IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 4 September 2022, accepted 22 October 2022, date of publication 3 November 2022, date of current version 22 November 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3219044

RESEARCH ARTICLE

Reference Service Model Framework for Identity Management

DANIELA PÖHN AND WOLFGANG HOMMEL
Research Institute CODE, Universität der Bundeswehr München, 85577 Neubiberg, Germany

Corresponding author: Daniela Pöhn (daniela.poehn@unibw.de)

This work is partly funded by the Bavarian Ministry for Digital Affairs (Project DISPUT/STMD-B3-4140-1-4). The authors alone are responsible for the content of the paper.

ABSTRACT Each person on the Internet typically has several digital accounts, which are associated with different identity information. During the last years, various identity and access management (I&AM) approaches were established to help manage all these digital identities and operate online services within an organization and beyond. This development has led to heterogeneity, making it hard to differentiate between, comply with, and combine these approaches. In this article, we propose a novel reference service model framework for different I&AM flavors designed with the open enterprise modeling language ArchiMate. The proposed identity management service model framework (IMSMF) consists, on the one hand, of a meta-model and several models for various protocols and implementations, and, on the other hand, models, which were designed in a generic service-oriented way. These models lead to a universal model to indicate additional components for an enhanced I&AM. IMSMF has been evaluated through several rounds of expert interviews. IMSMF helps to establish, enhance, and change I&AM systems while also being a base for profound further research.

INDEX TERMS Architecture, identity management, modeling, reference architecture, reference model, service model.

I. INTRODUCTION

A digital identity is a set of attributes used to identify a particular user in order to gain access to resources, such as Internet services. Managing identity across an ever-growing digital services landscape has become a challenging task for security experts. Over the years, different identity and access management (I&AM) systems were introduced and adopted to tackle the growing demand for identities and thereby offered services. Originally, centralized identity management was the first evolutionary step towards one source of truth for all services within an organization. With centralized I&AM, consistent data repositories are made possible, allowing timely provisioning and de-provisioning of users. Often, Single Sign-On (SSO) is implemented, allowing to authenticate once for all services. In order to enable cooperation across organizations' boundaries, either the user data has to be duplicated or federated identity management (FIM) is implemented. With FIM, each user has an identity at a home organization, the so-called identity provider (IdP), which becomes the source of truth for all services within the trust boundary of the federation. In order to enable FIM, IdP and service provider (SP) have to use the same identity management protocol via various possible implementations. Large-scale federations and inter-federations, e. g., eduGAIN and eIDAS, often rely on the Security Assertion Markup Language (SAML) 2.0. Peer-to-peer cooperation is more likely enabled by the protocols Open Authorization (OAuth) 2.0 for authorization and OpenID Connect (OIDC) for authentication. In parallel, more user-friendly approaches including User-Managed Access (UMA) 2.0 were introduced. Even though these user-centric identity management (UCIM) approaches give more control to the user and thus have the potential for more privacy-friendly implementations, providers still can gather data about which SP the user is actually using at what time. In this series, a recently emerging model is Self-Sovereign Identity (SSI), which offers more control and access to users regarding their identity. This feature

The associate editor coordinating the review of this manuscript and approving it for publication was Claudia Raibulet.

represents a major development towards privacy for users. While SSI is often mentioned in the context of distributed ledger technology (DLT), it can also be implemented, e. g., based on traditional public key infrastructures (PKI) instead of blockchains.

For different use cases, one or more models are better suited, leading to several models running in parallel. Whereas these models may sound distinct, they can be combined in several ways [1]. For example, UMA might be used in a FIM or Internet of Things (IoT) setting. Not all combinations are possible though; at the same time, these and other systems may be used for non-person identities. In addition, different products may require specific I&AM systems, leading to a multitude of different solutions within an organization. This heterogeneity makes it cumbersome to differentiate and combine these approaches, as well as to improve the security of the underlying I&AM systems and the underlying identities. The security of systems is though tightly tied to the security of I&AM. In order to get an understanding of the current status of the operated I&AM systems, an overview is required. In order to receive an overview of these complex structures, a systematic approach is required. To address these problems, a reference service model framework for identity management (IMSMF) based on [2] is described in this article. A reference architecture consists of reusable models and patterns, which can be customized, and needs to fulfill the following requirements:

- R1: Reusable architecture for I&AM with generic and universal terminology.
- R2: Systematic overview and detailed perspectives on selected aspects.
- R3: Adaptability to different protocols and use cases.
- R4: Dependencies between different providers with related interfaces, including requirements regarding appropriate service management.

Furthermore, the following research questions, based on [2], are addressed by IMSMF in this article:

- Q1: How to describe I&AM scenarios with a scenario-independent approach?
- Q2: Which elements and technical components are required to fulfill the requirements described above?
- Q3: What is required to adapt the reference architecture to different areas?
- Q4: How can different I&AM models and approaches be combined?
- Q5: Which elements are needed to have a more useful I&AM in place?

The contribution of this article is three-fold: 1) a framework of reference service models for different identity management approaches, 2) a universal identity management model showing combinations of existing approaches, and 3) a model visualizing helpful tools for identity management based on the proposed models. IMSMF is based on the supporting toolkit of Enterprise Architecture by utilizing the open enterprise modeling language ArchiMate as it is the most used modeling approach [3]. The framework is thereby compliant with Information Technology Infrastructure Library (ITIL), NATO Architecture Framework (NAF), Federated Mission Network (FMN), The Open Group Architecture Framework (TOGAF), and further frameworks. All proposed models were evaluated by expert surveys and interviews, as well as their applications to scenarios. To the best of our knowledge, there is no model framework describing this variety of I&AM approaches, their combinations, and helpful tools. This article enhances [2] by an improved reference service model for FIM and Kerberos. It further provides a generic and several well-evaluated use case-specific models, leading to a universal model and a visualization for helpful tools.

This article enhances [2] in several ways. The previous publication established a reference architecture for FIM, which was evaluated based on a use case and the application of Kerberos. IMSMF generalizes the idea in a meta-model and designs reference models for several identity protocols and models. This includes improved versions of both previously published models. In addition, a universal model is proposed to analyze parallel usages. Furthermore, the elevated FIM model serves as the basis to determine additional tools and features for identity management. All models are evaluated and enhanced by several rounds of expert interviews.

This article is structured as follows: After discussing related approaches in Section II, we introduce the meta-model of IMSMF with its key features in Section III. Based on the meta-model, we present reference service models for different protocols and approaches of IMSMF in Section IV. These models are combined to a universal model to identify combinations and missing components in Section V. All models are evaluated by expert interviews in multiple steps in Section VI. Section VII serves as discussion and Section VIII concludes the article by summarizing the content and giving an outlook to future research directions.

II. RELATED APPROACHES

In this section, we give an overview of related modeling approaches for identity management. Generic identity management models are mostly not universal, whereas other approaches concentrate on a single model or aspect. The first step toward IMSMF was proposed by Pöhn and Hillmann [2].

Several approaches and standards try to model generic identity management. The identity models mentioned in Section I are described in a high-level architecture. Whereas the developers of ArchiMate offer a rudimentary approach to identity management, this does not explore the technical possibilities and differences [4]. Elements of reference architectures are described in frameworks and standards, including International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) 24760 [5] and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-3 [6]. The US research and education federation InCommon [7] provides the Trust and Identity in Education and Research (TIER) / Trust Access Platform (TAP) reference architecture for its members.

Although these are standards, they are currently neither up-to-date nor universal.

Other approaches focus on a specific model. The reference design of LetMeAccess by Perroud and Inversini [8] provides different views on centralized I&AM architecture without following official meta-models. The company IDPro [9] published its own reference architecture. The architecture is modeled with the Unified Modeling Language (UML) and based on official frameworks and standards. Nonetheless, it only features their own reference architecture. The reference architecture for FIM by Dabrowski and Pacyna [10] applies no official meta-model, whereas Gaedke et al. [11] design selected aspects of FIM. While some ideas of these models can be used, they are not universally applicable. Pöhn and Hommel [12] utilize the classic Munich Network Management (MNM) service model [13] for describing FIM. Although this service model clearly distinguishes different views and stakeholders, it is not a modern approach and it solely focuses on FIM. Liu et al. [14] and Eddine et al. [15] concentrate on SSI without applying an official meta-model, whereas others, e. g., Grüner et al. [16], make use of different models for their own approach. Even though SSI is still progressing, applying a meta-model could facilitate progress.

In addition, specific aspects of I&AM are modeled by several authors. Yang et al. [17] and Katsikogiannis et al. [18] focus on the process of authentication and authorization. Amaral et al. [19] visualize the aspect of trust with ArchiMate. Similar models exist as pattern for resource and capabilities [20], services [21], and security object relationships [22] for ArchiMate. Zwattendorfer et al. [23] provide a reference architecture for trust-based digital ecosystems. These specific aspects can be applied in more generic models. In summary, no approach is universal and at the same time up-to-date. Nonetheless, they can be used as a basis.

III. META MODEL FOR IDENTITY MANAGEMENT

A reference architecture consists of reusable models and patterns, which are adaptable and customizable. Thereby, organizations can refer to it when adapting or improving identity management. The designed reference architectures offer overviews from different hierarchy levels and several more detailed perspectives. ArchiMate is the most used modeling approach for enterprise architectures, highlighting mainly the design and structure of a system. It supports the description, analysis, and visualization of architectures in a generic way. ArchiMate applies different notions, summarized in Fig. 12 in Appendix C. According to ArchiMate's approach, the overview consists of different layers to differentiate roles from business, applications, and technology. The reference architecture consists of an external layer, business service layer, business layer, application service layer, application layer, and the technical service layer. Hence, a clear distinction in the respective layer can be made:

- **External Layer:** This highest layer describes the internal and, if available, external actors, i. e., the users (human or devices), which want to interact by accessing a service.
- **Business Service Layer:** This layer shows the internal and, if available, external usage by the users. The layer helps to separate the internal structure and organization from the external) observable behavior expressed at the service layer.
- **Business Layer:** This layer includes actors, roles, collaborations, and interfaces regarding the provided services, which interact by processes, functions, events, and services. They represent elements with relevance from a business perspective.
- **Application Service Layer:** This layer is built upon the application layer and shows accessible services as well as interfaces for other entities and users.
- **Application Layer:** This layer gives an overview of the application layer concepts, describing different application components, software, and interfaces, and their relationships. In order to provide the required services, several software components need to be implemented. For example, a web service requires a web application, running on a web server, belonging to the technical service layer.
- **Technical Service Layer:** This bottom layer consists of the physical layer with the actual hardware with nodes, devices, infrastructure interfaces, communication paths, and networks.

In order to explain the approach, an introductory example of an online shopping account is featured in Fig. 1 and described next:

- **External Layer:** The business actor customer is assigned to the business role user, who uses (is associated with) a client application such as a web browser to access an online shopping service. As the client application is required for access, it is a requirement. The IdP previously created an account for the user with the digital identity. Depending on the required level of trust for the service, the IdP may perform an initial identity check using appropriate identification procedures for initial identification. This may be the case for eID and bank account services. Web services typically have no or lower trust verification methods. For authentication, the user makes use of the underlying I&AM system. Also, depending on the required trust, the user may require further authentication methods. This may be the case for the online shopping service, as the user's address and payment information are stored. The role user is associated with the meanings of digital identity and permissions, which are linked with the identity. The user roles and inherited permissions are assigned according to the role within the associated organization. For example, an administrator received more permissions than a regular user. Each user can take on different roles, identities, and permissions in relation to tasks. In the example, users are allowed to edit their accounts, buy items, and follow the shipping process.

- **Business Service Layer:** The user accesses the service via the business process access management, i. e., some kind of login screen. The user identifies themselves by different methods. Common authentication means are username and password. Increasingly, a second factor is required. The business service of authentication and authorization (AuthNZ) broker triggers the access management process. This broker offers different authentication and authorization methods, such as the already stated username and password, but also "Login with Google" or "Login with Facebook". The core business is extended by the business collaboration third party AuthN Broker, which manages trusted third parties (TTPs). These TTPs may include Google and Facebook. For this purpose, appropriate collaboration agreements are negotiated beforehand, ranging from formal contracts to simple configurations. In the case of Google and Facebook, services need to be preregistered. Hence, the third-party AuthN Broker serves the AuthNZ broker.
- **Business Layer:** The business layer represents elements with relevance from a business perspective. It describes the business view, enabling different login options as the main service provided to the end-user. This is represented as the business function AuthNZ possibilities, which serves the AuthNZ broker. This process typically has several quality of service (QoS) parameters, which the provider needs to fulfill internally or/and externally. AuthNZ is only provided to or by externals if they have a mutual agreement. In order to be able to provide these previously described login options, TTP processes are required. These enable trust establishment, either directly or via an independent party. Participating entities may have requirements regarding security management, commonly described by level of assurance (LoA), depending on the required trust. LoA is the quantification of factors leading to confidence in an entity and its underlying processes, which can be stated in identity protocols. In the case of the online shop, the registration has a two-step process requiring different elements. The business process can trigger the AuthNZ possibilities and discovery service, especially if changes occur. At the same time, the TTP process serves the TTP AuthN Broker.
- **Application Service Layer:** The main service is the online service, where users need to authenticate in order to shop. The login screen is featured by the application service AuthNZ Engine, which enables the discovery of the third parties service. The login with online social networks is typically hard-coded, whereas the discovery within large-scale inter-federations, e. g., eduGAIN, requires a long list of the possible identity providers. Thereby, the user is able to authenticate not only by username and password but also TTPs, e. g., Google and Facebook. The web service itself is triggered by the AuthNZ service interface, which also triggers the implementation service for managing user credentials. The service thereby uses different protocols. In our scenario, it is most likely some representational state transfer REST) interface for internal user management and at least OAuth towards Google and Facebook.
- **Application Layer:** In order to provide an online service, the service itself as well as the user management are required. The web service requires a web application, running on a web service. Thereby, the application server realizes the application. The core element for I&AM is the user management, i. e., the function of managing user credentials. The user management interacts with the service via different protocols. The user information is often either stored in a database, active directory (AD), or a lightweight directory access protocol (LDAP) implementation. For the scenario, it is most likely a database. Within the database, users can be granted different permissions depending on their roles. While customers may only be able to edit their account settings, employees can edit goods, which are sold. Thereby, the implementation interaction) triggers the component database, whereas it is serving the functionality of managing user credentials. In a distributed setting, services can enable more fine-grained permissions locally.
- **Technical Service Layer:** Separate servers are provided for the various applications. This differentiation makes the various servers visible, helping to implement specific security requirements while taking the idea of microservice architecture into account. The data for the user management is stored in some sort of user repository. In addition, at least an application service is required for having the service up and running. Both services are made available as infrastructure- or platform-as-a-service, which is a service as well. Therefore, the infrastructure is serving the respective servers.

