice. It recently gained more attention with the hype of blockchain. Two main directions can be seen: UMA and SSI. Both give the user more control over their personal data, but (REQ3) interoperability still has to be improved. (REQ10) liability and (REQ5) functionality depend on actual approach, client, and provider.

UMA [42, 48, 50] extends OAuth, although it can be applied to IoT [15] and other use cases. UMA works on interfaces to SSI. In parallel to SSI, other privacy enhancing technologies are developed [60, 61, 62]. Toth and Anderson-Priddy [72] describe the principle of SSI management. SSIs are typically implemented by verifiable, decentralized digital identities, like blockchain. The law of identities is adapted to SSI by Ferdous et al. [17], while the step from typical user-centric identity management to SSI is seen as a evolutionary step by Sovrin [70]. These research approaches [68, 21, 67, 69, 76, 5, 51, 52, 26, 47] differ in technology and architecture. Common drawbacks are (REQ4) scalability and, for early work, (REQ9) privacy. CREDENTIALS [74, 43, 40, 28] proposes a data sharing platform based on identity wallets, basically playing man in the middle. The cloud federation SUNFISH [1, 2] is a collaboration for sharing data hosted on private cloud infrastructures of organizations for business. It has limitations in (REQ6) trust, (REG11) integration, among others. Other approaches propose dynamic cloud federation on blockchain [41, 9, 8, 10], not taking methods like Vectors of Trust (VoT) [57] into account. It furthermore concentrates on one use case and has deficits in (REQ9) privacy.

In summary, user-centric identity management has drawbacks in (REQ3) interoperability, (REQ5) functionality, and (REQ10) liability. Benefits and drawbacks though depend on the approach. UMA could be adapted for further use cases, though not further explored. SSI often lacks (REQ4) scalability and (REQ9) privacy. (REQ4) scalability, (REQ6) trustworthiness, and (REQ11) integration are missing in cloud federations based on blockchain. By this, the following Table 4 condenses the analysis.

Table 4: Analysis of User-Centric Identity Management based on Requirements

No.	Name	Description
REQ1	Management	UMA allow federations. The management of identities and policies is thus out of scope. SSI could be used in federation use cases.
REQ2	Usability	This is out of scope.
REQ3	Interoperability	The principle of UMA can be applied to things [15] and theoretically to different protocols. Though it is not described, SSI could be used for different protocols and users.
REQ4	Scalability	As UMA builds upon OAuth and can be used with SSI, scalability is met. Some SSI approaches have drawbacks with scalability.
REQ5	Functionality	Besides functionality for the user, this is out of scope.
REQ6	Trustworthiness	The user is control, but otherwise it is out of scope.
REQ7	Security	Blockchain itself is secure, other parts including the actual implementation are mainly out of scope.
REQ8	Portability	This is out of scope, but could be easily integrated from the user-side.
REQ9	Privacy	UMA allows control of accounts and attributes, otherwise it is out of scope. With SSI, users have full control, though there might be drawbacks for privacy as well.
REQ10	Liability	For UMA, the user has more control, but otherwise it is out of scope. This is mainly out of scope, though Grabatin et al. [23] describe quality of service parameters and policies for a 5G scenario.
REQ11	Integration	This is out of scope.

4 IAMF, a Universal Identity and Access Management Framework

Neither centralized, federated identity management, UMA, nor SSIs fulfill all requirements. One big issue of the identity management ecosystem is (REQ3) interoperability between different approaches and protocols. With organizations using several protocols, e.g., to enable IoT devices, a universal framework, i.e., architecture with interfaces to processes, which still needs to be designed, can help to gain an overview and provide the missing interoperability. Frameworks [16, 66] known to the authors concentrate on a specific use case or protocol, but do not provide a generic framework for identity management. Norms and standards [37, 24, 35, 34] focus on special aspects, describing the requirements and recommendations. Therefore, norms and standards provide a comprehensive base for security management, accountability, and liability as well as trust.

4.1 Overview of the Framework IAMF

This section presents an overview of the Identity Management Framework IAMF, shown in Figure 1, which will be implemented in future work. The framework addresses the requirements stated in Section 2. As a result, the design goals focus on interoperability and integration. By providing an overview, the current state of the identity management system in place and, therefore, the (REQ7) security related to it can be gained. With no overview, security cannot be estimated and improved. Considering that the framework can work both centralized and decentralized, while the TTP is only involved during the initial setup, the framework is (REQ4) scalable. IAMF comprises of three different components and uses existing approaches, whenever it is possible. The TTP as well as the component for the end user are optional, though providing additional value.

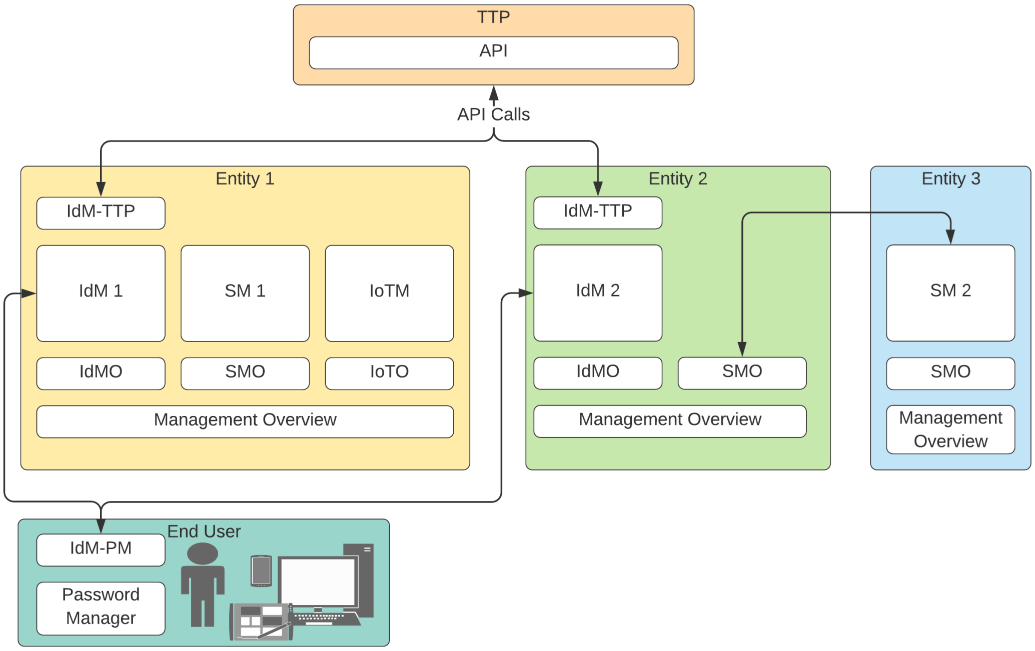


Figure 1: Overview of the Identity & Access Management Framework Architecture

- **TTP:** The TTP has an Application Programming Interface (API) for queries. Thereby, additional functionalities for, e.g., translation between protocols, mappings, and federation management can be provided. These are shown in detail in Figure 2a.

