MANAGEMENT ARCHITECTURE FOR DYNAMIC FEDERATED IDENTITY MANAGEMENT

Daniela Pöhn[1] and Wolfgang Hommel[1]

[1]Leibniz Supercomputing Centre, Munich Network Management Team,
Garching n. Munich, Germany
poehn@lrz.de, hommel@lrz.de

ABSTRACT

We present the concept and design of Dynamic Automated Metadata Exchange (DAME) in Security Assertion Markup Language (SAML) based user authentication and authorization infrastructures. This approach solves the real-world limitations in scalability of pre-exchanged metadata in SAML-based federations and inter-federations. The user initiates the metadata exchange on demand, therefore reducing the size of the exchanged metadata compared to traditional metadata aggregation. In order to specify and discuss the necessary changes to identity federation architectures, we apply the Munich Network Management (MNM) service model to Federated Identity Management via a trusted third party (TTP); an overview of all components and interactions is created. Based on this model, the management architecture of the TTP with its basic management functionalities is designed. This management architecture includes further functionality for automated management of entities and dynamic federations.

KEYWORDS

Federated Identity Management, SAML, Service Management, Management Architecture, Trust Management

1. INTRODUCTION

Organizations, such as universities, provide several services to their members, e.g., email, exam management, and video conferencing. Users within the organization typically log in via username and password with optional additional factors, such as smartcards or X.509v3 user certificates. Their authorization is based on their roles and optionally manually assigned permissions, which are commonly stored in the organization's centralized Identity & Access Management (I&AM) system. The I&AM system is typically based on Lightweight Directory Access Protocol (LDAP) servers or relational database management systems in the backend. When users are part of a project, which is jointly carried out by several organizations, inter-organizational identity management becomes necessary. In order to allow users to re-use their home organization's accounts for external services, *Federated Identity Management (FIM)* was introduced. It facilitates the identity management between different organizations. While the OASIS standard Security Assertion Markup Language (SAML) [1] enables the exchange of user information in

Jan Zizka et al. (Eds) : CCSEIT, AIAP, DMDB, MoWiN, CoSIT, CRIS, SIGL, ICBB, CNSA-2016
pp. 211–226, 2016. © CS & IT-CSCP 2016 DOI : 10.5121/csit.2016.60617

trust boundaries, OpenID Connect uses the “trust and accept all comers” paradigm. Research & Education (R&E) and many industry sectors mainly depend on the trust model offered by SAML. SAML divides participating organizations into identity providers (IDPs), which are the home organizations of the users running an I&AM system, and service providers (SPs), which operate the services that are to be used in an inter-organizational manner. These entities, i.e., all IDPs and SPs, operate within trust boundaries that are called federations. The trust boundaries are specified by the SAML metadata of the involved entities, which contains information about the communications' endpoints, e.g., X.509v3 signature certificates, used SAML bindings, and URLs for connection establishment. While SAML does not force the pre-exchange of the aggregated, XML-based SAML metadata within geographic and industrial-sector-specific borders, this has become common practice, which means that there are many industry-specific and national federations. The limitation of SAML is, at the same time, that both the IDP and the SP need to possess each other’s SAML metadata before the user can login to the service and user profile information can be transferred from the IDP to the SP. As collaborations are not restricted to such artificial federation borders, *Inter-Federated Identity Management (IFIM)* was introduced. IFIM builds an umbrella federation over the existing federation by policies, contracts, and the pre-exchange of the aggregated metadata of all member federations. Although the additional contracts required between federations and their members make the inter-federation more complex and cumbersome to manage, the inter-federation eduGAIN [2] is significantly growing, already covering 40 national federations in the R&E environment. The growth amplifies another problem: the inter-federation metadata file is huge, making it cumbersome to process even on state-of-the-art hardware and slowing down the user experience.

Therefore, a more scalable approach for metadata exchange via a trusted third party (TTP) was introduced in the project GÉANT-TrustBroker (GNTB) [3]. In GNTB, the user initiates the metadata exchange during the first-time login to a specific service. For that reason, SPs and IDPs solely integrate the necessary metadata instead of the metadata of all IDPs and SPs within the federation. GNTB works as a TTP, which primarily is a central metadata repository. Alternatively, entities can register URLs pointing to their SAML metadata location, which often is publically accessible. In order to establish technically trusted SAML connections on-demand, the TTP extends the so-called SAML discovery service. The service, formally known as WAYF (Where Are You From?), is used to localize the user's IDP and therefore knows both endpoints of the metadata exchange.

The user wants to make use of a service, i.e., he expresses his will to access a specific service at a SP. By that, if IDP and SP technically do not know each other beforehand, the TTP triggers the metadata exchange on-demand. The involved entities can apply the Metadata Query Protocol [4] by Young for the actual metadata exchange, while the TTP orchestrates the overall exchange process. This workflow has been submitted for standardization by IETF in the Internet-Draft Dynamic Automated Metadata Exchange (DAME) [5]. The TTP is only involved during the first contact between IDP and SP and does not interfere in further communication. In order to integrate the metadata automatically, an extension of existing IDP and SP software packages is needed. This eliminates the manual workload for SP and IDP administrators and avoids waiting time for the end users. As only the necessary metadata is exchanged, this significantly improves the scalability of the metadata exchange, while at the same time avoids performance bottlenecks.