As visible in the figure, ArchiMate uses different colors to better differentiate the different layers and functions. In addition, various symbols further detail the actors, functions, and interfaces. The same applies for arrows between the symbols. The names for these elements are applied in the description. An overview of the different meanings is shown in Fig. 12, displayed in Appendix A.

IV. IDENTITY MANAGEMENT SERVICE MODEL FRAMEWORK

In this section, a meta-model is applied to the most important protocols, identity models, and use cases in order to provide a comprehensive set of models for IMSMF:

- PAM: Section IV-A
- Kerberos: Section IV-B
- LDAP: Section IV-C
- IoT: Section IV-D
- FIM: Section IV-E
- UMA: Section IV-F
- SSI: Section IV-G

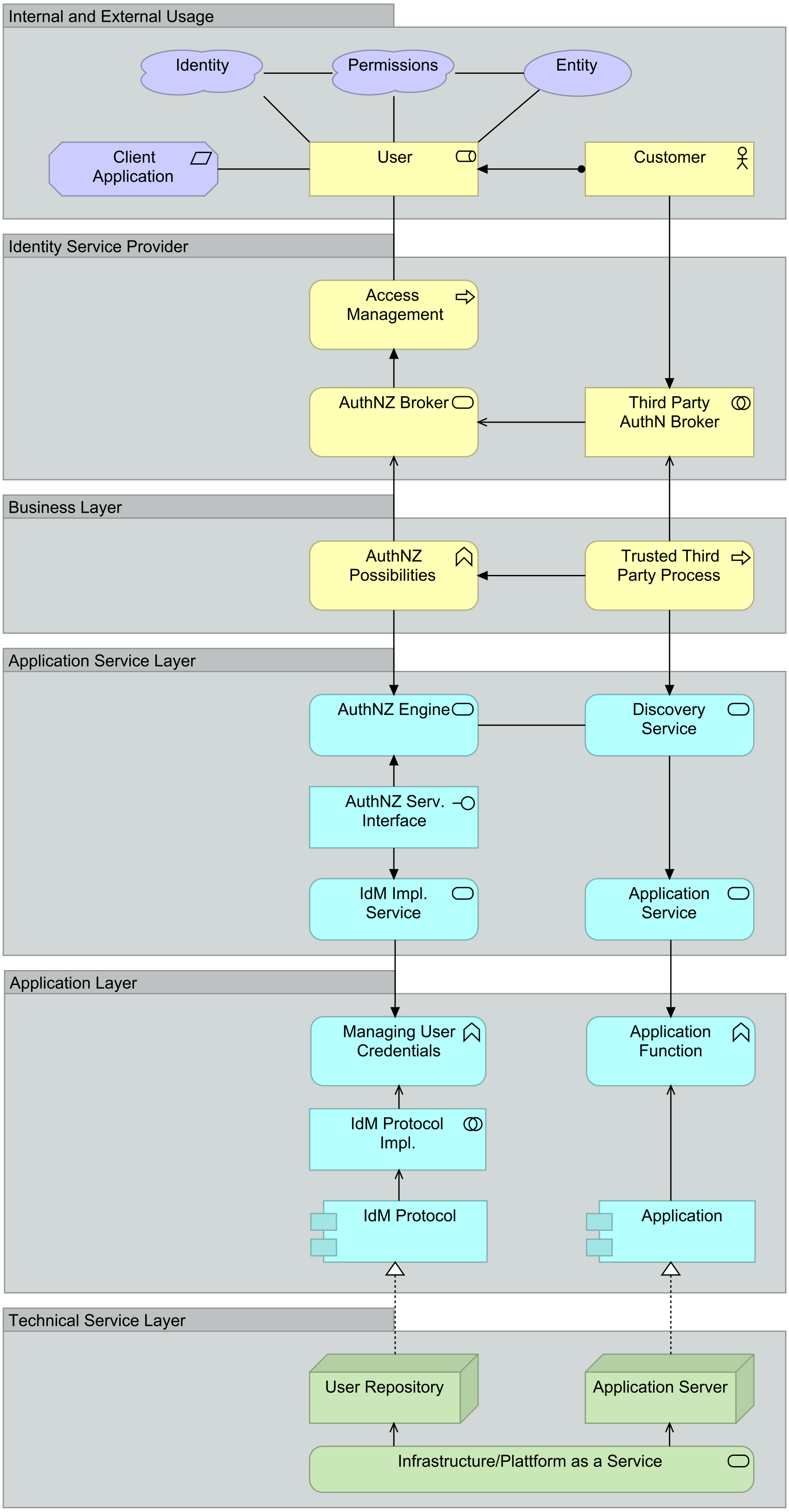

FIGURE 1. Generic identity service model.

A. PAM

A pluggable authentication module (PAM) is a mechanism to integrate multiple authentication schemes into an application programming interface (API). PAM thereby allows programs that rely on authentication to reuse these authentication schemes while being independent of them. Hence, PAM separates the tasks of authentication from applications. Instead of requiring each application developer to rewrite the authentication check for each new method, PAM for checking the authentication is embedded. Since no central standard of PAM behavior exists, there were some attempts to standardize it. The X/Open SSO (XSSO) standard is not ratified but is used by several PAM implementations, e. g., OpenPAM, which is an alternative to Linux PAM. Linux PAM is a suite of libraries that allow system administrators to configure authentication methods for users. The authentication methods include local passwords, LDAP, and fingerprint readers. Thereby, a PAM framework consists of at least a library, pluggable modules, and configuration files. In the following, PAM shown in Fig. 2 is described for Linux servers:

- **External Layer:** This layer consists of users with a client application for authentication. The client application is a requirement for accessing a service, whereas PAM is invisible to the user. For example, a user logs into a text-based console. The login application prompts for a username and password, making a `libpam` authentication call.
- **Business Service Layer:** To authenticate the user, the AuthNZ broker is triggered. The AuthNZ broker applies policies, e. g., checking who the user is and if the user is allowed to connect.
- **Business Layer:** The authentication process with QoS parameters is described by the authentication possibilities. Depending on the configured modules, different authentication methods are possible. This may include fingerprint with `pam_fprintd`.
- **Application Service Layer:** The AuthNZ engine is triggered by the AuthNZ possibilities. The main service for users and servers, i. e., authentication and authorization, is provided by PAM via its APIs. `pam_unix` is responsible for checking the local account authentication. Other modules may also be used. The result of the authentication is passed back to the login process. If the login process is continuing at this point, a session for the user is created. On logout, the session is closed and another session call to `libpam` is made.
- **Application Layer:** PAM has several interfaces, for example with LDAP, to enable authentication and authorization for users. In addition, interfaces to different applications, which require PAM, exist. PAM itself needs configuration and the integration of several modules. Each module or service requires its own configuration. For example, `/usr/lib64/security` has a collection of different PAM libraries performing various checks. The configuration files are located at `/etc/pam.d`, whereas additional security configuration files can be found in `/etc/security`.
- **Technical Service Layer:** This layer consists of the various servers required for the scenario. As a standard setup, the servers LDAP, PAM, and application are shown, which are operated based on infrastructure.

B. KERBEROS

Kerberos [24] is a computer network authentication protocol working based on tickets. These tickets allow nodes communicating over a non-secure network to prove their identity in a secure manner. Thereby, the design aims at a client-server model with mutual authentication. Kerberos utilizes symmetric-key cryptography and requires a TTP. Originally, Kerberos was developed by MIT. In 2005, the Internet Engineering Task Force (IETF) updated the Kerberos specification. Starting with Windows 2000, Microsoft uses Kerberos as their default authentication method. Joining a client to a Windows domain means enabling Kerberos for authentication. NT LAN Manager (NTLM) is used as a fallback. Many UNIX-like operating systems (OSs) include software for Kerberos authentication of users or services. The reference architecture, shown in Fig. 3, consists of the following layers:

- **External Layer:** This layer consists of users with a client application for authentication. The user triggers the client authentication. Therefore, the client sends a cleartext message of the user ID to the Kerberos authentication server (KAS). The answer of KAS helps to authenticate itself to the Ticket-Granting-Server (TGS).
- **Business Service Layer:** With the ticket-enhanced authentication, SSO is made available. In order to enable mutual trust, keys need to be exchanged.
- **Business Layer:** The authentication process with its quality of service parameters is described by the authentication engine requiring trust. The KAS checks to see whether the client is in the database. If so, the KAS generates the secret key by hashing the password of the user found in the database (e. g., AD) and sends it back to the client with the client/TGS session key and the ticket-granting-ticket (TGT). The TGS validates the TGT. If the TGT is valid, then a service ticket (ST) for the client is created. This ST is then sent from the client to the host server, which gives the client access to the requested service.
- **Application Service Layer:** The main service for users and servers, i. e., authentication is provided by Kerberos tickets. In order to provide this service, the endpoints have to be discovered.
- **Application Layer:** Kerberos is typically integrated into a software, e. g., AD. AD makes use of further protocols and can be combined with FIM.
- **Technical Service Layer:** AD requires several server applications running on Windows servers, including LDAP, Domain Name System (DNS), Key Distribution Center (KDC), consisting of TGS and KAS.

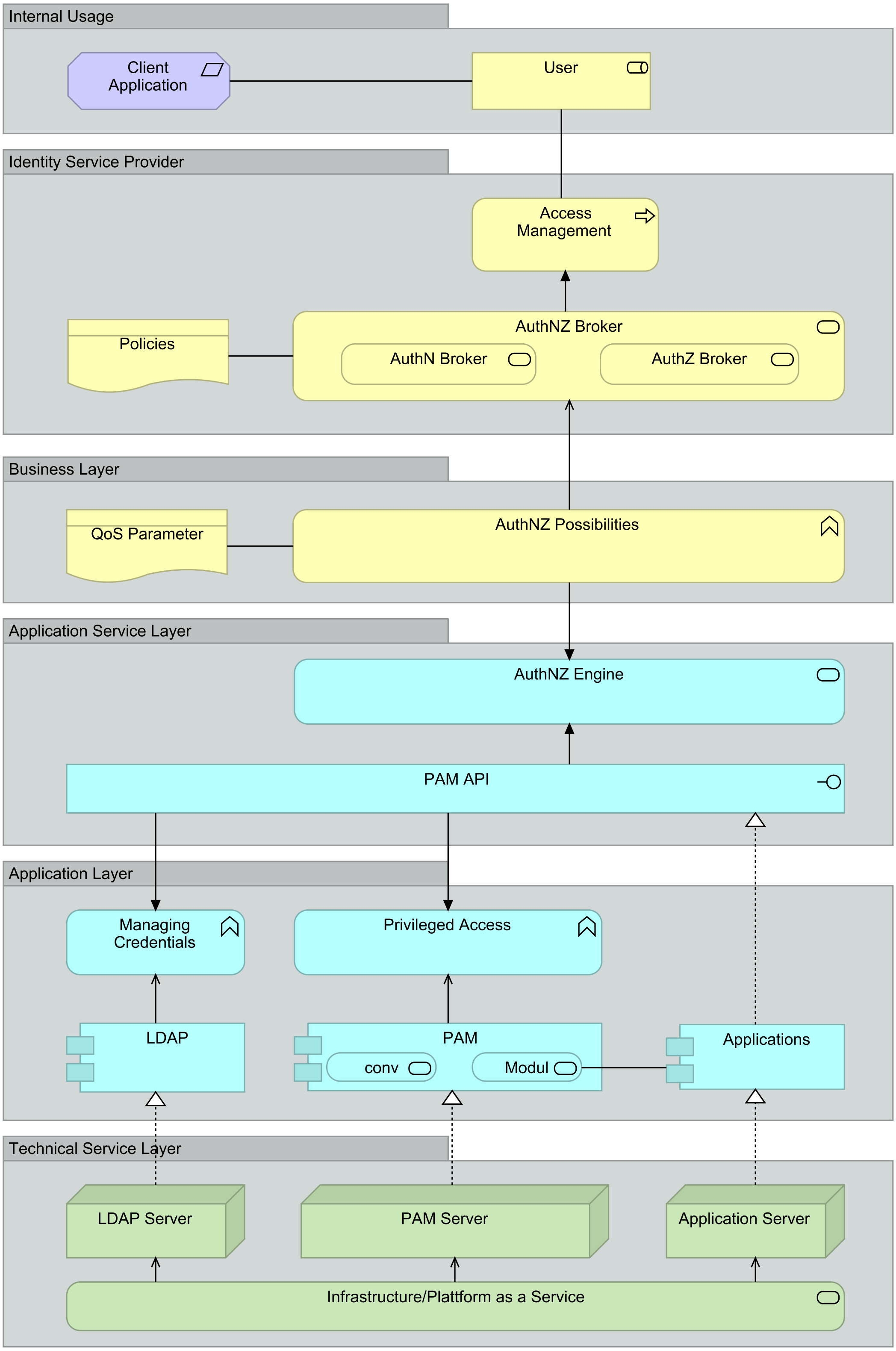

FIGURE 2. Reference model for PAM.

The authentication server forwards the username to KDC, which then issues a ticket-granting ticket, stamped and encrypted by TGS. Even though AS and TGS can be installed on different systems, they often are on a single server. In order to have the same system time on all systems, the network time protocol (NTP) is typically utilized. Kerberos is also possible without AD.