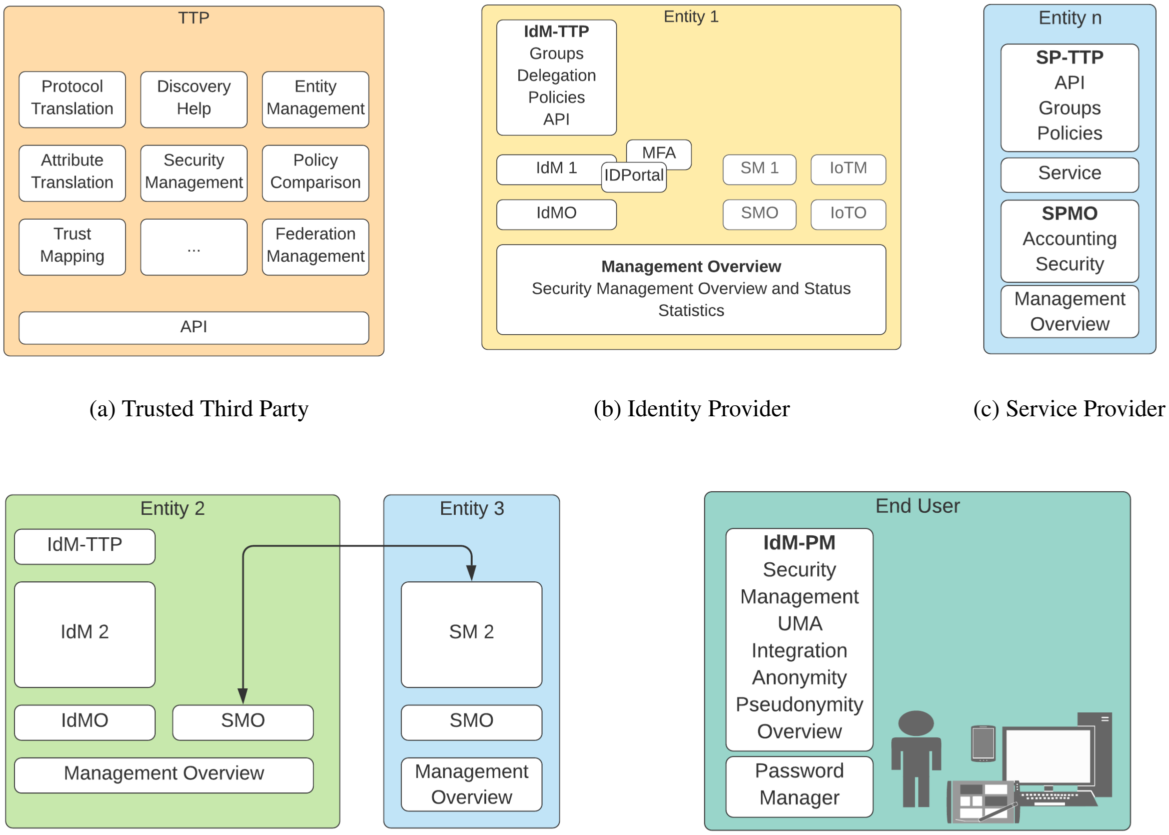
- **Components for Entities:** FIM consists of two main entities, i.e., IdP and SP. While Figure 1 describes two IdPs and an outsourced service, Figure 2c visualizes an SP. A more detailed IdP managing human users is displayed in Figure 2b. The components for IdPs and SPs can be divided into the following:

  - **Interfaces to the TTP**, i.e., IdP-TTP and SP-TTP, shown in Figure 2c. The add-on to the entity software provides the main supplementary functionality for the entities. In order to use the modules of the TTP in both directions, it includes an API. Most functionalities can be provided locally as well, if required.
  - **Overview**, i.e., IdMO, SPMO, and a generic management overview (MO). The overview presents information about the status of the identity management system, collaborations, federation memberships, security controls of identity management and their status, and thereby a status of the security management as well as policies.

  Besides identity management for human users, shown in Entity 1 as IdM 1, also server management (SM) and IoT management (IoTM) can be included. These do not need an interface with the TTP, but an overview, i.e., SMO and IoTO, to see if the security controls are met. These variants are left out for clarity reasons.

- **Component for the End User:** A kind of password management (PM) tool for end users. In addition to traditional password management tools, this identity management (IdM)-PM add-on helps the user to get an overview about the accounts and the related security status. It provides an interface for UMA and other user-centric identity management approaches. These are shown in Figure 2e in more detail.

In the following, the components of the IAMF are presented comprehensively. The figures and descriptions are focusing on identity management for human users for better understanding. Already available components are re-used when possible.



(a) Trusted Third Party (b) Identity Provider (c) Service Provider

(d) Outsourced Service (e) User

Figure 2: Overview of IAMF Component Architectures

4.2 Trusted Third Party

In SAML federations, federation operators run TTPs, which aggregate SAML metadata and provide further services dependent on the federation. Services can include conversion rules to translate from one schema to another. The research approach GEANT-TrustBroker [55] extended these TTPs, in order to provide dynamic metadata exchange, level of assurance automation [22], and conversion between different schemas. In addition, a distributed setting was proposed [53]. The IAMF TTP enhances this approach by the functionality derived from the requirements. Therefore, it is expended for general usage and includes further functionality. The TTP, shown in Figure 2a, has an API, enabling the automation of required steps. The modules added in the figure are Protocol Translation, Attribute Translation, Trust Mapping, Discovery Help, Security Management, Entity Management, Policy Comparison, and Federation Management. As the TTP is modular and configurable, not all modules need to be used and it can be made adjustable to fit for different use cases.

In the following, the main functionality is described. In order to make use of these functionalities, the entities, i.e., IdPs and SPs, first need to register. The entities should state used protocol, attribute schema, and trust schema locally in a configuration file. This can be done by pointing to an already existing configuration file, e.g., SAML metadata. The location of the entity configuration file is then stored. For a lightweight design, the TTP only points to the policies. The *policy management* and *trust mapping* of IAMF allow the comparison of entity policies and level of assurance, similarly to [22]. By that, a fast estimation is made related to the compatibility from the trust perspective. If entities want to form a formal *federation*, policies for the federation are configured as well. By stating protocols and schemata, the TTP helps to *translate between protocols*. Existing proxies between SAML variations, SAML and OAuth respectively OpenID Connect can be re-used. The TTP stores all known translations between protocols, attribute schemes, and trust schemes. The interface IdP-TTP downloads required translations before it translates messages. Thereby, only the needed amount of data is stored locally. If the IdP-TTP works as standalone component, all translations are integrated locally. Links to aggregated metadata for SAML and other *discovery* possibilities, e.g., Webfinger [38] and Metadata Query Protocol [78], can be added.