For example, the Leibniz Supercomputing Centre (LRZ) is part of the inter-federation eduGAIN, which currently includes about 1,030 SPs. This means that LRZ’s IDP has 1,030 potential trust relationships with SPs plus the metadata of further 1,487 IDPs, which are not relevant for an IDP. In practice, however, only 4 SPs are used at the most, while the metadata of 2,517 entities are exchanged including the own metadata. To complicate it further, also the metadata of all entities of the German federation DFN-AAI are exchanged, which are not part of the inter-federation. With dynamic metadata exchange, the number of received metadata is reduced to 4.

GNTB is currently implemented and improved within the project GÉANT GN4, which operates the inter-federation eduGAIN. The implementation of the TTP is based on the open source SAML implementation Shibboleth. The Internet-Draft is advanced by the REFEDS community, which will establish a new working group for FIM at large scale at the IETF in 2016.

This paper focuses on the design of a service model and the management architecture for this TTP. A management architecture is a framework for management-relevant information, organization, communication, and functionalities. By implementing the management architecture, the TTP becomes a management platform. This management platform adds functionalities to the technical TTP, helping IDPs and SP establishing and managing trust relationships. While the GNTB implementation is tailored for SAML, the TTP and all its functionalities are generically designed, so it can be adopted to other FIM protocols, such as OpenID Connect, without changes. The service model for federated access management, described in Section 2, is based on the Munich Network Management (MNM) service model. The service model for FIM is applied on the TTP, explained in detail in Section 3. The different views provided by the service model help to establish a common understanding about service-related terms and to specify the service functionality additionally to the management tasks. The service model is the basis for the management architecture, described in Section 4. The management architecture describes the organizational, informational, communication, and functional model for a management platform. The management platform adds functionalities to the technical TTP, helping IDPs and SP managing trust relationships, and contributes to service management, which is discussed in Section 5. The paper is concluded by a summary and an outlook to our future work in Section 6.

2. SERVICE MODEL FOR FIM

The MNM service model [7][8][9] is a generic model for IT service management, defining service-related terms, concepts, and structuring rules. It allows to model specific services for the purpose to analyse needs and demands in regard to an appropriate service management with quality of service (QoS) guarantees. The MNM service model consists of three different partial and views: the *basic service model*, the *service view*, and the *realization view*. The basic service model contains the relevant roles and associations. It distinguishes between customer side, provider side, and side-independent aspects. The customer side consists of the basic roles *customer* and *user*, while the role *provider* is part of the provider side. The provider makes the service available to the customer side, whereas more details about the service are provided by the two views.

The service view focuses on the components between service provider and customer side, while the realization view is appropriate to identify objects within the provider side. The combined views provide a detailed service description. The service view, therefore, contains the functionality of the service, i.e., usage for the role *user* and management functionality, which is accessed by the role *customer*. The realization view, in contrast, describes the service implementation and the service management implementation. Both depend on provider-internal resources (hardware, knowledge, and staff) and sub-services. While the service implementation serves to provide the service, the service management implementation includes a service management logic using basic management functionalities and external management sub-services.

As the MNM service model can be applied to arbitrary IT services, also recursively, we design the FIM service model on top of it. Based on the FIM service model, the dynamic automated metadata exchange via a TTP is designed in the service model. The detailed overview of all involved components can help to regard the security of a service and the interfaces. The basic service model for FIM contains the identified roles in the service interaction, as shown in Figure 1 (a). The roles are associated with different domains: the customer side, the service independent side, and the provider side. The notation of the roles is based on SAML, though the service model can be used for other protocols, like OpenID Connect. The customer side contains the IDP as well as the user, as the service is provided by the SP. Furthermore, the IDP can be a member of a federation, the so-called identity provider federation. The SP is part of the provider side, while the service provider can be a member of a federation, the so-called service provider federation. The service itself is independent of provider and customer side. A SAML attribute authority, which extends IDP functionality, can be placed on the side-independent part. This view can optionally be divided into different models as the IDP can be seen as a provider for the customer SP, which needs user information.

3. SERVICE MODEL FOR FIM WITH A TTP

In this section, we demonstrate the application of the MNM service model to FIM by modelling the dynamic metadata exchange via a TTP. This allows to identify the differences between FIM with pre-exchanged metadata and FIM with dynamic metadata exchange via a TTP. Furthermore, the service model explains the interactions between IDP, SP, and the user, while specifying the implementation from a service point of view. This will then become the basis for the management architecture.

In contrast to the basic service model for FIM, the service model for dynamic automated metadata exchange includes the side-independent TTP used to dynamically exchange the metadata. The TTP, as shown in Figure 1 (b), does not need to be part of a federation, though a federation, inter-federation, or any another trustworthy organization could operate it. As a result, the customer side consists of the user as well as the IDP and might include the identity provider federation. The provider side involves a service provider and an optional service provider federation. The side-independent part comprises the service, an optional attribute authority and the TTP.