C. LDAP

LDAP is a protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network. Thereby, directory services allow the sharing of information about users, systems, networks, services, and applications throughout the network. This information is typically hierarchically structured. The protocol follows the 1993 edition of the X.500 model: an entry consists of a unique identifier and a set of attributes with names and values. These attributes are defined in a schema. LDAP is specified by the IETF and typically stores the usernames and passwords of its users. This allows different applications, e. g., Docker, OpenVPN, and Samba server, to connect to the LDAP server to validate users. OpenLDAP is an open-source implementation, typically installed on Linux distributions. It consists of four main components: `slapd` (standalone daemon), `lloadd` (standalone load balancing proxy), libraries implementing the LDAP protocol and basic encoding rules, and client software. With these components, OpenLDAP enables the search for, modification, and deletion of entries, including passwords. Other LDAP implementations include AD, Red Hat Directory Servers, and IBM Tivoli Directory Servers. This shows that LDAP, visualized in Fig. 4, is often used by other services for AuthNZ:

- **External Layer:** The end-user wants to access a service via a client application for authentication. Authentication is a bind operation, which establishes the authentication state for a session.
- **Business Service Layer:** The user needs to authenticate to a service, triggering the AuthNZ broker. The client at some point has to start an LDAP session by connecting to the LDAP server, also called Directory System Agent. The client then sends the request to the server and the server sends the response in return. SSO might be implemented. Additionally, policies such as password policy state and other constraints might be deployed.
- **Business Layer:** The authentication engine enables the authentication.
- **Application Service Layer:** The main service for users and servers, i. e., authentication and authorization, is provided via an LDAP integration by the LDAP client. The counterpart is the LDAP server, which returns a `success` result after successful authentication. If the client for example attempts to bind with incorrect credentials (e. g., wrong password), then the process fails with an `invalidCredentials` result.
- **Application Layer:** The users are managed by LDAP, which might utilize a management interface. The users are LDAP entries, i. e., objects, consisting of a collection of information (so-called attributes).
- **Technical Service Layer:** This layer consists of the servers required for the scenario.

D. INTERNET OF THINGS (IoT)

IoT is experiencing growth in the consumer and business environment. Besides users and applications, all these IoT devices have a digital identity, which needs to be managed and may be connected to a network. This new identity ecosystem is sometimes also referred to as Identity of Things (IDoT). With things, traditional multi-factor authentication (MFA) is not always feasible. Hence, different standardization efforts, such as the IETF Authentication and Authorization for Constrained Environments (ACE) working group, try to improve the current state. Whereas centralized I&AM is used to streamline and enhance the security of the digital identities of human users, the management of IoT devices involves several devices and relationships between devices, applications, data, and users. For example, this can be done by vendor-specific or open-source provisioning platforms. At the same time, several enterprise I&AM systems try to include IoT devices or offer I&AM platforms similar to the usual enterprise solutions. Last but not least, different standards such as Long Range Wide Area Network (LoRaWAN) require various functionality. Fig. 5 shows the management of IoT devices with enterprise I&AM, which uses a similar principle to the other possibilities:

- **External Layer:** The users want to access a service via a client application for authentication. With IoT devices, the user can either be a human end-user, an IoT device, an application, or data.
- **Business Service Layer:** The user needs to authenticate to or access a service via the application interface. This may be restricted by policies. In order to use a service, a process broker may be enabled, having a service catalog of possible services.
- **Business Layer:** Services are made available via the service possibilities, which have QoS parameters. The services may be enabled by business connectors, which feature business models.
- **Application Service Layer:** The main service is made available by the IoT hub service engine, which helps to manage devices and applications. This engine has an interface, used for processing, speaking I&AM protocols, and communicating with the devices (i. e., nodes, gateways).
- **Application Layer:** The I&AM platform provides IoT possibilities, including an IoT broker with the implementation of protocols and the implementation of processing functionality. The interfaces are then based on different components: web application, database management system (DBMS), IoT processing, LDAP, storage, and the IoT components themselves. The IoT components again may use different means of communication.
- **Technical Service Layer:** This layer consists of the servers required for the scenario. The IoT components are further divided into devices and gateways, which build the IoT infrastructure. Most likely, the services are hosted in a cloud infrastructure.

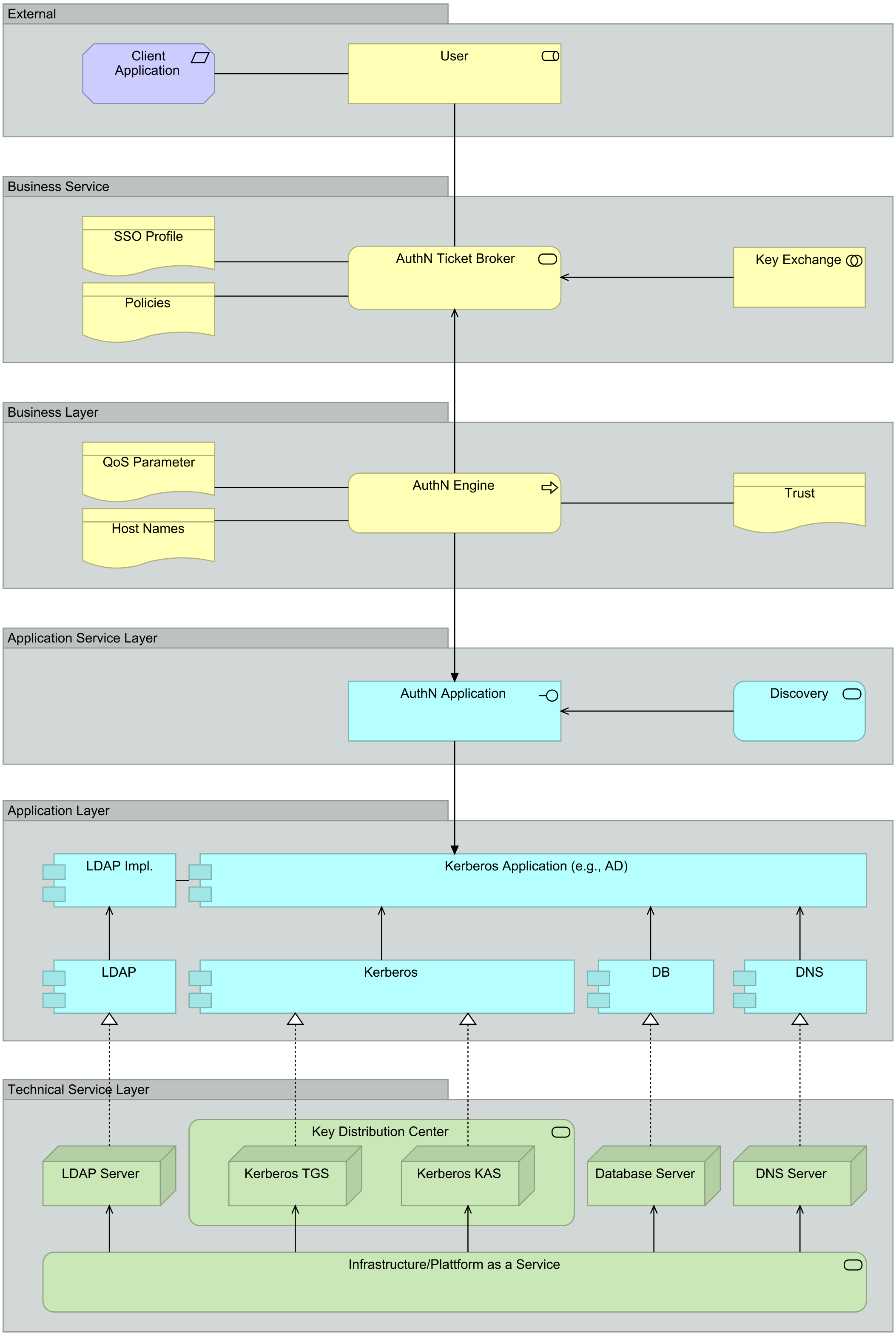

FIGURE 3. Reference model for Kerberos.

E. FEDERATED IDENTITY MANAGEMENT

FIM is an arrangement between multiple entities to enable their users to use the same identification data to access all their services. These partners are thereby part of a trust domain, which can range from a business unit to a branch of industry and egovernment in a nation. For FIM to work

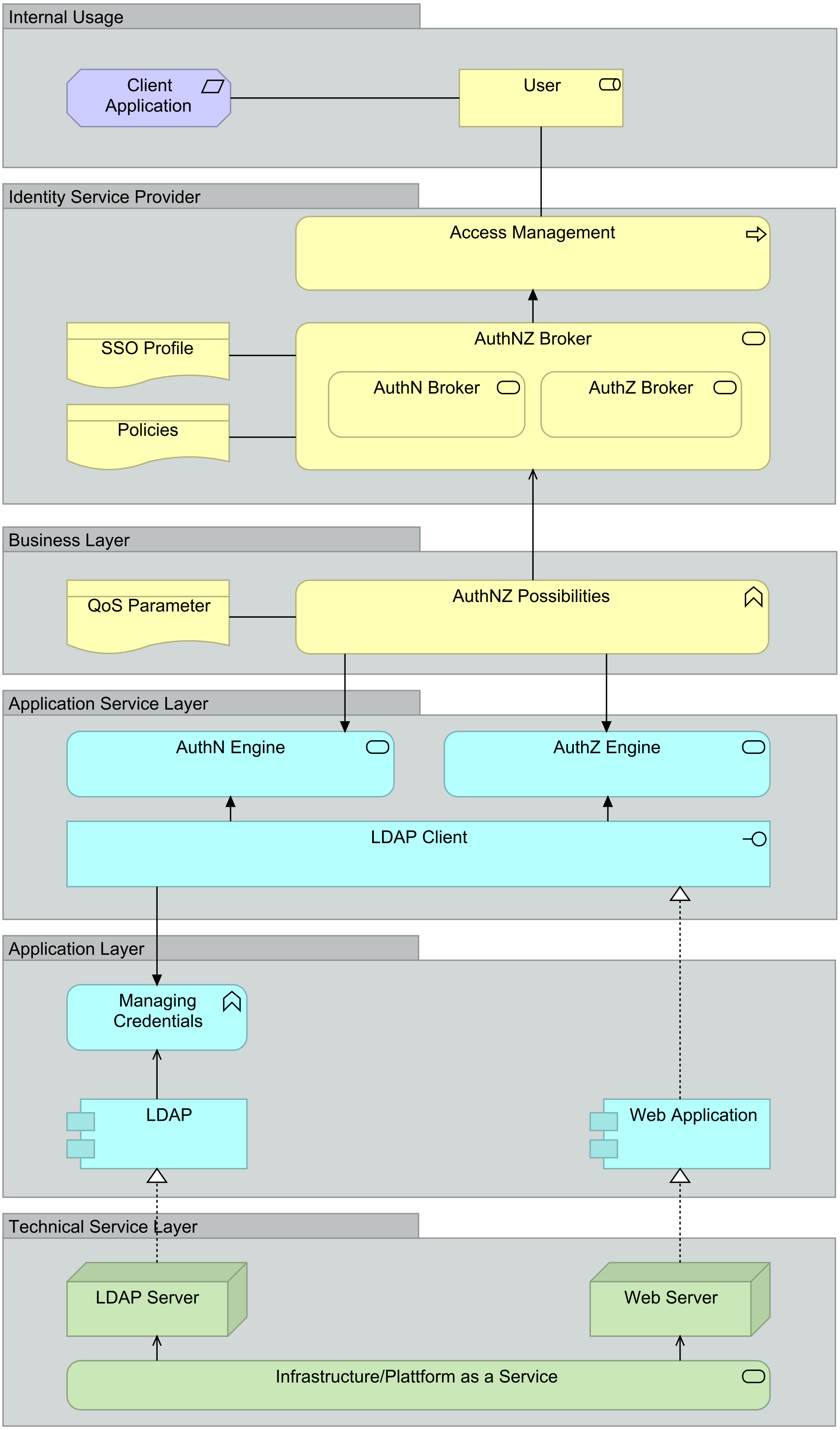

FIGURE 4. Reference model for LDAP.

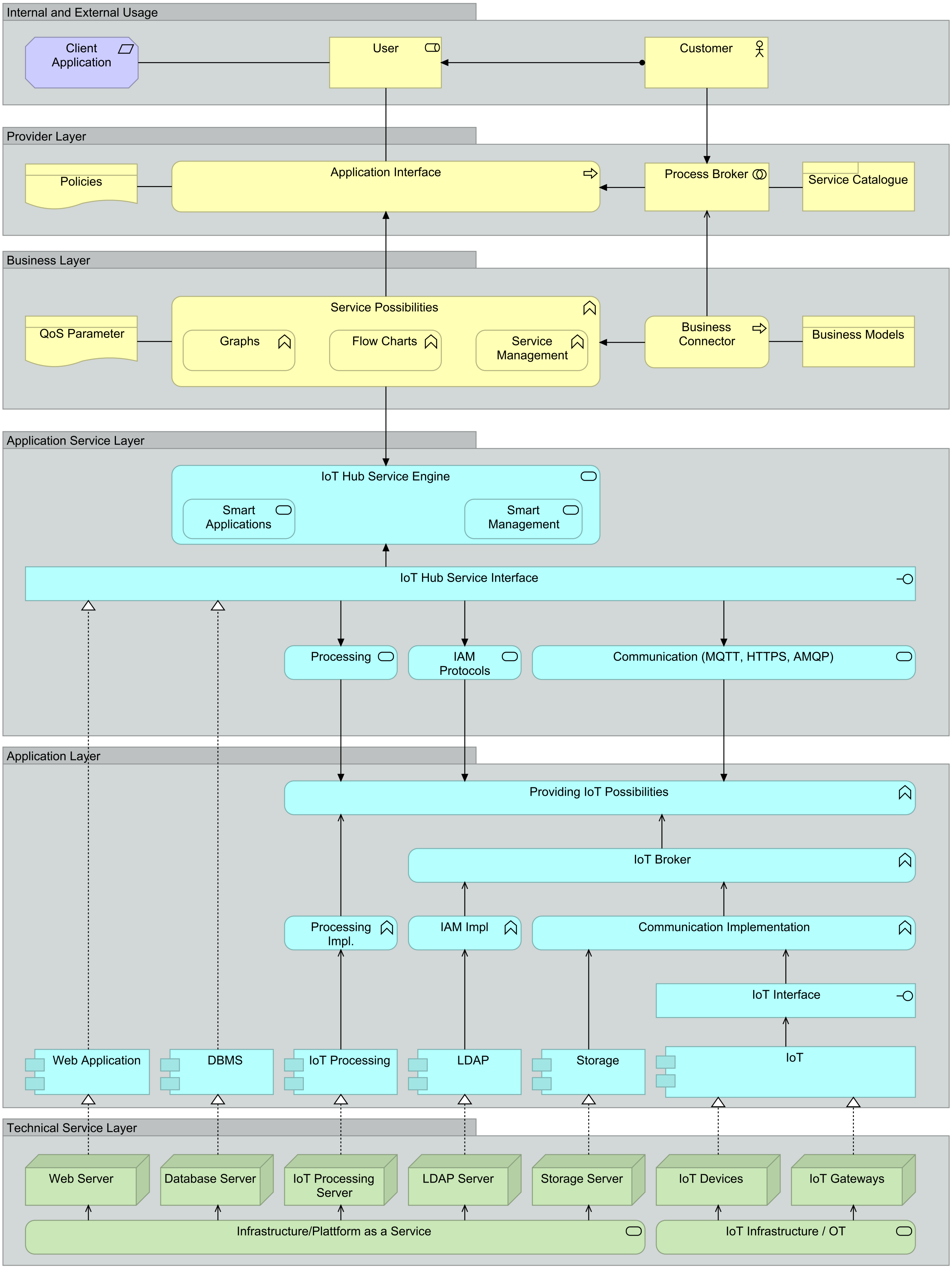

FIGURE 5. Reference model for IoT based on I&AM.

effectively, all involved entities must have a kind of mutual trust, a common set of policies and practices as well as use the same protocol/specification. I&AM with SSO enables users to use a single set of credentials to access multiple systems within a single organization, whereas FIM enables users to access systems across federated organizations. Therefore, several entities are involved in workflows. FIM is typically enabled by the protocol SAML or the combination OAuth and OIDC, as described in Section I.