4.3 Identity Provider Extension

The identity provider extension includes three main components: an interface to the TTP, called IdM-TTP, an IdP management overview IdMO, and the generic management overview, as shown in Figure 2b. *IdP-TTP* communicates with the TTP via an API. The additional functionality include providing policies, delegation of tasks, and group management. For group management, existing tools, like Grouper, can be re-used. This is run on top of the IdP software in operation. Internally, the users change passwords, request further accounts, and add additional factors at the IdP's ID Portal. These accounts can then be re-used at different SPs. By providing a per-IdP overview of the services and attributes, the IdP helps the user to get an overview of its data. Consents can be withdrawn. Even though SAML federations use consent, getting an overview of all data sent to SPs can be cumbersome. The *IdMO* and the generic *management overview* provide technical personnel as well as management with information about the status, security, and statistics. As accountability is required, log files can be viewed. A portability function is possible, though both functions are normally provided by already established means. The view is dependent on the role of the user. While the management is interested in a situation overview, technical personnel depends on deeper insights.

4.4 Service Provider Extension

Similarly to the IdP, the SP consists of SP-TTP, SPMO, and an overall management overview. The components are shown in Figure 2c. The *SP-TTP* includes interfaces for delegation and group management as well as policy. Group management helps to form dynamic groups for one or several services. The reason for the group are different, e.g., a project or a team of employees interested in a specific topic. *SPMO* provides a management overview including accounting and security for a specific service, while the generic *management overview* gives a summary of the all service status. The overview features different views, as technical personnel require enhanced information, while management wants to have an overall view. If an entity outsources a service, then both entities receive a related overview. This is shown in Figure 2d. The sort and amount of information vary and also depend on the contract.

4.5 End User

The end user, shown in Figure 2e, receives further control by the *IdM-PM* module. It is an add-on for password manager, providing an overview of the accounts. Additionally, it helps to increase the security of the accounts by security management. This includes requests to, e.g., HaveIbeenpwnd [30] to see, a) whether the password of an account is already known, b) irregular login attempts, c) information about passwords used for several accounts, and d) alerts about data breaches. Further queries to similar services and processing other sources are possible. If a user wants to port an account to another IdP, a portability request is sent by IdM-PM. Additional functionality is provided by UMA integration as well as an anonymity and pseudonymity service.

5 Discussion of IAMF

In this section, we discuss the presented architecture based on the motivating scenario. The added functionalities are analyzed next, followed by an evaluation based on the requirements. The workflows visualize the interactions between the components. Last but least, drawbacks and limitations are shown.

5.1 Application to the Research Cooperation Scenario

Using the motivating scenario given in Section 2.1, three entities participate in this federation. The university runs the SAML implementation Shibboleth on top of OpenLDAP. Company *A* uses AD and AD FS with OAuth and a variant of OIDC. Company *B* has no central identity management system. Based on a decision matrix, future work of IAMF, it installs and configures OpenLDAP and an OAuth implementation with the IAMF add-on. The university and company *A* implement the add-on as well. The federation operator of the university already runs the TTP. Both company *A* and *B* add the chosen TTP into their configuration. The further setup is completed automatically and not only the private cloud of company *A* can be used, but all services of the university as well. The translation between the protocols is carried out by the add-ons with help of the TTP. Company *B* can integrate user-centric identity management allowing users to control their accounts even across several platforms and organizations.

5.2 Analysis of the Functionality based on the Requirements

As described above, several services are included into the IAMF to meet the requirements and provide additional value. The services offered by the IAMF are shortly explained in this section. They can be added, configured, and adapted. In the future, further services might be possible.

- **Entity Management:** Functionality for managing the entity in FIM including policies, endpoints, protocol, and attribute schema. This module is integrated into the components TTP, IdP-TTP, and SP-TTP. As it only points to configuration files, it is still lightweight.

- **Federation Management:** Functionality for setting up static and dynamic federations with own policy. This module is integrated into TTP, but can be used locally with IdP-TTP and SP-TTP.

- **Policy Management:** Functionality for creating and comparing polices. Based on policies, a decision about the membership in a federation or trust establishment between two entities can be made. This module is integrated into TTP, but is able to be used locally with IdP-TTP and SP-TTP.

- **Security Management:** Functionality to increase the security of identities. A process cycle with various checks helps to improve the security. Interfaces to security management tools provide seamless integration and processes. This module is integrated into TTP for federated use cases, IdP-PM at the end user, IdMO, and SPMO. Security is shortly discussed in the following section.

- **Protocol Translation:** Bridges for translation between different protocols. This module is integrated into the component TTP, but can be used locally with IdP-TTP and SP-TTP. Known bridges are integrated, like the SATOSA SAML2SAML tool [32].
- **Attribute Translation:** Translation of attribute schema and attributes, i.e., user information. This module is integrated into TTP, but can be used locally with IdP-TTP and SP-TTP.
- **Trust Mapping:** Functionality for mapping different trust schemes and levels. This module is integrated into TTP, but can be used locally with IdP-TTP and SP-TTP. It is an extension of [22].
- **Discovery Help:** Functionality for helping discover entities. This module is integrated into TTP and broadens the scope of IdP discovery service in SAML and similar functionality.
- **Group Management:** Functionality for end users setting up dynamic groups, which are propagated to services. Group Management is partly integrated into the components TTP and SP-TTP. It is helped by IdP-TTP and can be added to IdM-PM for privacy-concerned users. By providing such a tool, the service overhead is reduced. Existing tools, like Grouper, are integrated.
- **Delegation Management:** Functionality for end users to delegate tasks and temporary permissions. Within one organization, this module is integrated into IdP-TTP. In federated use cases, it is part of SP-TTP and TTP. Theoretically, privacy-concerned users can add the module to IdM-PM.
- **Accounting:** Functionality for liability and financial reasons integrated into the component SPMO.
- **Management Overview:** Overview of the status of the service, security, and related information. This module is integrated into IdM-PM, IdPO respectively SPMO and management overview.
- **UMA Integration:** Integration of UMA for end users at the component IdM-PM.
- **Anonymity / Pseudonymity Service:** If possible, the user can get pseudonyms. A combination with UMA is recommended. This module is integrated into the component IdM-PM.

These functionalities fit to the requirements as follows, see Table 5. The analysis shows that the requirements can be met, although further work is needed. This includes a concrete design of the framework, a proof-of-concept implementation and evaluation, but also federated security processes. These will be targeted in future work.