After applying the basic service model to the dynamic automated metadata exchange via a TTP, the service view of the model is designed. This is shown in Figure 2. In order to better differentiate between service, SP, IDP, and the TTP, another part was added to the service view. The former customer side is renamed into IDP side, while the provider side is now called SP side. Along with the side-independent part a fourth side was introduced: the TTP side.

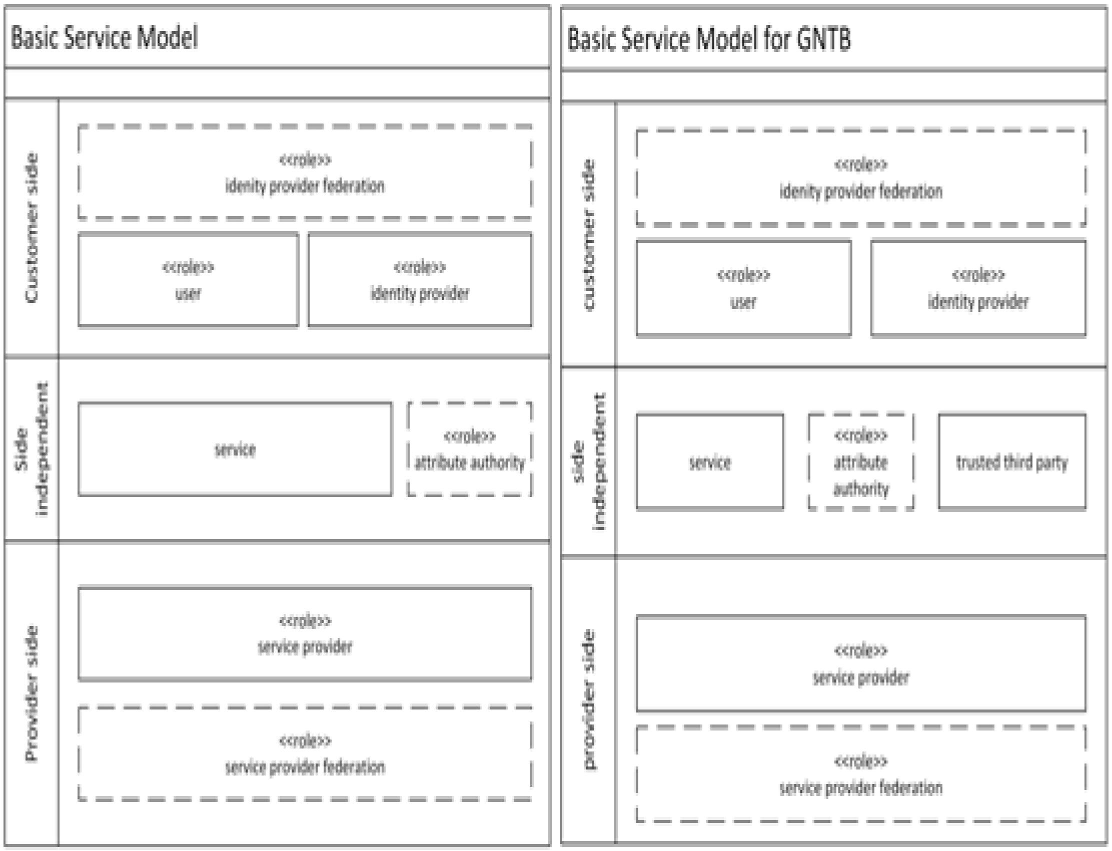


Figure 1: Basic Model for Federated Identity Management (a) without and (b) with a Trusted Third Party

The IDP side includes the user, the IDP, and the customer federation. The user accesses a service through the service client, which is normally a web browser. Intermediate, the service website of the original SP exists. The user information is stored in the local I&AM of the IDP and then passed to the IDP software, e.g., Shibboleth or SimpleSAMLphp. The provider side is basically not changed. An association between SP and service provider federation exists. Theoretically, an SP can have several service provider federations. The SP offers a service, which also makes use of the TTP.

The side independent part is modified in that respect that it makes use of the TTP. The functionality and the QoS parameters of the original service are not changed. As a result, we do not specify them in detail. The TTP is the service, which is used by the user of the localization service. The TTP is involved during the first time contact between the user and the service in order to exchange the metadata. Therefore, the TTP has a connection to the localization service, which is used to localize the user's IDP. The localization service supplies the external service access point of the original SP. The TTP is used by the IDP and SP to mediate service agreements. The TTP organization provides the implementation and the service of the TTP by operating the service. The TTP is therefore another service in the service view, which leads to the following:

- As SPs and IDPs actively use the TTP, they have access to the management functionality. The TTP management functionality provides information about the established connections, which can be used for further statistics and state reports. Since the customers need to be able to manage their registration and configure their level of trust at the TTP, this kind of management functionality is part of the service view. As the TTP is always involved during the first contact and different attack vectors apply, the TTP and the communication needs to be as secure as possible.