SAML [25] is an eXtensible Markup Language (XML)-based open standard for exchanging authentication and authorization data between entities. The specification defines three roles: the end-user, the IdP, and the SP. The SP requests and obtains so-called assertions from the IdP. On their basis, the SP can make access control decisions. SAML does not specify the authentication method. The IdP may use a username and password or some other form of authentication, depending on the infrastructure in place. Thereby, SAML builds upon existing services, such as LDAP and AD. The protocol is implemented by different software, including AD and the open-source implementation Shibboleth.

OAuth [26] is an open standard for access delegation, i. e., authorization. Commonly, it is applied for users to grant applications access to their information on another application without giving them their passwords. This mechanism is used by major companies such as Amazon, Google, and Meta, to permit users to share information about their accounts with third-party applications. OAuth provides specific authorization flows for web applications, mobile phones, etc. These flows involve the roles resource owner, which is the end-user, a client application, resource server, and authorization server. The client application wants to access a resource. Therefore, it first asks for authorization from the user. Next, the application receives an access token by the authorization server. This access token is used by the application to access the resource. Similar to SAML, OAuth can make use of the existing infrastructure.

OIDC [27] is a decentralized authentication protocol based on OAuth. It allows users to be authenticated by applications using a third-party IdP service in an interoperable and REST-like manner. Thereby, users can securely reuse existing accounts at OAuth providers. In order to utilize OAuth, the framework for communication needs to be in place between the involved entities. These entities include a client and am authorization server. The client, the so-called relying party, sends an authentication and authorization request to the server, i. e., OpenID Provider, which authenticates resp. authorizes the client. With the authorization code, the client can request a token, providing access for the client. The end-user, which is not the client, authenticates via a web browser to the server.

Both protocol families are included in the reference architecture, see Fig. 6, for FIM. Further protocol extensions and input may be included in OAuth Framework resp. OAuth Framework Implementation with the more recent new protocol developments OAuth 2.1 [28] and GNAP [29].

- **External Layer:** The end-user wants to access a service. For authentication, they use I&AM by accessing it via a client application, typically a web browser or smartphone application.
- **Business Service Layer:** Access to the selected services is provided by the process of access management, where users can identify themselves, e. g., with username and password. This triggers the AuthNZ broker, which could subsequently activate the handling of trustworthy third parties. In order to use third parties, some kind of collaboration agreement needs to be in place. The corresponding policies may define the criteria for using the service. Typically, SSO is enabled across the federation. Theoretically, a service catalog could provide an overview of offered services.
- **Business Layer:** The main service AuthNZ has specific QoS parameters a provider needs to fulfill. The handling of external customers is embedded into the TTP process, enabling the trust establishment, e. g., by an agreement or a contract, between the participating parties. These may have requirements regarding security and security management, as estimated by LoA.
- **Application Service Layer:** The web service requests the AuthNZ engine to authenticate the users. In order to do that, the discovery service is started, helping to find the user's home organization. The discovery service is fed by the list of TTPs. The web service itself uses and triggers different protocols, such as SAML and the OAuth framework with REST interfaces. Many web services offer both variants.
- **Application Layer:** The core service provided to other entities and end-users is I&AM with its components for managing user credentials. Different protocols, e. g., SAML or OAuth, and sources of information, such as LDAP or DBMS, can be used for this. AD offers the extension Active Directory Federation Service (ADFS) for federation services. In order to enable more than one service for ADFS, a proxy is needed. An entity is able to run all forms of FIM in parallel but may decide on a specific software, implementation, and protocol. Further extensions and protocol variants can be added.
- **Technical Service Layer:** Separate services are required for the various applications, taking the micro-service architectures into account. The different servers are made available as infrastructure or platform as a service (PaaS) according to the cloud business service model.

F. USER-MANAGED ACCESS

UMA [30] is an OAuth-based access management protocol enabling a resource owner to control the authorization of data sharing and protected-resource access made between online services on behalf of the owner. The protocol optionally uses OIDC for collecting identity claims. One simple example is the sharing of photo albums with family members. The Health

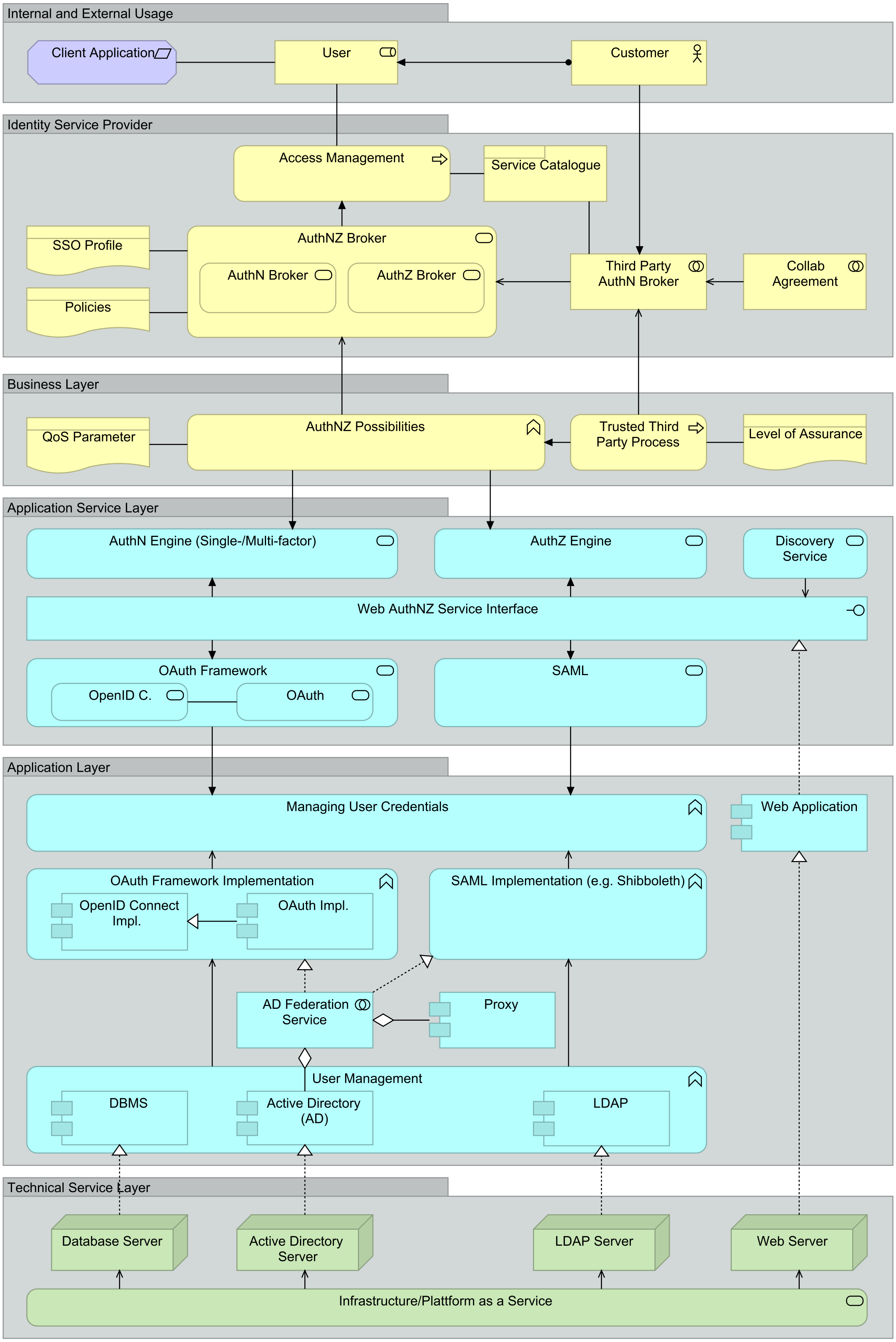

FIGURE 6. Reference model for FIM.

Relationship Trust (HEART) [31] working group applies UMA for a secure sharing of health-related data, enabling individual control of the access. The user can, e. g., distribute medical prescriptions and blood reports to doctors, the health insurance company, and family members depending on preset rules. This allows a privacy-concerned and at the same time flexible sharing of resources based on the decisions of the end-user. In order to utilize UMA, the following roles and underlying software elements are required: a human resource owner (RO), an authorization server (AS), a resource server (RS), and a requesting party (RqP), which makes use of a client (C). The RO manages the RS and sets rules at the AS. The RqP gets authorized by the AS to access the RS. Hence, the RS manages the content for the RO, whereas the AS protects the RS. The reference architecture of UMA, shown in Fig. 7 and based on Fig. 6, is described as follows:

- **External Layer:** The user (RqP) wants to access a resource via a client application (C), i. e., a web browser. In addition, a RO may want to set or modify rules at the AS, also requiring some kind of client application.
- **Business Service Layer:** Access to the selected services (RS resp. AS) is provided by access management at the AS, which triggers the AuthNZ broker. The corresponding UMA policies may refine other policies.
- **Business Layer:** The service AuthNZ has specific QoS parameters a provider needs to fulfill. The same applies to the RS.
- **Application Service Layer:** The main service is the AS, which gives access to the RS. UMA is based on OAuth, therefore this protocol is shown in the figure. Theoretically, it can be applied in parallel to OIDC or with other implementations in combination with SAML.
- **Application Layer:** The main difference is an additional UMA implementation, which is typically in combination with OAuth implementation. UMA hence gives access to the requested data or resource.
- **Technical Service Layer:** Several services are required for the described applications.

G. SELF-SOVEREIGN IDENTITIES

SSI [32] gives the end-user the full control of their digital identities. The SSI model addresses the difficulty of privacy within FIM settings. As the user needs to authenticate at the IdP, the IdP theoretically can aggregate information about which service the user is using when. Thereby, the user is dependent on the information provided by the IdP. In contrast, in SSI the users control the verifiable credentials (VCs) they hold and their consent is required to use those credentials, which were issued by the issuers. This may reduce the unintended sharing of users' personal data. The users, also called holders, generate, manage, and control unique identifiers, i. e., decentralized identifiers (DIDs). A representation of their claims can be shown to service providers, i. e., verifiers. SSI is typically based on decentralized structures, such as decentralized ledger technologies (DLTs) like blockchain. DLTs and blockchains apply different fault-tolerant consensus mechanisms to ensure that the network can agree on a single truth about data states and transactions, and to make certain the consistent state of the network without having to trust a central entity. The current state of the SSI ecosystem is heavily influenced by the first large proponent, the Sovrin Foundation. The research and implementation of the Sovrin Foundation were transferred to the Linux Foundation. Prominent SSI projects are Hyperledger Indy and Aries. As the model SSI is evolving, several aspects are still to be developed. The reference architecture of SSI, shown in Fig. 8, is explained in the following, showing a clear and distinct difference from the reference architecture before:

- **External Layer:** The user (holder) wants to access a service via their wallet with the principle of full control. The data are received as VCs from different issuers. This means that the user can decide whom to give which data. Typically, an agent is involved as well.
- **Business Service Layer:** In contrast to most other protocols, SSI triggers both, the service broker as well as the AuthNZ broker as the user is in control of all their data. The service broker consists of the DID service broker and the credential service broker, providing several service possibilities. Although AuthN and AuthZ are both displayed, AuthZ is towards the verifier to access services, whereas AuthN takes place via the wallet.
- **Business Layer:** In consequence, two main services can be found: general SSI services as well as AuthNZ.
- **Application Service Layer:** In addition to the AuthNZ engine, DID services and credential services are required for SSI. Therefore, the service engine is triggered by DID services and credential services, while AuthNZ engine is in line with credential services and runs on a web application.
- **Application Layer:** In order to provide DID and credential services, smart contracts and different repositories may be operated. For example, smart contracts are optional and not used by Hyperledger. DID services rely on DID documents and schema as well as issuer repository, which both can be on-chain or on the node. Credential services are possible with DID documents and schema, identity and fact data repository, issuer repository, and credential repository.
- **Technical Service Layer:** Smart contracts and DID documents and schema typically reside at the on-chain data layer. Repositories can be counted to nodes. For web applications, web servers are required. These services are run in cloud infrastructure.