5.3 Exemplary Workflows

In order to visualize the interactions between the components and the re-use of already established protocols, exemplary workflows are described. These are shown with a TTP for simplicity. For registration, the entity first configures its component locally. If a TTP is enabled, the registration is sent to a TTP via an API, shown in Figure 3a. The entity respectively the IdP-TTP or SP-TTP sends required information of the configuration file to the TTP, which verifies it. If the entity wants to apply for membership in a federation, the entity sends a request to the TTP for verification. The same applies for policies. The entity creates a policy, which gets registered at the TTP. It can be changed and deleted. The TTP answers with the status of the request. The workflow for the usage of conversion rules is similar. The rules are verified by the TTP. Changes are notified to the entities using it.

Table 5: Analysis of the IAMF Framework based on Requirements

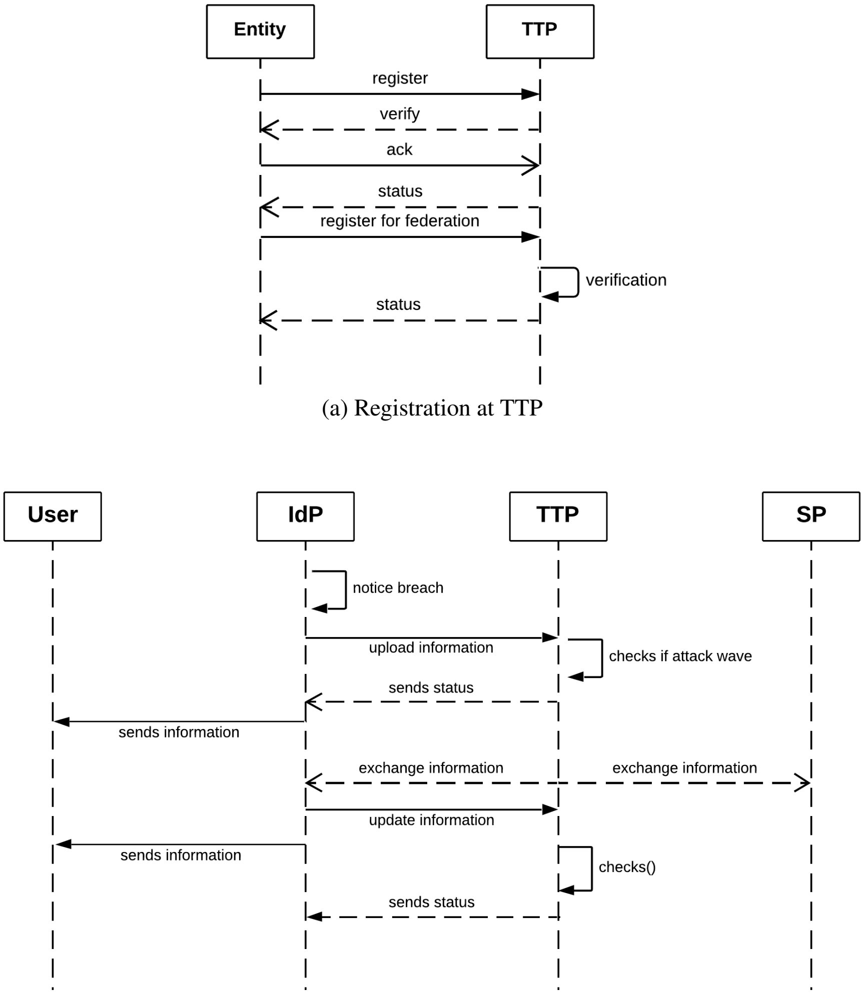
No.	Name	Description
REQ1	Management	With the different management overviews, several layers of overview are provided. Additionally, all modules can be configured and help to manage identity management.
REQ2	Usability	So far, usability is achieved by the component IdM-PM with UMA integration, anonymity / pseudonymity service, and a management overview. Further work is needed to understand usability better.
REQ3	Interoperability	Extensions to several protocols as well as the different translation functionalities help to provide interoperability.
REQ4	Scalability	Since the TTP is only involved in the first trust establishment and further queried if needed, it does not result in a bottleneck. Furthermore, several TTPs can be used in parallel.
REQ5	Functionality	The functionalities described above fulfill this requirement.
REQ6	Trustworthiness	By trust mapping and policy management, trust requirements can automatically be compared. This helps to provide trustworthiness.
REQ7	Security	IAMF provides a security module for federated incidents, helping to multilateral improve security by seamless integration into already established tools. The processes needed still need to be designed. The security of the IAMF is shortly analyzed in the following section.
REQ8	Portability	A request functionality can be added at IdM-PM, asking the IdP to export the account data, which then should be able to import into another service. A translation of the attributes might need to take place.
REQ9	Privacy	Anonymity and pseudonymity help to provide privacy. Additionally, only the needed information is stored at the TTP and other entities.
REQ10	Liability	Accounting helps to provide liability in addition to logging.
REQ11	Integration	The integration takes place with add-ons for IdP, SP, TTP, and user. Further protocols can be added, although each adaption requires effort.

An example workflow for federated security management is shown in Figure 3b. If the IdP notices a data breach of a user, it first starts a security management process inside the organization. Anonymized information is uploaded to the TTP, which checks if similar attacks accumulate in the last time. The TTP sends the status of this check to the IdP. The IdP informs the user as well. IdP and involved SPs exchange required information without additional communication with the TTP. If further information has come up, the IdP updates the distributed information accordingly.

5.4 Limitations of IAMF

While the effort for setting this cooperation up differs between the organizations, especially organizations with several cooperation benefit from the dynamic establishment of connections while still providing trust by policy and assurance comparison. Although the IAMF components require configuration in the beginning, it can save time for service desk and administrators in the long run. This is the case with group management, as described in the scenario, but also with dynamic federations and trust management. The different translation services help to reduce duplicated accounts and, thereby, effort for service desk and administrators. However, all partner organizations should enable IAMF for fully dynamic establishment and functionality.

In FIM, TTPs already exist, as federation operators run services for SAML federations. The TTPs



(a) Registration at TTP

(b) Security Management

Figure 3: Exemplary Workflows

of IAMF provide additional value for the federation operators and their customers, i.e., universities, research institutions, and commercial services. The services and modules of the TTP can be adapted. This example also shows that several organizations might run TTPs in parallel, similarly to [53]. In order to minimize data, these TTPs should know each other. As TTPs are mostly not involved in the communication, the performance is only reduced during the initial setup between two entities. The proxies between protocols require time to translate messages, although this is a simple transformation. Without proxies, the communication would not be possible. As this is a real-world problem, several proxies between SAML and OpenID Connect already exist and Shibboleth, an open source SAML implementation, is planning to provide an official OpenID Connect plug-in [64]. These proxies should be able to integrate into IAMF, though with an increasing number of variants, this can be difficult. Depending on future protocol and concept developments, adaptations for IAMF might be needed though.