- The usage functionality is the initiation of the metadata exchange and the information for the user about the status of the exchange. From the customer's point of view, the management of the metadata exchange is a core functionality. Basic QoS parameters can be specified as availability, accessibility, and the metadata exchange time. The security properties are further parameters.

- Besides the service access point for the user, which redirects the user to the localization service, the customers use a web frontend respectively the extension of their SAML implementation, which is needed for the communication with the TTP. The web frontend functionality consists of the required functions for metadata management and account management. These functions can be used by the extension of the IDP/SP software. The extension furthermore automates predefined workflows. The security of these components is crucial as well.

- After specifying all details of the service, the service agreement needs to be presented.

The realization view in Figure 3 describes the realization of a service from the provider’s point of view. The service in this case is the TTP itself. The hierarchical relations between the services are developed in this view. The service could rely on, e.g., 2nd-level support. As no sub-services are implemented, no corresponding sub-service clients are needed. In addition to sub-services, a TTP provider operates and maintains the service. The information stored in the database and file-based data system is the main resource of the TTP. Another aspect is the service logic; workflows coordinate the usage of the resources. This leads to the realization view as described in the figure. The stored information is managed by the basic management functionality. Both SP and IDP make use of the functionality. The service logic, especially the metadata exchange, acts as user. The user wants to use a service, therefore the metadata needs to be exchanged. The user utilizes the service client to initiate the service logic, which is implemented.

The basic service model as well as both views visualize the TTP being another service within the FIM environment. The TTP interacts with IDP, SP and the user. If federations want to manage their federation via the TTP, they interact with the TTP as well. A TTP provider operates and administrates the TTP. As the TTP needs to provide management functionalities, e.g., in order to securely manage the metadata and trust information, the management architecture is shown in the next section.

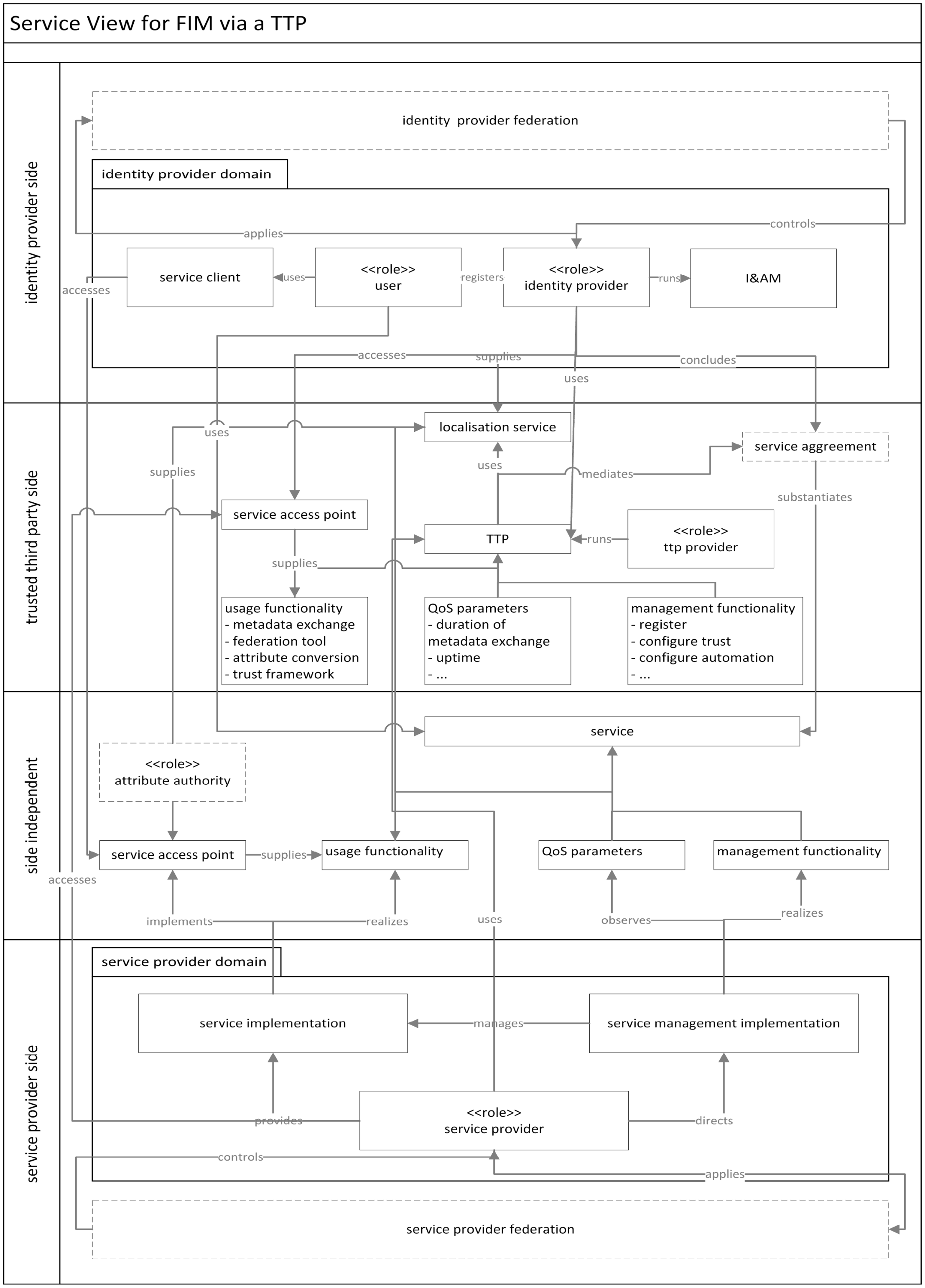


Figure 2: Service View for Federated Identity Management via a Trusted Third Party