V. UNIVERSAL SERVICE MODEL

In the previous Section IV, IMSMF was applied to the most prominent protocols, models, and implementations. As most likely not only one variant but several are operated in an organization, it is important to identify combinations as well as missing components. Therefore, in Section V-A a universal service model for I&AM is established. This service model

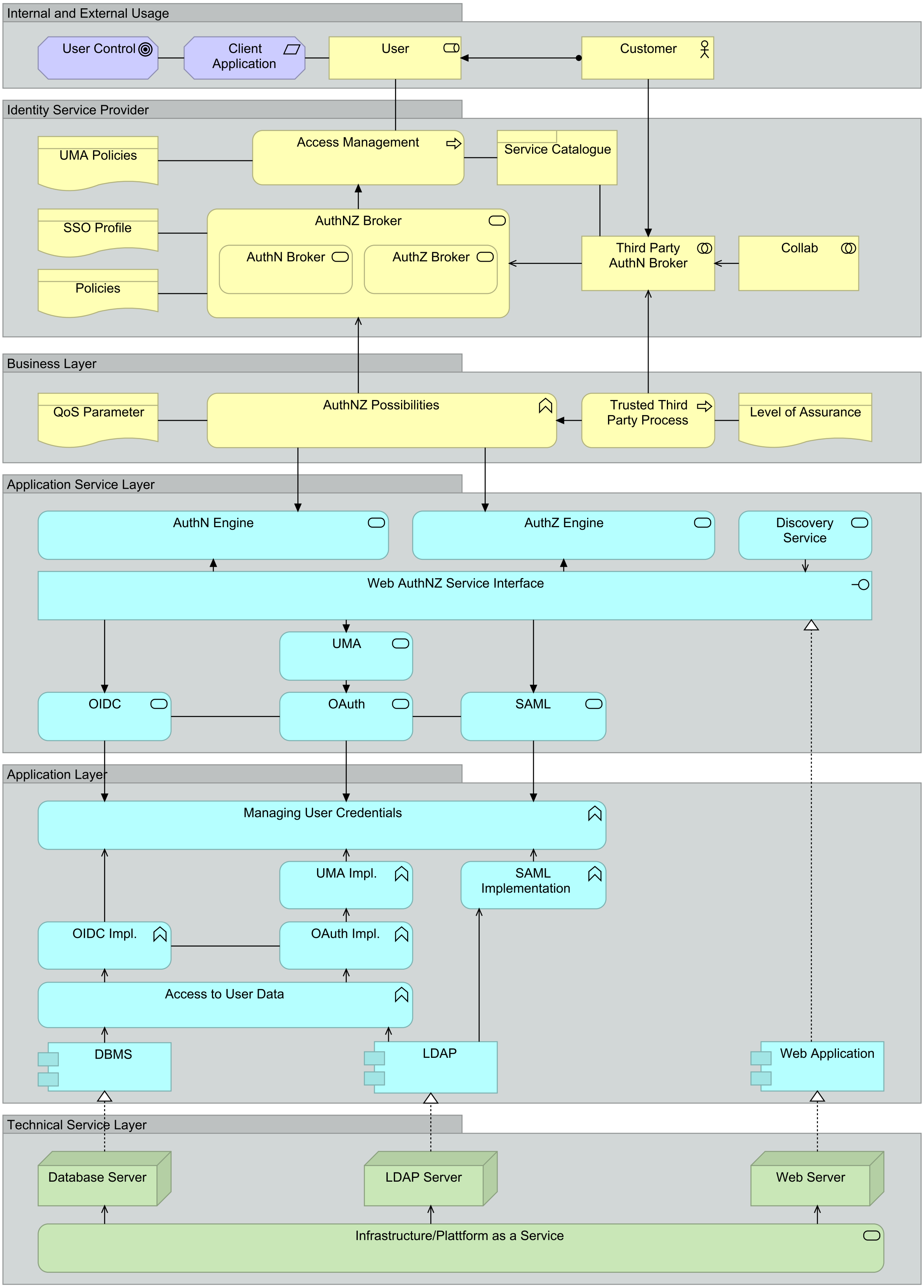

FIGURE 7. Reference model for UMA.

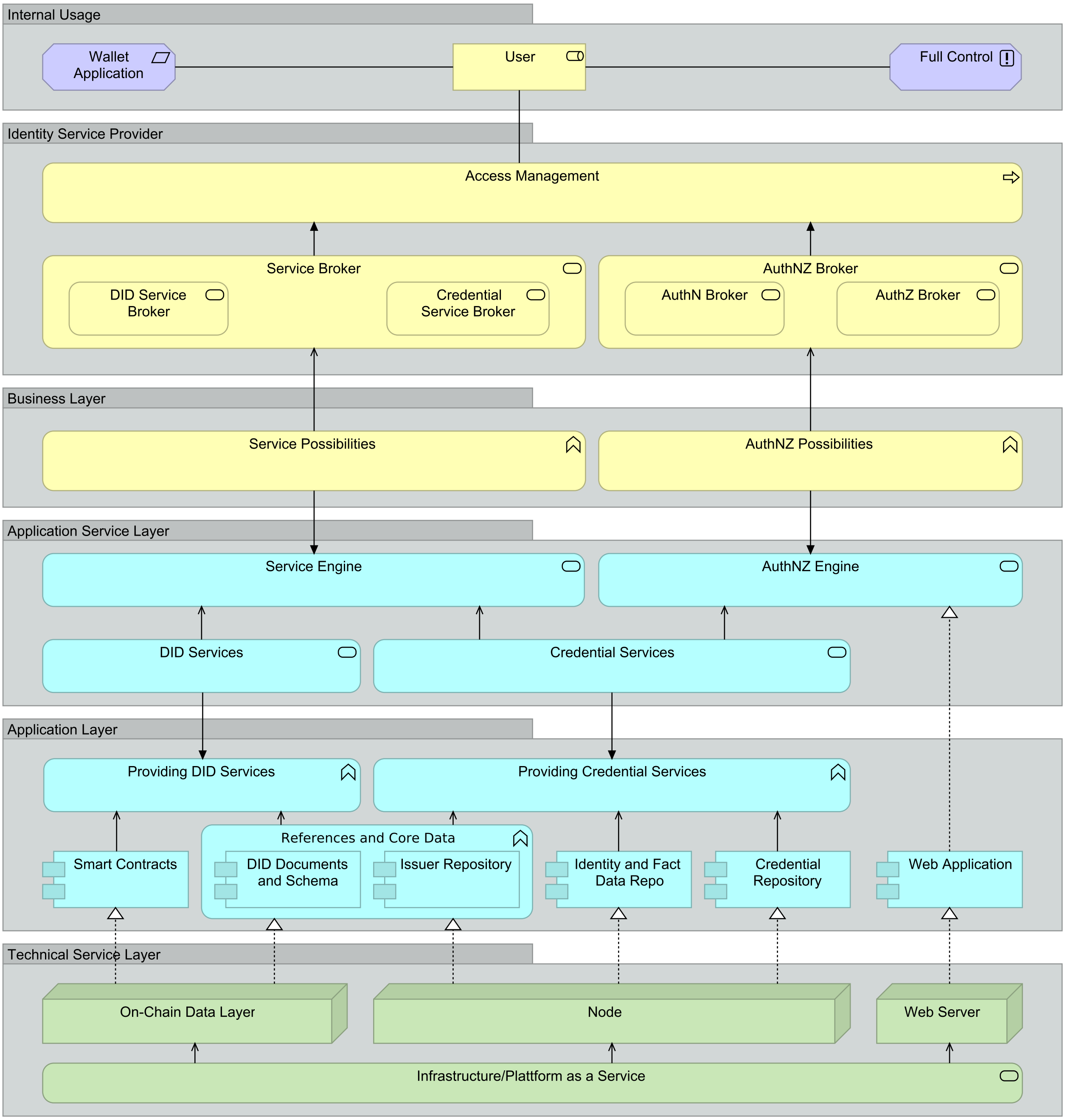

FIGURE 8. Reference model for SSI.

shows possible combinations and similar components, which could be used for several I&AM systems. In the next step (see Section V-B), this model is used to identify missing components for a more usable I&AM.

A. SERVICE MODEL FOR UNIVERSAL I&AM

In order to establish a universal model, each component of the previous models needs to be added. In the next step, duplicates are erased and arrows are adjusted accordingly. If the symbols and arrows differ, then the average used item is chosen. To enhance the clarity, minor elements are left out. Last but not least, the model is evaluated for reasonableness.

The result of this methodology shows that several models and protocols can be operated in parallel, like Enterprise I&AM, FIM, and UMA, whereas integrating SSI requires additional effort. The UMA- and SSI-specific user control functionality provides end-users with more control and overview over their accounts, helping also traditional I&AM. The idea of a service broker is similar to a service catalog, which could be generated by, e. g., processing the metadata, but is in reality often not carried out. Another synergy is trust: Kerberos explicitly establishes trust, whereas other protocols typically use a level of assurance to estimate trust, though trust is the core requirement. The universal reference architecture in Fig. 9 shows the multitude of possibilities of I&AM:

- **External Layer:** The user, which may be the human end-user, an application, data, or a device, wants to access a service via a client application, such as a web browser or a wallet. The user has, depended on the applied I&AM model, different levels of control, ranging from giving consent to full control.
- **Business Service Layer:** Either only the AuthNZ broker or additionally the service broker is triggered by the access management. Access management may have protocol-specific policies and could feature a service catalog. SSO profile, policies, and a third party AuthN broker are common elements in the I&AM landscape. The TTP broker comes with collaboration agreements and key exchange. Although the service broker is SSI-specific, it could be adapted for other models.
- **Business Layer:** In consequence, two main services can be found: general SSI services as well as AuthNZ featuring a trusted third party process and QoS parameters. The TTP process requires some kind of trust, typically described by LoA. Even though this is especially true for FIM, trust is also an important element for SSI, which could be enabled by governance frameworks.
- **Application Service Layer:** This layer has two engines: the AuthNZ engine and the service engine. Whereas the latter is only required for SSI with credential services and DID services via a service interface, the AuthNZ engine is used by every model and protocol with different variations. The TTP process results in a discovery service, displaying or featuring all trusted parties. This is possible due to a list of enabled parties, e. g., by metadata. MFA might be enabled either at this or at the application layer level. Depending on the setup, it may be a requirement of the AuthNZ broker. The web AuthNZ service interface is using different protocols, depending on what is implemented.
- **Application Layer:** Depending on the protocol and model, different applications may be used. For SSI, it is essential to provide credential services and DID services, realized by different repositories and smart contracts. PAM uses, e. g., PAM, LDAP, and applications. LDAP is utilized by not only PAM, but also several others, e. g., SAML implementation, AD, and maybe OIDC and OAuth implementations. These might be configured for DBMS as well, whereas AD requires Kerberos and DNS. Basically saying, I&AM protocols are required to enable I&AM functionalities.
- **Technical Service Layer:** This plurality results in several servers, which may be run in a cloud environment.

B. COMPONENTS FOR UNIVERSAL IDENTITY MANAGEMENT

In order to provide a functional and usable I&AM, several additional components are already in place. The description above showed some synergies, which could be used to enhance the current landscape. These components need to be marked and evaluated. Further components may be possible to enhance cooperation, interoperability, trustworthiness, and more. To find those potential components for a service-oriented architecture, the desired functionalities are determined by reviewing the different entities and their requirements [33].

End-users want to have control over their identities, an overview of the identities and their status, and easy-to-use systems. The already explored service catalog as an extension of a discovery service may be a handsome addition. The functionality may include flexible sharing of resources, see UMA, either alone or in groups.

IdPs and SPs already have (full or lightweight) I&AM in place, which enables access control by following organizational structures with a role concept in a role lifecycle. This setup needs to be up-to-date and thereby involves underlying business processes. This may include delegation and other short-time changes, which may be propagated to further protocols. In order to have an audit record, such a mechanism needs to be implemented for all external changes. Policies are enforced by governance and compliance features. Segregation of duties separates privileges to avoid dangerous privilege combinations. Some kind of IT service management integration is typically in place. Additionally, these entities may require an overview for security, especially if several I&AM systems are operated in parallel while the policies need to be aligned. Parallel or diverse systems may depend upon some kind of translation. With third parties, according components and underlying processes are necessary.

TTPs may offer central functionalities, such as discovery service, translation service, and coordination. This also points out that the functionality is provided in different domains: end-user, entities, and TTPs for cooperation. Thereby, the components have interfaces with existing infrastructures.

Based on the reference service model for FIM due to simplicity reasons, we identify the location of additional components (marked in green), as shown in Fig. 10. When comparing the reference service model for FIM with this figure, we notice fewer differences than one might expect. The reason for this is that some tools are already in use for specific use cases. The components are described in the following:

- **End-User Overview:** Some users utilize password managers to store passwords and further account information. At the same time, password managers sometimes help to improve security, e. g., by checking for leaked passwords and generating passwords with high entropy. Even though password managers come with several barriers [34], [35], they can be enhanced to evaluate the security of the user's account network. With SSI this functionality is partly realized by wallets. At the same time, this is yet another tool for the user. This description shows several starting points for future work.