IAMF is a framework on top of existing protocols and software for interoperability and security. To the authors, no further frameworks are known with this broad scope. Therefore, a comparison to other approaches of identity management is not feasible.

6 Security Considerations

Identity information is an interesting target for attacks. The attackers can be insider as well as outsider, while the knowledge ranges from script kiddies to state-sponsored attackers. In the following, security considerations for IAMF and components, attack vectors, and security benefits are discussed. The brief analysis concentrates on attackers up to criminals. For a more detailed analysis, the architecture will be modeled in the future.

6.1 IAMF and related Components

The security of the IAMF is mainly linked to the security of the different parties, the design, and the implementation of the components. The framework itself is lightweight and does not store unnecessary information, which already reduces the attack surface. Instead of a TTP, the functionality can also be provided decentralized.

The TTP of the IAMF has access to public information about SP, IdP, and end user, such as attribute types, endpoints, and level of assurance. Therefore, the TTP stores no sensitive data besides basic account information of IdPs and SPs, which are publicly available. The account information are kept according to current state-of-the-art methods. If changes to the federation setting occur, involved administrators get notified. Updates of the TTP, the local data, and software need to be accepted beforehand. In case of attribute mapping, the IAMF provides conversion rules, which are approved and integrated by the IdP administrator. The components of the framework do not receive user information.

6.2 Attack Vectors

Possible attacks can result from different vectors. One way is man-in-the-middle (MITM), if an attacker manages to listen and change communication between components. As components need to authenticate and a sequence number is added, MITM attacks are mitigated. A checksum helps to identify changed messages during transaction. Different attacks can target the TTP, as it includes modules for trust establishment. One example is a spoofing attack of a user targeting a policy in order to receive access to a service. The TTP needs to be hardened and the code should be security by design. The API requires authentication and administrators get at least notified for changes as well as corrupt states. As a result, attacks targeting the TTP are hindered. The same applies for IdP and SP components. Bugs within the code can be another vector. Pentests and fuzzing can, e.g., be used to improve the code. Another vector uses social engineering, especially at the end user side and targeting administrators. If a malware, like a key logger, is installed on the user's computer, accounts are compromised. This vector already exists. With security management, the consequences are at least contained. In order to reduce the risk of masquerade entries, they can be checked by the module.

6.3 Security Benefits

Resulting from the increasing identity theft and the consequences for individuals and organizations [31], security management for identities is added at different levels of the IAMF. Thereby, different aspects, like password breaches, unusual behavior, and missing second factors are reported as soon as discovered. Identity-related security controls should be configurable. Subsequent actions in a controlled process help to increase the security and readiness level even further. This helps to limit data breaches and further security incidents. The process provided by the IAMF should be integrated in already existing processes, e.g., ISO/IEC 27001. As a result, the module needs interfaces, like APIs, to already running software.

7 Conclusion and Future Work

Identities are everywhere. Each and every person has several digital identities to participate in the digitized world. An increasing number of identity management approaches have been developed and several are in the making. This diversity of solutions makes it difficult to get an overview. Interoperability is even more challenging. With growing identity theft, secure identity management gets more relevant than before. As security is getting into focus, management becomes cumbersome. In this article, we give a broad overview of the identity management models centralized, federated, and user-centric identity management and related approaches. These are mapped with the requirements gained from a motivating scenario with three different entities and literature review. The findings lead to the design of the work in progress framework IAMF, helping to make the silos interoperable. The framework includes additional functionalities for, e.g., translation, group management, and delegation. Additionally, it provides an overview of the used identity management systems in an organization and their related status. As an overview is the first step to improve security, it also helps to align policies and progress. The outline of the framework is concluded by a discussion based on the motivating scenario, the gathered requirements, workflows, and security considerations. For future work, we plan to investigate into the role of identity management in standards, like IT Infrastructure Library (ITIL) and ISO/IEC 27001, in more detail and describe generic identity management processes. As the security of the whole framework can be boiled down into the security of the different components and the interaction between them, we plan to establish a federated security management process. Security controls will be derived, helping to establish security processes for different use cases. A reference architecture of different identity management models and of IAMF may guide administrators as template and help us to identify further missing functionalities and components. With a reference model in place, the attack vectors are analyzed in greater depth. Last but not least, the framework designed in this article will be implemented and evaluated.

References

[1] S. Alansari, F. Paci, A. Margheri, and V. Sassone. Privacy-Preserving Access Control in Cloud Federations. In *Proc. of the 10th International Conference on Cloud Computing (CLOUD'17), Honolulu, Hawaii, USA*, pages 757–760. IEEE, June 2017.

[2] S. Alansari, F. Paci, and V. Sassone. A Distributed Access Control System for Cloud Federations. In *Proc. of the 37th International Conference on Distributed Computing Systems (ICDCS'17), Atlanta, Georgia, USA*, pages 2131–2136. IEEE, June 2017.

[3] A. Alonso, A. Pozo, J. Choque, G. Bueno, J. Salvachúa, L. Diez, J. Marìn, and P. L. C. Alonso. An Identity Framework for Providing Access to FIWARE OAuth 2.0 - Based Services According to the eIDAS European Regulation. *IEEE Access*, 7:88435–88449, July 2019.

[4] P. Arias Cabarcos, F. Almenárez, F. Gómez Mármol, and A. Marín. To Federate or Not To Federate: A Reputation-Based Mechanism to Dynamize Cooperation in Identity Management. *Wireless Personal Communications*, 75(3):1769–1786, August 2013.

[5] L. Axon and M. Goldsmith. PB-PKI: A Privacy-aware Blockchain-based PKI. In *Proc. of the 14th International Joint Conference on e-Business and Telecommunications (ICETE'17), Madrid, Spain*, pages 311–318. SciTePress, July 2017.

[6] M. S. Bargh, B. Hulsebosch, and H. Zandbelt. Scalability of Trust and Metadata Exchange Across Federations. In *Proc. of the 2011 TERENA Networking Conference (TNC'11), Prague, Czech Republic*, May 2011.

[7] V. Beltran and A. F. Skarmeta. An overview on delegated authorization for CoAP: Authentication and authorization for Constrained Environments (ACE). In *Proc. of the 3rd World Forum on Internet of Things (WF-IoT'16), Reston, Virginia, USA*, pages 706–710. IEEE, December 2016.

[8] G. Bendiab, N. Kolokotronis, S. Shiaeles, and S. Boucherkha. WiP: A Novel Blockchain-Based Trust Model for Cloud Identity Management. In *Proc. of the IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing (DASC'18), Athens, Greece*, pages 724–729. IEEE, August 2018.

[9] G. Bendiab, S. Shiaeles, and S. Boucherkha. A New Dynamic Trust Model for "On Cloud" Federated Identity Management. In *Proc. of the 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS'18), Paris, France*, pages 1–5. IEEE, February 2018.