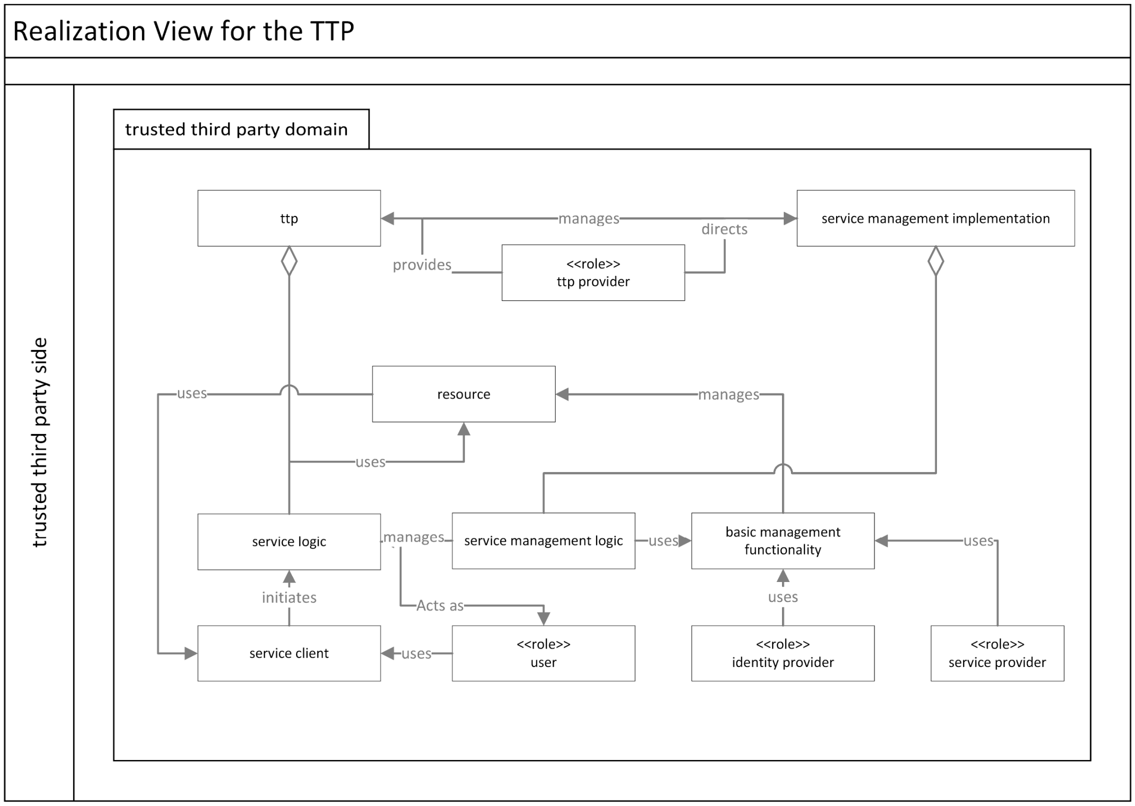


Figure 3: Realization View for the Service Trusted Third Party

4. FIM MANAGEMENT ARCHITECTURE

Standardized management architectures, which are derived from the dimensions of IT management, support the combination of management modules. These architectures are specified by different models [6], which need to be considered when implementing a TTP for dynamic automated metadata exchange:

- The information model defines a standardized format for management information.

- The organizational model specifies the roles of involved systems and their domains. Policies can be part of the organizational model describing targets or processes for technical management. This is shown above in the basic service model.

- Principles and concepts for the exchange of management information between the roles are defined in the organization model. Furthermore, the way of communication is defined, which is then realized by management protocols.

- The functional model divides the functions of the management in sub-functions, which are specified as basic management functionalities. These functions are normally implemented by management platforms and agent systems. The functionalities can be then used by the defined application programming interface (API).

As the security of dynamic metadata exchange is highly relevant for the operation of the service, it needs to be regarded in all models. These models are described for the management platform for FIM via a TTP in the following subsections.

4.1. Organizational Model

The organizational model describes which management domains are necessary for the management architecture with which roles and how these roles interact. Based on the service model for FIM, the domains SPDomain, IDPDomain, AADomain, fedDomain, and interfedDomain can be derived. The SPDomain is the management domain for the SP, representing the local domain of the SP, which provides the original service. The IDPDomain is the local domain of the IDP, which manages the user information. The AADomain is responsible for further user information, while fedDomain and interfedDomain represent the domain of a federation respectively inter-federation. These federation/inter-federation domains can have different structures, from an ad-hoc federation and hub-and-spoke federation to an identity network with different local coverage and differing trust models.