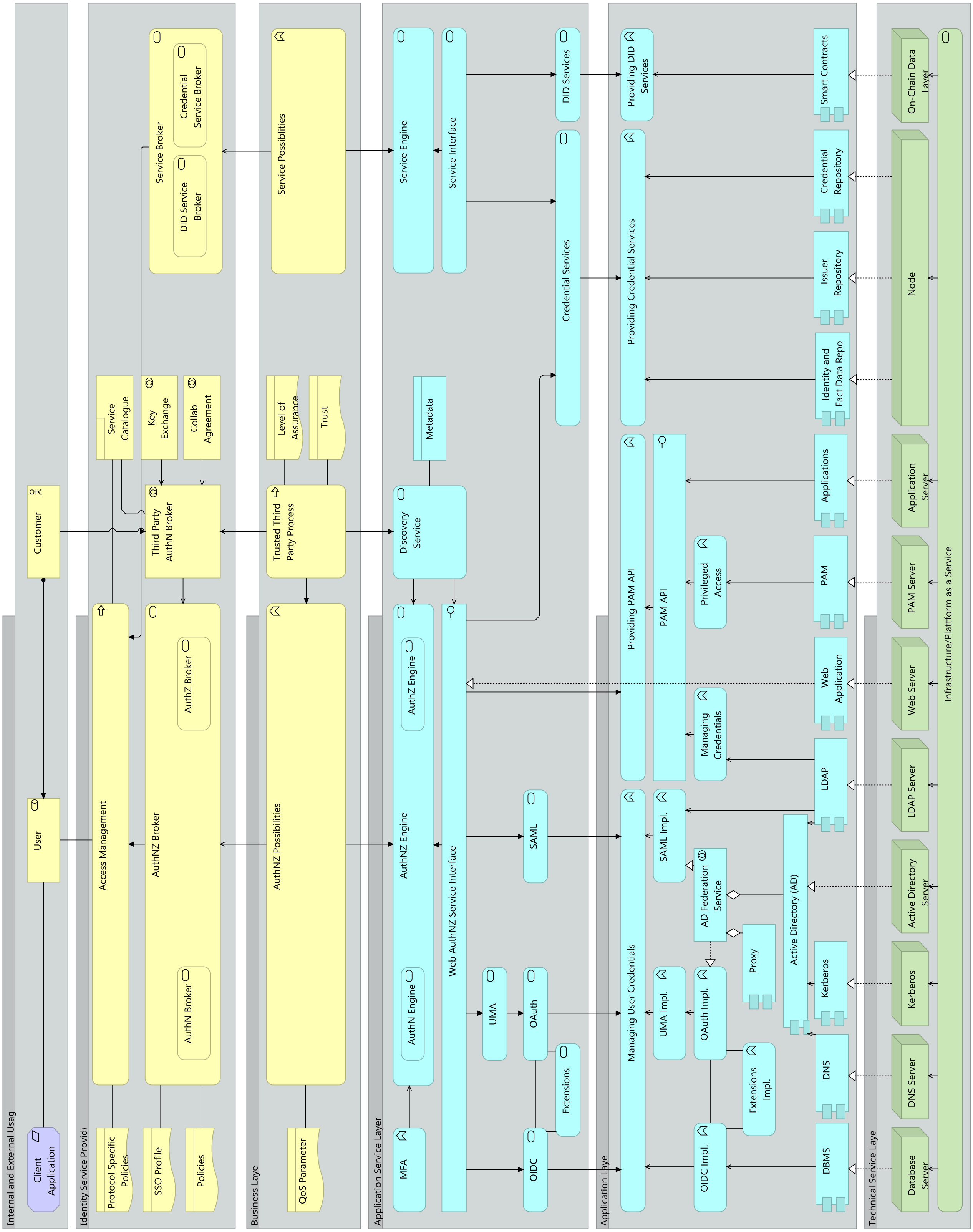

FIGURE 9. Reference model for Universal Identity Management.

- **User Management Overview:** Currently, several I&AM solutions are operated in parallel for internal users, customers, devices, and many more. This may be due to, e. g., business merger, historic or proprietary systems. A modular all-in-one approach with different protocols would reduce the complexity, while allowing the application of the same policies to the modules, streamlining the management of users with improved compliance. By providing one source of truth, the complexity of event logging, auditing, and aggregating the data is reduced, helping to improve the overall security. This information can then be used as the source for reports for the management and more technical information for the IT personnel. Although one single system reduces the complexity, it represents a more interesting target for attackers. As it is one single system instead of several in parallel, it can be hardened accordingly. Due to security requirements, it may be the case that the internal I&AM is separated from the rest. If several I&AM solutions in parallel are used, a meta-system provides a combined overview. Such an overview helps to get the current status of the system. It could, e. g., validate the permissions of several I&AM systems. With an interface to the later discussed translation proxy, migration paths between systems, such as from OpenLDAP to AD, may be provided, enabling some kind of digital twin for I&AM systems.
- **Group and Resource Management:** UMA added value lies within the individual and flexible resource sharing. Generalized, this can be described as some kind of group and resource management. Group management can be used by individuals, organization-internally as well as in cooperation with externals. In addition, group management software can be provided as a service to a wider community. In either case, the connected service needs to enable group management. To make group management available, either the I&AM or specific tools provide these services.
- **Third Party Elements:** With cooperation, a third-party process with trust estimation, i. e., evaluating the trustworthiness of the other entity, is required. The trust in the IdP is typically described as LoA. A similar level could be established for SPs. The process can at least be partly automated according to local policies if using a service such as a TTP, which translates LoAs. Nevertheless, interfaces to business processes and other software may be needed. If the entities do not use the same protocol or flavor, then some sort of translation, as described later, is involved. Bring Your Own Identity (BYOI) enables users to reuse credentials from a third party for convenience by reducing privacy. The third party assumes the privacy and security liability of the I&AM. The organization though still maintains the I&AM related to permissions. In this context, it is also referred to as Identity-as-a-Service (IDaaS). A best practice is to store some attributes in the local I&AM to filter users. In case the third-party login is not secure enough for one resource, step-up authentication, i. e., gaining a higher LoA by adding another authentication method, is triggered.
- **Discovery Service and Service Catalog:** Even though the discovery of the user's IdP is common with SAML and OAuth/OIDC, the discovery process needs to be adapted if SSI is enabled at the same time. Different variants of selecting the corresponding IdP were developed in the past. AccountChooser [36], originally developed by an OpenID Foundation working group, was closed in 2019, whereas the design pattern survived at major sites such as Google and Facebook. Future developments may provide enhanced versions. The aggregated information form a kind of service catalog, showing possible IdPs. At the same time, IdPs could provide service catalogs making available services public to their users.
- **Translation Proxy:** Interoperability is needed on different levels: 1) protocol, 2) account data, and 3) attributes. Whereas account data is more difficult, some solutions for protocol and attributes already exist. For protocols, either the software can speak all required protocols or a proxy translating between both is operated. A proxy typically demands another server, whereas having both protocol implementations in the I&AM system or service is easier to maintain. Protocol conformity is more difficult though if the protocol flavor is diverse. The SAML to SAML proxy between eduGAIN and eID in Europe is an example for this problem. Translation of attributes is typically performed at the IdP side. The IdP translates the attributes into the scheme of the SP before sending them to the entity. Currently, the SAML federation SWITCH [37] provides several translation rules for typically used schemes, which the IdPs can download and integrate. The problem does not only exist within SAML federations but also in other protocols and models. In order to provide a scalable approach, attribute translation rules can be offered by TTPs.

VI. EXPERT EVALUATION

In order to validate and elaborate on the correctness and utility of IMSMF with its model, we organized iterations of sessions with selected experts. First, the method and evaluation design of the evaluation is described in Section VI-A, before the three steps are detailed in Sections VI-B to VI-D. Last but not least, the results are summarized in Section VI-E.

A. METHOD AND EVALUATION DESIGN

The evaluation is based on the incentives of selected experts. These sessions serve as proof of the quality of IMSMF. The details of the design are summarized as follows:

- **Goals:**
  - Validation and elaboration IMSMF;
  - Applicability of ArchiMate for IMSMF;
  - Usage of a universal model.

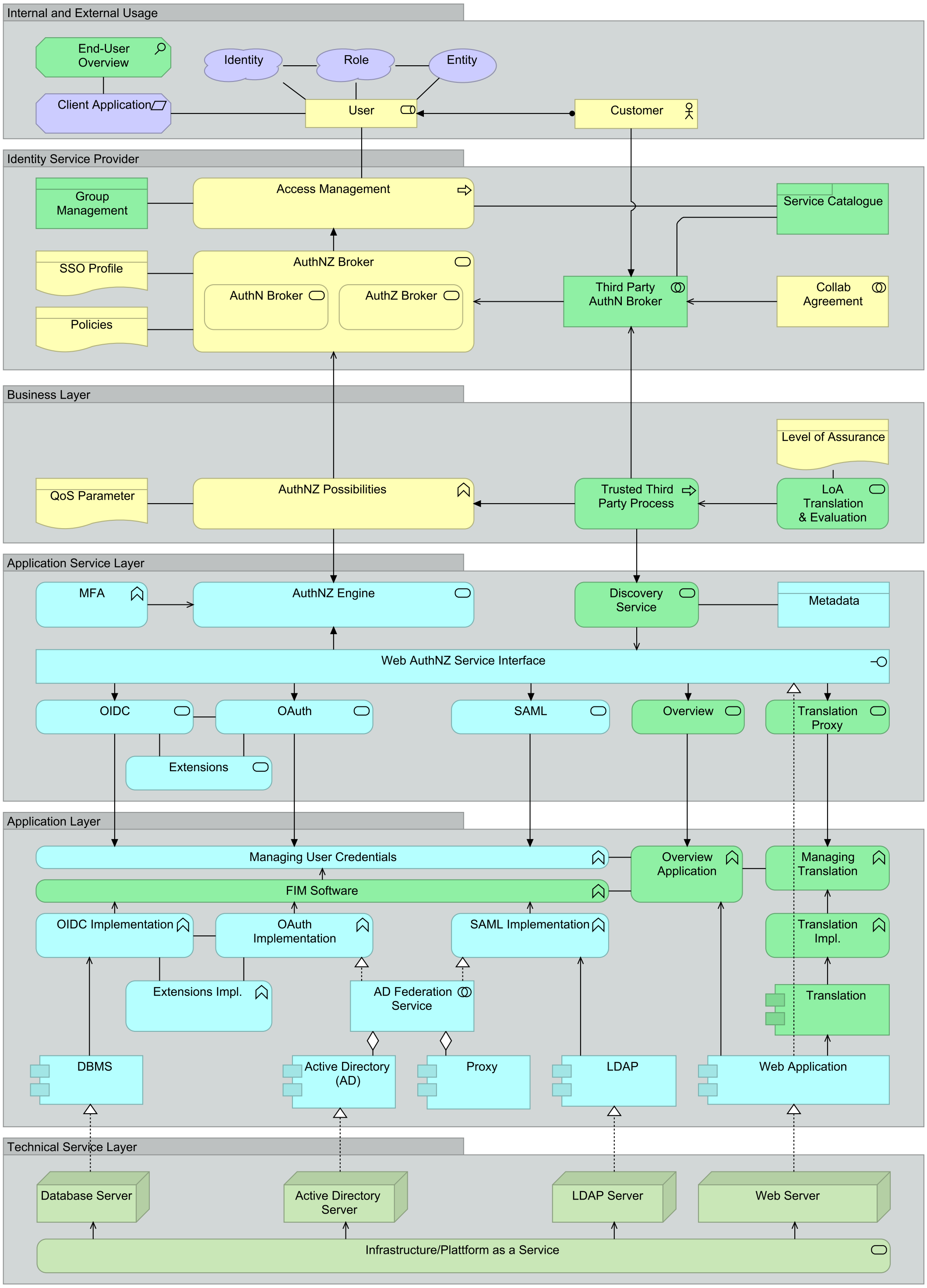

FIGURE 10. Components for Universal Identity Management.

- **Iterations:**
  - Questionnaire: Internal review, invitation sent to experts, which then answer the questions;
  - Discussions;
  - Final round of expert interviews.
- **Recruitment:** The experts were already known by the authors due to membership of the faculty or former projects with focus on identity management and were directly asked. No compensation was paid.

The details of the survey are as follows:

- **Participants:** The invitation to the questionnaire was sent to 15 experts in the field of I&AM or a subarea. The experts typically come from Germany with one exception from Switzerland. Of these experts, 14 were male

and 1 female. In total, 3 were involved in the pre-test, 4 answered the questionnaire, and 5 were participants in the discussions.
- **Survey:** The questionnaire was pre-tested with 3 colleagues. Both the pre-test and real survey took place online via a survey tool with servers in Germany. The survey itself can be found in Appendix B.
- **Time:** The survey was online from mid-March until the end of April 2022.
- **Ethics:** The survey was within the ethical guideline of the university and therefore did not require further acceptance.
- **Limitations:** Limited amount of answers, participants solely from the DACH region, thereby, not representative enough.

The details of the interviews are as follows:
- **Participants:** 8 experts were asked to participate in interviews; 7 excepted the invitation. The experts come from Germany (5), Sweden (2) and Norway (1). Of these experts, 7 were male and 1 female.
- **Interviews:** The interviews with the expert were unstructured, focusing on the correctness of the models, and took mostly 30 to 60 minutes. The key elements of the interviews were recorded on paper.
- **Time:** The interviews took place in August 2022.
- **Ethics:** The interviews were within the ethical guideline of the university and therefore did not require further acceptance.
- **Limitations:** Limited amount of answers, participants Europe.

B. STEP 1: QUESTIONNAIRE

We design the questionnaire by referring to the sub-characteristics of functional suitability, i. e., completeness, correctness, and appropriateness, and casting doubt on the main elements of IMSMF, i. e., design process, modeling language, meta-model, and re-usability for externals. As shown in Appendix B, the questionnaire consists of four parts: 1) generic participant questions, 2) specific questions related to IMSMF, 3) specific questions related to the universal model, and 4) open questions for further improvements. The experts respond to the questions either with open answers or with the Likert Scale ranging from 1 to 5. The questionnaire was designed as such that the questions can be answered anonymously. Depending on the open answers, the respective expert could be determined. The questionnaire is pre-tested with 3 colleagues to improve it and fix possible problems. The questionnaire is then sent to 15 experts, of whom 4 answered. As the questionnaire was also sent to the colleagues, which already answered the pre-test, this may be a reason why they have probably not answered the questionnaire a second time. The content-wise answers are nevertheless incorporated. In addition, to answer the questionnaire, at least 30-45 minutes were measured. Not all participants have the will and time for this. Last but not least, the participants did not get an expense allowance.

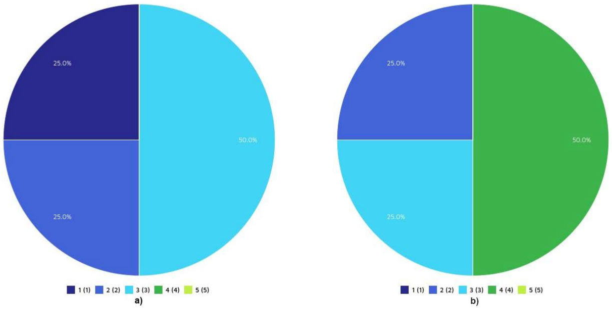

FIGURE 11. Comparison of understanding the models without (a) and with (b) explanations.