[10] G. Bendiab, S. Shiaeles, S. Boucherkha, and B. Ghita. FCMDT: A Novel Fuzzy Cognitive Maps Dynamic Trust Model for Cloud Federated Identity Management. *Computers & Security*, 86:270–290, September 2019.

[11] D. Berbecaru, A. Atzeni, M. d. Benedictis, and P. Smiraglia. Towards Stronger Data Security in an eID Management Infrastructure. In *Proc. of the 25th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP'17), St. Petersburg, Russia*, pages 391–395. IEEE, March 2017.

[12] D. Berbecaru and A. Lioy. On integration of academic attributes in the eIDAS infrastructure to support cross-border services. In *Proc. of the 22nd International Conference on System Theory, Control and Computing (ICSTCC'18), Sinaia, Romania*, pages 691–696. IEEE, October 2018.

[13] D. Berbecaru, A. Lioy, and C. Cameroni. Electronic Identification for Universities: Building Cross-Border Services Based on the eIDAS Infrastructure. *Information*, 10(6), June 2019.

[14] H. Boujezza, M. AL-Mufti, H. K. B. Ayed, and L. Saidane. A taxonomy of identities management systems in IOT. In *Prof. of the 12th International Conference of Computer Systems and Applications (AICCSA'15), Marrakech, Morocco*, pages 1–8. IEEE, November 2015.

[15] L. Cruz-Piris, D. Rivera, I. Marsa-Maestre, E. De la Hoz, and J. R. Velasco. Access Control Mechanism for IoT Environments Based on Modelling Communication Procedures as Resources. *Sensors*, 18(3), March 2018.

[16] R. D. Dhungana, A. Mohammad, A. Sharma, and I. Schoen. Identity Management Framework for Cloud Networking Infrastructure. In *Proc. of the 9th International Conference on Innovations in Information Technology (IIT'13), Abu Dhabi, UAE*, pages 13–17. IEEE, March 2013.

[17] M. S. Ferdous, F. Chowdhury, and M. O. Alassafi. In Search of Self-Sovereign Identity Leveraging Blockchain Technology. *IEEE Access*, 7:103059–103079, July 2019.

[18] M. S. Ferdous and R. Poet. A comparative analysis of Identity Management Systems. In *Proc. of the 10th International Conference on High Performance Computing Simulation (HPCS'12), Madrid, Spain*, pages 454–461. IEEE, July 2012.

[19] M. S. Ferdous and R. Poet. Dynamic Identity Federation Using Security Assertion Markup Language (SAML). In *Proc. of the 3rd IFIP Working Conference on Policies and Research in Identity Management (IDMAN'13), London, UK*, pages 131–146. Springer-Verlag, April 2013.

[20] I. Florea, R. Rughinis, L. Ruse, and D. Dragomir. Survey of Standardized Protocols for the Internet of Things. In *Proc. of the 21st International Conference on Control Systems and Computer Science (CSCS'17), Bucharest, Romania*, pages 190–196. IEEE, May 2017.

[21] S. Friebe, I. Sobik, and M. Zitterbart. DecentID: Decentralized and Privacy-Preserving Identity Storage System Using Smart Contracts. In *Proc. of the 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications (TrustCom'18), New York, New York, USA*, pages 37–42. IEEE, August 2018.

[22] M. Grabatin, W. Hommel, S. Metzger, and D. Pöhn. Improving the Scalability of Identity Federations Through Level of Assurance Management Automation. In *Proc. of the 9th DFN-Forum Kommunikationstechnologien, Rostock, Germany*, pages 67–76. GI, May 2016.

[23] M. Grabatin, W. Hommel, and M. Steinke. Policy-Based Network and Security Management in Federated Service Infrastructures with Permissioned Blockchains. In *Proc. of the 6th International Symposium Security in Computing and Communications (SSCC'18), Bangalore, India*, volume 969, pages 145–156. Springer-Verlag, September 2018.

[24] P. A. Grassi, M. E. Garcia, and J. L. Fenton. NIST Special Publication 800-63-3 – Digital Identity Guideline. Technical report, National Institute of Standards and Technology, U.S. Department of Commerce, June 2017.

[25] S. E. Haddouti and M. D. Ech-Cherif El Kettani. Analysis of Identity Management Systems Using Blockchain

Technology. In *Proc. of the 2nd International Conference on Advanced Communication Technologies and Networking (CommNet'19), Rabat, Morocco*, pages 1–7. IEEE, April 2019.

[26] H. Halpin. NEXTLEAP: Decentralizing Identity with Privacy for Secure Messaging. In *Proc. of the 12th International Conference on Availability, Reliability and Security (ARES'17), Reggio Calabria, Italy*, pages 92:1–92:10. ACM, August 2017.

[27] J. L. Hernandez-Ardieta, J. Heppe, and J. F. Carvajal-Vion. STORK: The European Electronic Identity Interoperability Platform. *IEEE Latin America Transactions*, 8(2):190–193, April 2010.

[28] F. Hörandner, S. Krenn, A. Migliavacca, F. Thiemer, and B. Zwattendorfer. CREDENTIAL: A Framework for Privacy-Preserving Cloud-Based Data Sharing. In *Proc. of the 11th International Conference on Availability, Reliability and Security (ARES'16), Salzburg, Austria*, pages 742–749. IEEE, August 2016.

[29] R. J. Hulsebosch, M. Bargh, P. H. Fennema, J. F. Zandbelt, M. Snijders, and H. Eertink. Using Identity Management and Secure DNS for Effective and Trusted User Controlled Light-Path Establishment. In *Proc. of the 1st International Conference on Networking and Services (ICNS'06), Silicon Valley, California, USA*, pages 79–79. IEEE, July 2006.

[30] T. Hunt. Have I Been Pwned: Check if your email has been compromised in a data breach, 2021. `https://haveibeenpwned.com` [Online; accessed on March 22, 2021].

[31] Identity Defined Security Alliance. Identity Security: A Work in Progress, February 2021. `https://www.idsalliance.org/identity-security-a-work-in-progress/` [Online; accessed on March 22, 2021].

[32] idpy.org. SATOSA, February 2021. `https://github.com/IdentityPython/SATOSA` [Online; accessed on March 22, 2021].

[33] M. Isaakidis, H. Halpin, and G. Danezis. UnlimitID: Privacy-Preserving Federated Identity Management Using Algebraic MACs. In *Proc. of the 15th Workshop on Privacy in the Electronic Society (WPES'16), Vienna, Austria*, pages 139–142. ACM, October 2016.

[34] ISO Central Secretary. ISO/IEC 27001:2013/COR 2:2015 – Information technology – Security techniques – Information security management systems – Requirements – Technical Corrigendum 2. Technical report, International Organization for Standardization, October 2015.