The domains contain several roles. The IDPDomain has *user* as a unique role. AADomain, SPDomain, and IDPDomain include a *general administrator*, which runs and configures the local software. A *relationship manager* is responsible for cooperation, e.g., with the federation and service providers. The *service desk* as the third technical role at AADomain, SPDomain, and IDPDomain is the contact point for incidents and problems. There are probably more roles within the organizations, which are not directly involved with the management platform and therefore not regarded.

The domains fedDomain and interfedDomain have, additionally to relationship manager, administrator, and service desk, several further roles, which are important for the platform. Federations and inter-federations are at some point initiated, either because of a project, a long-term cooperation, like in virtual organizations, or because of FIM as a general purpose. Therefore, the *initiator* is an additional role, which can initiate a federation at the management platform. Later, the role can pass the federation to a *general manager*, which is in control of it. If the service desk cannot solve a problem, technical *specialists* might be asked. The federation needs to be configured, e.g., the trust level needed to participate has to be set, by a *configuration manager*. As changes might have larger impact, a *change manager* is established as an additional role. These different roles have only the needed permissions to fulfil their job. The authentication should be done via SAML. For users without IDPs, local accounts have to be set up.

These specified roles interact via certain interaction channels, which need to be secure. While the administrators are in the background, all problems and incidents are communicated via the established service desks. This methodology is compliant with IT service management good practices such as ITIL and ISO/IEC 20000-1. Relationship managers should first interact via the service desk, though this is not likely to happen in reality. For federations participating in inter-federations and not with single other entities, the interaction is directed via the federation. The management platform can therefore serve as a united communication platform. This also means that the management platform needs the functionality and information for this task.

4.2 Information Model

The relevant information exchanged between domains within the management architecture is designed in the information model. It also specifies different domains and the format of information and resources. The goal of provisioning a management architecture is to handle federations respectively inter-federations as managed objects (MOs) and to automate the metadata exchange via a TTP. The specified information model defines MOs, which are relevant for the management, and their relationships. The definition has to take the expansion of the management platform into account, in order to be able to provide additional functionalities

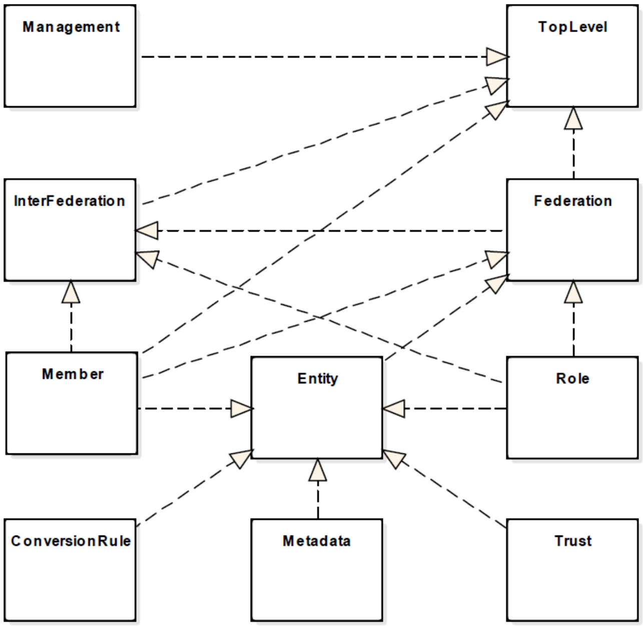


Figure 4: Domains of the Information Model

The information model for the FIM management architecture is shown in Figure 4. The domain specification contains the specifications at large, while the domain TopLevel represents the most generic class of the model. TopLevel contains different root elements and abstract root classes. These root classes, called domains, and dependent domains are the following: federation, inter-federation, entity, member, metadata, trust, conversion rule, and management.

As seen in the organizational model, federations, inter-federations, and entities contain different roles. The managed object federation can have different characteristics. Federations and inter-federation traverse the life cycle; a federation is first initiated, then it is operated, adapted, before it is closed. The representation of the federation is done via the domain federation, including all information about the structure and roles. Each federation consists of several entities, i.e., IDPs, SPs, and AAs. These entities are combined within the model domain entity. An organization can run several entities. Entities might be members of one or several federations. Entities need to exchange metadata, in order to establish technical trust. Entities need to register at the management platform as a prerequisite to exchange metadata. Given that federations consist of different entities, the membership of entities is shaped in the domain member. The domain is responsible for applying, verifying, accepting or denying, adding, and changing of memberships. Entities can exchange metadata independently of federations, if a user wants to make use of a certain service. In order to exchange metadata via the management platform, the metadata needs to be managed. This is the purpose of the domain metadata. Whether SP and IDP are allowed to exchange metadata on demand depends on the risk and the trust in the partner entity. To calculate the trust in the other entity, different tools and standards can be used, such as the levels of assurance (LoA) paradigm. The trust in entities is modelled and compared in the domain trust. In order to understand the user information the IDP has, IDP and SP have to find a common syntax and semantics. In practice, IDPs have to convert the user information, also called attributes, into the SP's format. The domain conversion rule converts user information into the required format. Federations are, as described, seen as MOs. For the management of federations, policies and application processes are important among other things. These aspects of the management are described in the domain management.