The experts mainly have a diploma resp. master with one exception of a Ph.D. The years of experience (in research or industry) of our experts range from 0 to 17 years, with an average of 9.4 years. One of the experts with a specific sub-area has probably chosen 0 years. The applied protocols range from SAML and OIDC to LDAP, Structured Query Language (SQL), and DirXML. The reference architectures the experts know are diverse: ISO/IEC 27000, ISO/IEC 20000, Object-Oriented Design (OOD) Object-Oriented Modeling (OOM) Object-Oriented Programming (OOP), MNM Service Model, TM Forum SID, and Software-Defined Networking (SDN). These architectures are rather generic or ITSM-related. Hence, the modeling languages tools comprise UML, draw.io, Business Process Model and Notation (BPMN), Entity Relationship Model (ERM), Eclipse Papyrus, Topology and Orchestration Specification for Cloud Applications (TOSCA), and Yet Another Next Generation (YANG). Based on a Likert scale from 1 to 5, with 1 being the highest and 5 the lowest, the experts value their experience at 3.75, which correlates with their usage. The experts apply modeling resp. reference architectures to make I&AM process visible, to visualize complex facts, for research, and model-based programming. The reasons to use it mainly concentrate on comprehensibility and clarity. The goals are diverse with no goals, better understanding of processes for stakeholders, standardized procedure, striving for completeness, specification of a framework, and formalization of architectures. Half of the experts apply models in the field of I&AM, either for research or to comply with norms and standards. The experts estimate the challenges ''Understanding and Acceptance'', ''Verification and Validation'', and ''Transformation and Variants'' (18.2% each) as highest, followed by ''Training and Expertise'', ''Quality'', ''Modeling Language/Tool'', ''Complexity'', and ''Practical Application'' (9.1%) each. Models for I&AM should include data/entity models, system components, processes and workflows, data representations, provisioning models and interfaces, as well as cross-organizational aspects, e. g., policies and LoA.

In summary, the experts express that the reference models require detailed descriptions to fully understand them, as shown in Fig. 11. Nevertheless, the provided description was probably not good enough. In the next step, it is refined. The reference models are on average correct. This varies though through the different models: PAM, Kerberos, and SSI (undecided) in contrast to LDAP, FIM, and UMA (mainly correct). The experts commented that a description of the notation is missing, which is added during step 2. Another question, which came up, was what is relevant and what is irrelevant. One expert noted that some arrows were missing, as other combinations are possible, but might not be common. In order to include this remark while making the models not too complicated, some generalization, such as "User Management", which includes DBMS, AD, and LDAP, is incorporated. Further comments related to specific models. In Kerberos, several variations are introduced in the next step to include implementations, such as MIT Kerberos and Heimdal Kerberos. The differentiation of primary and supportive services is enhanced within the description of the FIM model, whereas the exchanged information is not further detailed. Full control and the prioritization of authentication vs. authorization at the SSI description are made clear during the next step.

In order to evaluate ArchiMate as the applied modeling tool, further questions were asked. The answers demonstrate that ArchiMate can be used (50%), although 50% of the experts were not sure as the models are rather complex. In a session within step 2, this topic came up again. It showed that the different options ArchiMate offers make the overview even more complicated while detailing the models at the same time. No differentiation between the different providers was made, which was another remark. Although this is possible within ArchiMate, it would make the models more complex. Therefore, the decision was made to improve the description instead. The usage and its difficulty were estimated on average.

The experts expected guidance for large-scale I&AM systems, migrations to new I&AM systems, extensions of current I&AM systems, and ways of interoperability between different I&AM systems by the universal model. On average, the experts judge the model as mostly correct (2.25 in a scale from 1 to 5, with 1 being completely correct). As a remark, a more generic model was proposed, which is added in step 2. The control question, what can be derived from the universal model, showed that the expectations were met.

C. STEP 2: IMPROVEMENTS

In order to improve IMSMF, the answers of the experts were evaluated and incorporated whenever possible. In addition, specific questions, which came up during the refinement, were discussed with colleagues and experts in unstructured interviews to further enhance IMSMF. One virtual session led to several further questions and ideas on how to improve the understanding of the models. A result of this discussion is the meta-model, described in Section III.

D. STEP 3: FINAL EXPERT INTERVIEWS

A last round of unstructured interviews with experts (from the group of experts of Step 1 and further recruited experts) was conducted. The interviewees were generally fine with the results. One expert emphasized on the correct usage of the arrows. Two experts provided practical examples, one for parallelism of systems in organizations and one for the IoT protocol LoRa. When asked, the experts were against further detailing the models as it would make them more complex. This is in line with the decision made after the questionnaire. Furthermore, the provided description was seen as detailed enough. This is especially true as the meta-model with an according example in Section III was added. For non-experts, further guidelines may be added as future work. Hence, all remarks were included to the satisfaction of the experts.

E. RESULTS

In the following, we report the results. The presented reference models visualize different views or models. Relating to the Zachman Framework [38], IMSMF mainly covers system model (row 3) and technology model (row 4). The deployment (row 5) can be based on IMSMF, while functioning enterprise (row 6) is at least partly helped by the added tools. Nevertheless, a business process view (row 2) is missing, which was expected by some experts. The scope (row 1) has to be defined by the organization applying I&AM resp. IMSMF. The meta-model generically describes IMSMF and can be adapted for the different use cases and protocols as shown in Section IV. The meta-model was added as feedback from Step 1 and 2 of the evaluation and was evaluated as useful. In order to give guidance for adoption, further guidelines may be needed. In addition, practical examples may be provided. While the experts assessed the models as mainly correct to correct in Step 1, the rating was improved to correct in Step 3.

VII. DISCUSSION

In this section, we discuss whether IMSMF supports experts in modeling diverse identity management scenarios and analyzing alternative architectures with respect to the business objectives and quality attributes. For this purpose, we first analyze the quality of IMSMF with its models of protocols, implementations, and models, based on the meta-model in Section VII-A. Then we discuss the research questions in Section VII-B, before exploring the limitations of our approach in Section VII-C.

A. QUALITY OF THE MODELS

In order to define and discuss the quality of the presented IMSMF with its models, we apply the quality framework for reference models by Taylor and Sedera [39].

Syntactic quality refers to the language, i. e., the implied meta-model as well as the layout, overall design, and underlying concepts, of the model. The syntactic quality is therefore not only the strict application of the grammar and symbols but also how these are used in terms of consistency. We apply the concepts and notions of ArchiMate, which are clearly defined, to the field of I&AM. The generic model is then consistently used and employed on various protocols, models, and implementations.

Semantic quality reflects how well the model captures its goals. An ideal fit is when the model captures everything of relevance and nothing of irrelevance. Therefore, relevance, completeness, and correctness are important terms. We have derived the models from literature, protocol specifications, implementations, and good practice. In addition, we enhanced the models by expert evaluation. Thus, we included standard cases as well as exceptions. In addition, we had a meeting with selected experts, where we discussed the relevance and irrelevance of elements of the model. As a result, the models have sufficient quality.

Pragmatic quality defines how well the model is understood, which includes the quality itself and the quality of the support material. In order to understand IMSMF with its models easily, additional texts as indicated by our experts are relevant. With them, the models can be comprehended and applied to specific use cases. This shows that the support material is important to gain pragmatic quality.

B. RESEARCH QUESTIONS

In the following, we discuss the research questions previously stated in Section I.

Q1 How to describe I&AM scenarios with a scenario-independent approach? IMSMF provides a generic meta-model (see Section III), which can be applied to different scenarios. The following models in Section IV detail the meta-model for certain settings, while still being scenario-independent. These models can be adapted for specific scenarios.

Q2 Which elements are required to fulfill the requirements described above? The research question is answered by the requirements:

- R1: In order to get a reusable architecture, the meta-model was designed. Within all IMSMF models, generic and universal terminology in accordance with standards was used.
- R2: The models of IMSMF provide a systematic overview. Although they describe major aspects, specific characteristics would require further models. This decision was made to restrict the complexity of the individual models.
- R3: The models of IMSMF show that the meta-model is adaptability to different protocols and use cases. Nevertheless, there might be limitations to that as discussed in the next section.
- R4: The dependencies between different providers with related interfaces are made visible, whereas the different providers are not clearly separated due to complexity reasons. Several components indicate appropriate service management, although further models could visualize ITSM.

Q3 What is required to adapt the reference architecture to different areas? The meta-model in Section III has been adapted to different areas, as shown in Section IV. In order to detail the model, the important components, primary and supportive services, functionalities, and stakeholders have to be identified. In the next step, differences and modifications to the meta-model have to be emphasized. The model has to be detailed accordingly. Last but not least, the resulting model needs to be iteratively evaluated, enhanced, and checked for correctness, as described in Section VII-A.

Q4 How can different I&AM models and approaches be combined? The universal model in Section V-A shows how different models and approaches can be combined. While some components are the same or at least similar in several approaches, others are rather specific to some flavors. Therefore, the efforts needed to combine approaches ranges depending on the selected I&AM systems.

Q5 Which elements are needed to have a more useful I&AM in place? This research question is answered by the derivation of components in Section V-B. By adding different overviews, translation components, group management in addition with third party components, I&AM is enhanced.

In order to position the universal identity management model and put references to those requirements of ITIL, NAF, etc and evaluate the compliance of them in the paper, as the reviewers suggested, we added further references (aka the difference) in the introduction, where they are first stated, and a section here about the contribution and the compliance with ITIL, NAF etc.

C. LIMITATIONS

Even though IMSMF meets the quality criteria, it has some limitations. Whereas IMSMF does include several models, it does not comprise of all protocols, implementations, and models in the I&AM universe. Therefore, it is not complete and there might be an approach, which cannot be applied to the meta-model. In addition, as I&AM is progressing, further models might be needed in the future. This is especially true for SSI, which is still enhanced. Although different requirements from the stakeholders were taken into account, the visualization with the FIM model might have made it possible to overlook components, which are relevant for usable and functional I&AM. In order to improve the adoption, further guidelines and practical examples may be required. Last but not least, the evaluation was limited to only a few experts mainly in the DACH region. Even though the evaluation had several rounds and further experts from other regions were included, this limitation might result in restricted applicability.

VIII. CONCLUSION AND OUTLOOK

The sudden adoption of remote work at the beginning of the COVID-19 pandemic with its increase in using various online services shaped I&AM also in the following year. As security could partly not keep up, issues with I&AM became visible. The I&AM landscape is rather complex and diverse due to different approaches and protocols. In order to improve the current state, an overview is important. To address these problems, the IMSMF with a meta-model and several models for selected protocols, implementations, and models was designed. Based on the set of models, a universal I&AM model was designed, identifying additional components, which could enhance the current landscape. All these proposed models were evaluated in several rounds by experts. Finally, IMSMF was discussed by quality metrics and limitations.

The models show that there is neither an inside nor an outside. Therefore, security measures need to be adapted accordingly. In future work, we want to explore existing and to-be-created security measures based on IMSMF. Furthermore, we plan to investigate end-user and entity-based overviews. The end-user overview depends on a systematic evaluation strategy, usability, and interoperability. For the entity-side, a meta-model is required first. In addition, process models as commented by the experts need to be established. Last but not least, we will update IMSMF when new approaches emerge.

APPENDIX A NOTION ON ARROWS AND OTHER SYMBOLS

Fig. 12 shows different notions on arrows and other symbols, used by ArchiMate.

APPENDIX B QUESTIONNAIRE

The questions of the questionnaire are listed here. First, the generic questions are shown, followed by IMSMF-specific and universal model-specific questions. Last but not least, the two final questions are displayed.

A. GENERIC QUESTIONS

The following generic questions were asked:

- What is your highest academic degree? (Open answer)
- What is your current professional position? (Open answer)
- How big is the organization you work in? (Different scales)
- How many years have you been involved with identity management? (Open answer)
- What protocols do you deal with in the field of identity management? (Open answer)

The following modeling-related questions showed up:

- Which reference architectures do you know? (Open answer)
- What modeling languages and tools do you know? (Open answer)
- How much experience do you have with modeling or reference architectures? (Likert scale 1 to 5 with 1: very much; 5: none at all)
- How often do you use modeling or reference architectures? (Different scales from never (0%) to always)
- Where do you use modeling or reference architectures? (Open answer)
- Why do you use modeling or reference architectures? (Open answer)
- Do you know any models or reference architectures in the field of identity management? (Yes, no, not sure, I don't want to answer)
- Which reference architectures and models do you know for identity management? (Open answer)
- Do you use identity management models or reference architectures yourself? (Yes, no, not sure, I don't want to answer)
- What are your reasons for this? (Open answer)
- What challenges do you face with models or reference architectures in the field of identity management? (Selection possibility)
- If you checked "Other", which ones do you also have? (Open answer)
- What do you think must be included in an identity management reference architecture (elements, protocols, software,...)? (Open answer)

B. IMSMF-SPECIFIC QUESTIONS

First, the following generic questions about the IMSMF had to be answered:

- To what extent do you generally understand the reference architectures without explanations? (Likert scale 1 to 5 with 1: very good; 5: not at all)
- Now read the explanations. In general, do you now understand the reference architectures? (Likert scale)
- Are the reference architectures generally technically correct? (Likert scale)

Then, model-specific questions followed. These questions were asked for each model:

- Is the reference architecture for the model (PAM, Kerberos, etc.) technically correct? (Likert scale)
- What is technically incorrect in the model (PAM, Kerberos, etc.) or could be solved better? (Open answer)

Last but not least, further generic questions about the IMSMF were asked:

- In your opinion, is modeling with ArchiMate suitable for these reference architectures? (Yes, no, not sure, I don't want to answer)
- Which modeling language do you think is better suited for the reference architectures? (Open answer)
- Do you see any general improvement and/or expansion options for the reference architectures? If yes, which? (Open answer)
- If you had to suspend a system, would you use the reference architectures shown? (Likert scale)
- How easy or difficult do you think it is to implement in your environment? (Likert scale)

C. UNIVERSAL MODEL-SPECIFIC QUESTIONS

The following questions concerning the universal model had to be answered:

- What do you expect from a universal reference architecture for identity management? (Open answer)