[35] ISO Central Secretary. ISO 29146 – Information technology – Security techniques – A framework for access management. Technical report, International Organization for Standardization, June 2016.

[36] C. Jesus, G. Izquierdo-Moreno, M. Vasile-Cabezas, and J. Garcia-Blas. Federated Identity Architecture of the European eID System. *IEEE Access*, 6:75302–75326, November 2018.

[37] Joint Task Force. Draft NIST Special Publication 800-53 – Revision 5 – Security and Privacy Controls for Information Systems and Organizations. Technical report, National Institute of Standards and Technology, U.S. Department of Commerce, December 2020.

[38] P. E. Jones, G. Salgueiro, M. B. Jones, and J. Smarr. WebFinger. IETF RFC 7033, September 2013. `https://www.ietf.org/rfc/rfc7033.txt` [Online; accessed on March 22, 2021].

[39] M. Kang and A. Khashnobish. A Peer-to-Peer Federated Authentication System. In *Proc. of the 6th International Conference on Information Technology: New Generations (ITNG'09), Las Vegas, Nevada, USA*, pages 382–387. IEEE, April 2009.

[40] F. Karegar, C. Striecks, S. Krenn, F. Hörandner, T. Lorünser, and S. Fischer-Hübner. Opportunities and Challenges of CREDENTIAL. In *Proc. of the 2016 IFIP International Summer School on Privacy and Identity Management, Karlstad, Sweden*, pages 76–91. Springer-Verlag, August 2016.

[41] B. Keltoum and B. Samia. A Dynamic Federated Identity Management Approach for Cloud-based Environments. In *Proc. of the 2nd International Conference on Internet of Things, Data and Cloud Computing (ICC'17), Cambridge, UK*, pages 104:1–104:5. ACM, March 2017.

[42] F. Kobayashi and J. R. Talburt. Decoupling Identity Resolution from the Maintenance of Identity Information. In *Proc. of the 11th International Conference on Information Technology: New Generations (ITNG'14), Las Vegas, Nevada, USA*, pages 349–354. IEEE, April 2014.

[43] A. Kostopoulos, E. Sfakianakis, I. Chochliouros, J. S. Pettersson, S. Krenn, W. Tesfay, A. Migliavacca, and F. Hörandner. Towards the Adoption of Secure Cloud Identity Services. In *Proceedings of the 12th International Conference on Availability, Reliability and Security (ARES'17), Reggio Calabria, Italy*, pages

90:1–90:7. ACM, August 2017.

[44] D. Kumar Srivastava, B. Roychoudhury, and H. Vardhan Samalia. Importance of User's Profile Attributes in Identity Matching Across Multiple Online Social Networking Sites. In *Proc. of the 8th International Conference on Cloud Computing, Data Science Engineering (Confluence'18), Noida, India*, pages 14–15. IEEE, January 2018.

[45] S. Lee, J. P. Jeong, and J.-S. Park. DNSNA: DNS name autoconfiguration for Internet of Things devices. In *Proc. of the 18th International Conference on Advanced Communication Technology (ICACT'16), PyeongChang, Korea*, pages 1–1. IEEE, January 2016.

[46] N. Lord. Uncovering Password Habits: Are Users' Password Security Habits Improving? (Infographic), September 2020. `https://digitalguardian.com/blog/uncovering-password-habits-are-users-password-security-habits-improving-infographic` [Online; accessed on March 22, 2021].

[47] P. J. Lu, L.-Y. Yeh, and J.-L. Huang. An Privacy-Preserving Cross-Organizational Authentication/Authorization/Accounting System Using Blockchain Technology. In *Proc. of the 31st International Conference on Communications (ICC'18), Kansas City, Missouri, USA*, pages 1–6. IEEE, May 2018.

[48] M. P. Machulak, E. L. Maler, D. Catalano, and A. van Moorsel. User-Managed Access to Web Resources. In *Proc. of the 6th ACM Workshop on Digital Identity Management (DIM'10), Chicago, Illinois, USA*, pages 35–44. ACM, October 2010.

[49] P. Mahalle. *Identity Management Framework for Internet of Things*. PhD thesis, Aalborg University, January 2014.

[50] E. Maler. Extending the Power of Consent with User-Managed Access: A Standard Architecture for Asynchronous, Centralizable, Internet-Scalable Consent. In *Proc. of the 2015 IEEE Symposium on Security and Privacy Workshops (SPW'15), San Jose, California, USA*, pages 175–179. IEEE, May 2015.

[51] A. Othman and J. Callahan. The Horcrux Protocol: A Method for Decentralized Biometric-based Self-sovereign Identity. In *Proc. of the 28th International Joint Conference on Neural Networks (IJCNN'18), Rio de Janeiro, Brazil*, pages 1–7. IEEE, July 2018.

[52] A. Othman and J. Callahan. *The Horcrux Protocol: A Distributed Mobile Biometric Self-sovereign Identity Protocol*, pages 355–377. Springer-Verlag, September 2019.

[53] D. Pöhn. Topology of Dynamic Metadata Exchange via a Trusted Third Party. In *Proc. of the 3rd Open Identity Summit, Berlin, Germany*, pages 101–113. GI, November 2015.

[54] D. Pöhn and W. Hommel. An Overview of Limitations and Approaches in Identity Management. In *Proc. of the 15th International Conference on Availability, Reliability and Security (ARES'20), Virtual Event, Ireland*, pages 1–10. ACM, August 2020.

[55] D. Pöhn, S. Metzger, and W. Hommel. Géant-TrustBroker: Dynamic, Scalable Management of SAML-Based Inter-federation Authentication and Authorization Infrastructures. In *Proc. of the 29th IFIP International Information Security Conference (SEC'14), Marrakech, Morocco*, pages 307–320. Springer-Verlag, June 2014.

[56] C. Ribeiro, H. Leitold, S. Esposito, and D. Mitzam. STORK: A Real, Heterogeneous, Large-scale eID Management System. *International Journal of Information Security*, 17(5):569–585, October 2018.

[57] J. Richer and L. Johansson. Vectors of Trust. IETF RFC 8485, October 2018. `https://www.ietf.org/rfc/rfc8485.txt` [Online; accessed on March 22, 2021].

[58] H. Roßnagel. A Mechanism for Discovery and Verification of Trust Scheme Memberships: The Lightest Reference Architecture. In *Proc. of the 5th Open Identity Summit, Karlstad, Sweden*, pages 81–92. GI, October 2017.

[59] H. Roßnagel and S. Wagner. LIGHTest. *Datenschutz und Datensicherheit - DuD*, 43(4):220–224, April 2019.

[60] M. Schanzenbach and C. Banse. Managing and Presenting User Attributes over a Decentralized Secure Name System. In *Proc. of the 11th Data Privacy Management and Security Assurance Workshop (DPM'16), Heraklion, Crete, Greece*, volume 9963 of *Lecture Notes in Computer Science*, pages 213–220. Springer-Verlag, November 2016.