4.3 Communication Model

The communication model specifies which entities communicate management information in which format and what communication mechanisms are used for management interventions, monitoring, and asynchronous notifications. The model also described additional services needed to support the communication mechanisms and the embedment of management protocols into the architecture and FIM.

Typical methods for communications are *post*, *get*, *set*, *query*, *create*, *delete*, and *update*. Register is needed to register a management object, while notify is used to inform other management instances. Furthermore, *discover* identifies management instances. These methods are then transferred into workflows, protocols, and an API to provide the needed functionality (described in the next section) and to communicate and interact, as described above. The protocols should be transformed into SAML, as it is the predominant standard for R&E and commercial sectors. The methods need to be able to securely exchange metadata, trust information, and conversion rules. Authorization and publication/discovery of interfaces for interaction channels is another important functionality. The interaction channels need to support loose as well as defined structures of cooperation, while different actions and activities are logged.

The method register is explained as an example. In order to communicate over an interaction channel, the different roles and entities need to be aware of each other. As prerequisite, all entities need to register at the management platform. The registration is the basis to publish a service and therefore make the own service, SP service or IDP user information, available for other entities. Registration is also important for federations and inter-federations, as they can use the management platform as management tool. In this example, an entity registers at the management platform, here described as TTP. It is then verified, e.g., by a certificate. Afterwards, the entity applies at a federation, which first verifies the entity. This might be done automatically, dependent on the application process. If the federation approves, the entity becomes a member of the federation.

4.4 Functional Model

The functional model structures the management into different functional areas and establishes common management functionalities. The goal is to determine generic functional components, which are required for the management of federations and FIM.

The entity level contains IDP, SP, and AA, while the federation and inter-federation level comprises the same functional areas. The functional area conversion rule management is relevant for both, IDPs and AAs. Conversion rules can be created, changed, deleted, downloaded, and validated. As the entity might not want to download and integrate conversion rules automatically, the degree of automation can be configured. Metadata management contains the upload, change, deletion, exchange of metadata, and the configuration of the degree of automation. Also notifications and logging are important. Users as well as entities should be notified, if the metadata exchange fails and the user, when he successfully can use a service. The configuration management handles the configuration with generating, changing, and deleting a configuration. The configuration refers, in this context, to the configuration of both, (inter-)federation and entities.

Besides the technical trust, established by exchanging metadata, further aspects of trust, like behavioural trust, might apply. The trust value can be set, verified, configured, and compared. For example, a SP requires a certain trust level for its service, which depends on the risk for the service. Therefore, the administrator configures the required trust level. When a user of an IDP wants to use a service, the trust level of the IDP is compared to the configured trust level, before the metadata exchange takes place. If the trust level of the IDP is high enough, the metadata exchange takes place and the user can immediately use the service. Otherwise, the administrator of the IDP and the user get a notification about the problem. The most primitive case of trust is some sort of black and white list, while different LoA schemes might be used as well.

By applying for membership in a federation, an entity accepts the use of the federation's policy. Policy management is one functional area at the federation/inter-federation level. The policy, written in XML, should allow a mostly automatic validation of the entity. A parser should counter-check the elements in the entity's metadata, if possible. The relationship manager of the (inter-federation) first has to create such a policy. Later onwards, he can change and delete it. When the policy is changed, members of the federation need to be notified and checked again against the policy. If conflicts arise, the relationship manager needs to solve them. Policy management is closely related to member management, where federations manage their members. This functional area contains the query of member, memberships, and role information. Memberships might need to be changed, applicants accepted or denied. Roles for the administration tool can be changed, and notifications for changes should to be sent. The policy as well as the application process have to be determined, while important actions are logged.

Another functional area for the federation/inter-federation level is service management. The general managers of federations and inter-federations need an overview of all provided services and their usage. While this information has to be queried and visualized, the management information also can be sent to members, if appropriate.

5. FIM SERVICE MANAGEMENT

In order to discuss how service management, the management architecture, and the management platform can improve the TTP, FIM service management is explained in detail. Many IDPs and SPs run their own scripts to parse SAML software log files for relevant events in order to gather data for statistics of service usage. Additionally, a few tools for monitoring SAML entities exist. To create a comprehensive overview for a federation and its members, a unified aggregation architecture needs to be developed, which suits most implementations. In order to ensure this, this extension is separated from the provider implementation.