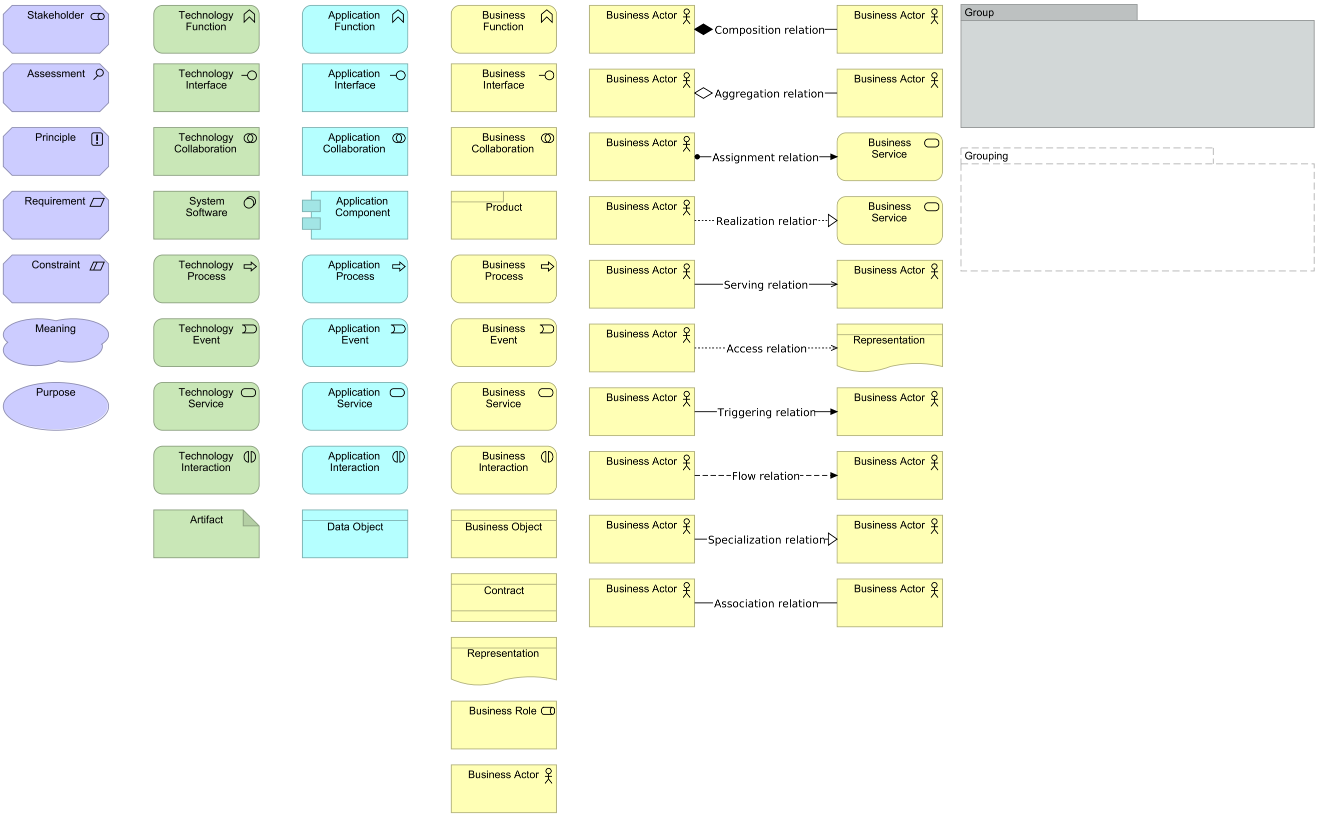

FIGURE 12. Notion on arrows and other symbols.

- Where should a universal reference architecture for identity management be used? (Open answer)
- What elements/protocols/roles must be included in a universal reference architecture for identity management? (Open answer)
- Is the reference architecture for universal identity management technically correct? (Likert scale)
- What elements are you missing from the universal reference architecture for identity management, or what can be improved? (Open answer)
- What can you derive from the universal reference architecture? (Selection possibility)
- If you ticked other: What else can be derived from the universal reference architecture? (Open answer)

D. FINAL QUESTIONS

Last but not least, the two final questions were presented:

- Do you have any other comments on the reference architectures? (Open answer)
- Do you have any other comments/feedback on the survey? (Open answer)

REFERENCES

[1] D. Pöhn and W. Hommel, "IMC: A classification of identity management approaches," in *Computer Security*, I. Boureanu, C. C. Drăgan, M. Manulis, T. Giannetsos, C. Dadoyan, P. Gouvas, R. A. Hallman, S. Li, V. Chang, F. Pallas, J. Pohle, and A. Sasse, Eds. Springer, 2020, pp. 3–20.

[2] D. Pöhn and P. Hillmann, "Reference service model for federated identity management," in *Enterprise, Business-Process and Information Systems Modeling*, A. Augusto, A. Gill, S. Nurcan, I. Reinhartz-Berger, R. Schmidt, and J. Zdravkovic, Eds. Cham, Switzerland: Springer, 2021, pp. 196–211.

[3] F. Buschmann, K. Henney, and D. C. Schmidt, *Pattern-Oriented Software Architecture: On Patterns and Pattern Languages*, vol. 5. Hoboken, NJ, USA: Wiley, 2007.

[4] J. Schoonderbeek. (2018). *Modelling Identity in Enterprise Architecture/ArchiMate*. [Online]. Available: https://www.archimatetool.com/blog/2018/12/07/long-read-modelling-identity-in-enterprise-architecture-archimate/

[5] *A Framework for Identity Management—Part 2: Reference Architecture and Requirements*, Standard ISO/IEC 24760-2:2015, 2015.

[6] P. A. Grassi, M. E. Garcia, and J. L. Fenton, "NIST special publication 800–63–3—Digital identity guideline," U.S. Dept. Commerce, Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep., 2017.

[7] K. Hazelton. (2021). *The TAP Reference Architecture (RA)*. [Online]. Available: https://spaces.at.internet2.edu/pages/viewpage.action?pageId=98306902

[8] Y. Cao and L. Yang, "A survey of identity management technology," in *Proc. IEEE Int. Conf. Inf. Theory Inf. Secur.*, Dec. 2010, pp. 287–293.

[9] G. B. Dobbs, "IAM reference architecture," *IDPro Body Knowl.*, vol. 1, no. 6, 2021.

[10] M. Dabrowski and P. Pacyna, "Modular reference framework architecture for identity management," in *Proc. 11th IEEE Singap. Int. Conf. Commun. Syst.*, Nov. 2008, pp. 743–749.

[11] M. Gaedke, J. Meinecke, and M. Nussbaumer, "A modeling approach to federated identity and access management," in *Proc. 14th Int. Conf. World Wide Web (WWW)*, 2005, pp. 1156–1157.

[12] D. Pöhn and W. Hommel, "Management architecture for dynamic federated identity management," in *Proc. Comput. Sci. Inf. Technol. (CSIT)*, May 2016, pp. 211–226.

[13] M. Garschhammer, R. Hauck, B. Kempter, I. Radisic, H. Roelle, and H. Schmidt, "The MNM service model—Refined views on generic service management," *J. Commun. Netw.*, vol. 3, no. 4, pp. 297–306, 2001.

[14] Y. Liu, Q. Lu, H.-Y. Paik, X. Xu, S. Chen, and L. Zhu, ''Design pattern as a service for blockchain-based self-sovereign identity,'' *IEEE Softw.*, vol. 37, no. 5, pp. 30–36, Sep. 2020.

[15] B. N. Eddine, A. Ouaddah, and A. Mezrioui, ''Exploring blockchain-based self sovereign identity systems: Challenges and comparative analysis,'' in *Proc. 3rd Conf. Blockchain Res. Appl. Innov. Netw. Services (BRAINS)*, Sep. 2021, pp. 21–22.

[16] A. Grüner, A. Mühle, and C. Meinel, ''ATIB: Design and evaluation of an architecture for brokered self-sovereign identity integration and trust-enhancing attribute aggregation for service provider,'' *IEEE Access*, vol. 9, pp. 138553–138570, 2021.

[17] Y. Yang, X. Chen, G. Wang, and L. Cao, ''An identity and access management architecture in cloud,'' in *Proc. 7th Int. Symp. Comput. Intell. Design*, Dec. 2014, pp. 200–203.

[18] G. Katsikogiannis, S. Mitropoulos, and C. Douligeris, ''An identity and access management approach for SOA,'' in *Proc. IEEE Int. Symp. Signal Process. Inf. Technol. (ISSPIT)*, Dec. 2016, pp. 126–131.

[19] G. Amaral, T. P. Sales, G. Guizzardi, J. P. A. Almeida, and D. Porello, ''Modeling trust in enterprise architecture: A pattern language for archimate,'' in *The Practice of Enterprise Modeling*, J. Grabis and D. Bork, Eds. Berlin, Germany: Springer, 2020, pp. 73–89.

[20] C. L. B. Azevedo, M.-E. Iacob, J. P. A. Almeida, M. van Sinderen, L. F. Pires, and G. Guizzardi, ''Modeling resources and capabilities in enterprise architecture: A well-founded ontology-based proposal for ArchiMate,'' *Inf. Syst.*, vol. 54, pp. 235–262, Dec. 2015.

[21] C. Griffo, J. P. A. Almeida, G. Guizzardi, and J. C. Nardi, ''From an ontology of service contracts to contract modeling in enterprise architecture,'' in *Proc. 21st Int. Enterprise Distrib. Object Comput. Conf. (EDOC)*, 2017, pp. 40–49.

[22] J. Petrovska, A. Memeti, and F. Imeri, ''SOA approach—Identity and access management for the risk management platform,'' in *Proc. 8th Medit. Conf. Embedded Comput. (MECO)*, 2019, pp. 1–4.

[23] B. Zwattendorfer, T. Zefferer, and K. Stranacher, ''An overview of cloud identity management-models,'' in *Proc. 10th Int. Conf. Web Inf. Syst. Technol. (WEBIST)*, 2014, pp. 82–92.

[24] K. Consortium, ''The role of kerberos in modern information systems,'' Kerberos Consortium, Cambridge, MA, USA, White Paper, 2008.

[25] N. Ragouzis, J. Hughes, R. Philpott, and E. Maler, ''Security assertion markup language (SAML) V2.0 technical overview,'' OASIS Secur. Services Tech. Committee Standard, Burlington, MA, USA, Tech. Rep. sstc-saml-tech-overview-2.0-cd-02, 2008.

[26] D. Hardt, *The OAuth 2.0 Authorization Framework*, document RFC 6749, RFC Editor, Internet Requests for Comments, Oct. 2012. [Online]. Available: http://www.rfc-editor.org/rfc/rfc6749.txt

[27] N. Sakimura, J. Bradley, and M. B. Jones, ''OpenID Connect dynamic client registration 1.0,'' OpenID Foundation, San Ramon, CA, USA, Tech. Rep., Nov. 2014.

[28] D. Hardt, A. Parecki, and T. Lodderstedt, ''The OAuth 2.1 authorization framework,'' Working Draft, Internet Eng. Task Force, Fremont, CA, USA, Tech. Rep. draft-ietf-oauth-v2-1-05, Mar. 2022, [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-oauth-v2-1/05/

[29] J. Richer, A. Parecki, and F. Imbault, ''Grant negotiation and authorization protocol,'' Working Draft, Internet Eng. Task Force, Fremont, CA, USA, Tech. Rep. draft-ietf-gnap-core-protocol-05, Mar. 2022. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-gnap-core-protocol/09/

[30] E. Maler, M. Machulak, and J. Richer, ''User-managed access (UMA) 2.0 grant for oauth 2.0 authorization,'' Kantara Initiative, Kantara Specification, Richmond, VA, USA, Tech. Rep., 2018.

[31] J. Richer, ''Health relationship trust profile for user-managed access 2.0,'' Kantara Initiative, Kantara Specification, Richmond, VA, USA, 2018.

[32] A. Mühle, A. Grüner, T. Gayvoronskaya, and C. Meinel, ''A survey on essential components of a self-sovereign identity,'' 2018, *arXiv:1807.06346*.

[33] K. Pohl and N. Ulfat-Bunyadi, *The Three Dimensions of Requirements Engineering: 20 Years Later*. Berlin, Germany: Springer, 2013, pp. 81–87.

[34] S. G. Lyastani, M. Schilling, S. Fahl, M. Backes, and S. Bugiel, ''Better managed than memorized? Studying the impact of managers on password strength and reuse,'' in *Proc. 27th USENIX Secur. Symp. (USENIX Security)*, 2018, pp. 203–220.

[35] H. Ray, F. Wolf, R. Kuber, and A. J. Aviv, ''Why older adults (don't) use password managers,'' in *Proc. 30th USENIX Secur. Symp. (USENIX Security)*, 2021, pp. 73–90.

[36] OpenID Foundation. (2019). *Account Chooser & Open YOLO (You Only Login Once) Working Group Homepage*. [Online]. Available: https://openid.net/wg/ac/

[37] SWITCH. (2022). *SWITCHaai Attributes*. [Online]. Available: https://www.switch.ch/aai/support/documents/attributes/

[38] J. A. Zachman, ''A framework for information systems architecture,'' *IBM Syst. J.*, vol. 26, no. 3, pp. 276–292, 1987.

[39] C. Taylor and W. Sedera, ''Defining the quality business process reference models,'' in *Proc. Australas. Conf. Inf. Syst. (ACIS)*, 2003, pp. 1–10.

DANIELA PÖHN received the Ph.D. degree in dynamic identity management in federations from the Ludwig Maximilians University of Munich. She is currently a Senior Researcher at the Research Institute CODE, Universität der Bundeswehr München. Her research is mainly on identity management, in particular federated identity management, integration of security management, and level of assurance. At the same time, she is active involved in projects related to interactive cyber training. In her role as a Research Assistant at the Leibniz Supercomputing Centre, she was a Task Leader in the EU Project GÉANT improving the global federation eduGAIN.

WOLFGANG HOMMEL is currently a Professor of software and data security at the Universität der Bundeswehr München and the Director of the Research Institute Cyber Defence (RI CODE). He worked on the systematic conception and practical implementation of identity federations on national and international scales in research and education networks as well as eGovernment for the past 15 years. Advancing identity management protocols and service management processes for identity federations and self-sovereign identity infrastructures has been the subject of numerous dissertations, student theses, and scientific publications of his research group.