[61] M. Schanzenbach, C. Banse, and J. Schütte. Practical Decentralized Attribute-Based Delegation Using Secure Name Systems . In *Proc. of the 17th International Conference on Trust, Security and Privacy in*

Computing and Communications (TrustCom'18), New York, New York, USA, pages 244–251. IEEE, August 2018.

[62] M. Schanzenbach, G. Bramm, and J. Schütte. reclaimID: Secure, Self-Sovereign Identities Using Name Systems and Attribute-Based Encryption. In *Proc. of the 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications (TrustCom'18), New York, New York, USA*, pages 946–957. IEEE, August 2018.

[63] L. Seitz, S. Gerdes, G. Selander, M. Mani, and S. S. Kumar. Use Cases for Authentication and Authorization in Constrained Environments. IETF RFC, January 2016. `https://www.ietf.org/rfc/rfc7744.txt` [Online; accessed on March 22, 2021].

[64] Shibboleth. Project Roadmap, January 2021. `https://wiki.shibboleth.net/confluence/display/DEV/Project+Roadmap` [Online; accessed on March 22, 2021].

[65] A. Slomovic. Privacy Issues in Identity Verification. *IEEE Security Privacy*, 12(3):71–73, May 2014.

[66] K. Speck. Independent, Federated Digital Identity Management Solution ID4me Announces Public Beta at CloudFest 2019, May 2019. `https://id4me.org/independent-federated-digital-identity-management-solution\-id4me-announces-public-beta-at-cloudfest-2019/` [Online; accessed on March 22, 2021].

[67] M. Steichen, B. Fiz, R. Norvill, W. Shbair, and R. State. Blockchain-Based, Decentralized Access Control for IPFS. In *Proc. of the 8th IEEE/ACM International Conference on Cyber, Physical and Social Computing (CPSCom'18) Green Computing and Communications (GreenCom'18), Halifax, Nova Scotia, Canada*, pages 1499–1506. IEEE, July 2018.

[68] Q. Stokkink and J. Pouwelse. Deployment of a Blockchain-Based Self-Sovereign Identity. In *Proc. of the 8th IEEE/ACM International Conference on Cyber, Physical and Social Computing (CPSCom'18) Green Computing and Communications (GreenCom'18), Halifax, Nova Scotia, Canada*, pages 1336–1342. IEEE, July 2018.

[69] M. Takemiya and B. Vanieiev. Sora Identity: Secure, Digital Identity on the Blockchain. In *Proc. of the 42nd Annual Computer Software and Applications Conference (COMPSAC'18), Tokyo, Japan*, pages 582–587. IEEE, July 2018.

[70] A. Tobin and D. Reed. The Inevitable Rise of Self-Sovereign Identity, March 2017. `https://sovrin.org/wp-content/uploads/2018/03/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf` [Online; accessed on March 22, 2021].

[71] J. Torres, M. Nogueira, and G. Pujolle. A Survey on Identity Management for the Future Network. *IEEE Communications Surveys & Tutorials*, 15(2):787–802, February 2013.

[72] K. Toth and A. Anderson-Priddy. Self-Sovereign Digital Identity: A Paradigm Shift for Identity. *IEEE Security Privacy*, 17(3):17–27, May 2019.

[73] D. van Thuan, P. Butkus, and D. van Thanh. A User Centric Identity Management for Internet of Things. In *Proc. of the 2nd International Conference on IT Convergence and Security (ICITCS'14), Beijing, China*, pages 1–4. IEEE, October 2014.

[74] F. Veseli, J. S. Olvera, T. Pulls, and K. Rannenberg. Engineering Privacy by Design: Lessons from the Design and Implementation of an Identity Wallet Platform. In *Proc. of the 34th ACM/SIGAPP Symposium on Applied Computing (SAC'19), Limassol, Cyprus*, pages 1475–1483. ACM, April 2019.

[75] C. Wang, S. T. Jan, H. Hu, D. Bossart, and G. Wang. The Next Domino to Fall: Empirical Analysis of User Passwords across Online Services. In *Proc. of the 8th ACM Conference on Data and Application Security and Privacy (CODASPY'18), Tempe, Arizona, USA*, pages 196–203. ACM, March 2018.

[76] A. Yakubov, W. M. Shbair, A. Wallbom, D. Sanda, and R. State. A blockchain-based PKI management framework. In *Proc. of the 14th IEEE/IFIP Network Operations and Management Symposium (NOMS'18), Taipei, Taiwan*, pages 1–6. IEEE, April 2018.

[77] Yanjiong Wang and Qiaoyan Wen. A privacy enhanced DNS scheme for the Internet Of Things. In *Proc. of the International Conference on Communication Technology and Application (ICCTA'11), Beijing, China*, pages 699–702. IET, October 2011.

[78] I. Young. Metadata Query Protocol. IETF Internet-draft (work in progress), January 2021. `https://www.ietf.org/archive/id/draft-young-md-query-14.txt` [Online; accessed on March 22, 2021].

[79] Yuan Cao and Lin Yang. A survey of Identity Management technology. In *Proc. of the 1st International Conference on Information Theory and Information Security (ICITIS'10), Beijing, China*, pages 287–293. IEEE, December 2010.

[80] T. Zefferer, D. Ziegler, and A. Reiter. Best of Two Worlds: Secure Cloud Federations meet eIDAS. In *Proc. of the 12th International Conference for Internet Technology and Secured Transactions (ICITST'17), Cambridge, UK*, pages 396–401. IEEE, December 2017.

[81] Z.-K. Zhang, M. C. Y. Cho, Z.-Y. Wu, and S. W. Shieh. Identifying and Authenticating IoT Objects in a Natural Context. *IEEE Computer*, 48(8):81–83, August 2015.

[82] J. Zouari and M. Hamdi. AIDF: An Identity as a Service Framework for the Cloud. In *Proc. of the 3rd International Symposium on Networks, Computers and Communications (ISNCC'16), Yasmine Hammamet, Tunisia*, pages 1–5. IEEE, May 2016.

Author Biography

Daniela Pöhn received a M. Comp. Sc. degree from FernUniversität in Hagen and her Ph.D. degree with focus on identity management from LMU Munich in 2006. Currently she is Senior Researcher at the research institute CODE at the Universität der Bundeswehr München. Her research is mainly on identity management, in particular federated identity management, integration of security management, and level of assurance.

Wolfgang Hommel has held the professorship for Software and Data Security at UniBw M since April 2016 and is the technical director of UniBw M's Cyber Defence and Smart Data Research Institute (FI CODE). Under the guiding principle of implementing and operating secure networked applications, his group focuses its research on the topics of secure coding, security monitoring, and technical security management.