An overview of all services and their usage as well as generic information about federations and inter-federations should be displayed. Further interesting facts for administrators are:

- Number of participants, IDPs, and SPs
- Number of metadata exchanges
- Number and ranking of used services by popularity
- Overview of trust within a federation
- Overview of conversion rules and their usage
- Overview of technical information
- Overview of queried user attributes in general and per service entity category

The query about service management should be done by a defined method and displayed via a dashboard, to which only administrators should have access. The dashboard should show the numbers but also visualise them and their relationships. For example, the established trust relationships between IDPs and SPs can be shown on a map or globe, allowing information about the dimension of the federation and the trust to be viewed in different scales. While the overview might give an idea about the dimension, a more detailed view shows the entities and the problems of trust, while a drilled-down view shows detailed information about the entity. This information can be used, for example, to facilitate inter-organizational security incident management when users misused their permissions or SPs have gone rogue.

Additionally, the trust information can be encoded by colours, in order to display errors during the metadata exchange, but also other categories, such as:

- IDPs vs. SPs
- Different federations or other pre-established trust boundaries
- Levels of Trust applied by the SAML entities
- Schemas that are used for user attributes
- Age of metadata and X.509v3 server certificates as well as timespan until the certificate expires
- Period of membership
- Number of successful metadata exchanges

The expiration of the certificate can be a source for errors, if metadata with expired certificates is not processed by an IDP or SP.

In order to visualise this information, it needs to be collected beforehand. The collecting server can be the TTP. Additionally, the following components are required:

- Provider: IDP or SP, which provides some kind of statistics. Usually, the data can be read from or determined by parsing SAML software log files.
- Agent: The agent software is used to read, parse, filter, and relay the log events generated by the provider. The agent supports multiple destinations and can apply different filter rules.

- Aggregator: A central instance that aggregates the statistics sent by the providers via the agents.
- Web frontend: Method of displaying the generated statistics.

The agent contains parsers for the specific SAML software in order to determine metrics by parsing log files, reading status pages, or other methods. Filtering is based on the configuration of the responsible administrators. Furthermore, the log files have to be written in a standardised format. This is done by a defined syntax. By applying different filters and aggregators, the administrators can differentiate between detailed local and general federation-wide statistics. After authenticating, the agent's filtered performance data is stored in a database, based on the ID of the provider, the type of the event, and a timestamp.

In order to display statistics, the web frontend requests data from the aggregator's database. The returned data is filtered according to the scope of the user's request. Depending on the configuration of the client, the event is then sent to the aggregator immediately or interval-based, which in turn informs the web frontend of the updated data and refreshes the display in the user's browser. The statistics can be a functionality of a portal, combining all the different functionalities from the functional model.

6. Conclusion and Outlook

Dynamic automated metadata exchange (DAME) for FIM enables the on-demand, user-triggered exchange of SAML metadata between IDPs and SP across current federations' borders. The scalability of the metadata exchange in federations and inter-federations is improved at the same time, as only the really necessary metadata is exchanged. It therefore increases the automation and scalability of formerly manual implementation steps by administrators. Consequently, the users can immediately use a new service without extended waiting periods due to the involvement of administrators.

In order to create an overview of the changed architecture and the service of the TTP, the MNM service model was applied to both, traditional FIM and FIM via a TTP. The MNM service model helps to distinguish between customer and service provider, and gives a neutral view on the service. The service view for FIM via a TTP added another side, the trusted third party side, to the view, as the service TTP is an additional service. The TTP can be provided by a federation or inter-federation operator, helping members to connect to the outside world.

Based on the service view and the realization view for FIM via a TTP, the management architecture was designed. While the technical TTP helps to exchange metadata on demand, the management architecture describes functional areas relevant for FIM. Federations and entities can use the management platform to manage metadata, members and make use of further functional areas. The approach of dynamic metadata exchange with the addition of a management platform, as described in this paper, allows for example the configuration of trust, reducing the risk of data loss and prohibited usage of services. Federations and inter-federations can make use of the management platform to manage their members, while entities have a tool to manage metadata and conversion rules. The organizational, information, and communication model describes the information, interactions, interfaces, and roles within organizations, which need to be regarded during the next step, the design and implementation of the management platform. This leads to an extended TTP, helping organizations to manage FIM and gather statistics about their FIM usage.

Further research topics relate to a detailed security and risk analysis of such an extended TTP as well as the trust between two entities. Though the technical trust is exchanged via the metadata, the quality of the entity could be assured or estimated by a level of assurance and dynamic trust. Furthermore, visualization of information should be regarded in more detail, especially with the focus on inter-organizational security incident management.

ACKNOWLEDGEMENTS

The authors wish to thank the members of the Munich Network Management (MNM) Team for helpful comments on previous versions of this paper. The MNM-Team, directed by Prof. Dr. Dieter Kranzlmüller and Prof. Dr. Heinz-Gerd Hegering, is a group of researchers at Ludwig-Maximilians-Universität München, Technische Universität München, the University of the Federal Armed Forces, and the Leibniz Supercomputing Centre of the Bavarian Academy of Sciences and Humanities.

REFERENCES

[1] Cantor, S., Kemp, J., Philpott, R., and Maler, E.: Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0. OASIS Security Services Technical Committee Standard (2005)

[2] GÉANT: eduGAIN technical site. https://technical.edugain.org/status.php [Online; 12.01.2016]

[3] Hommel, W., Metzger, S. and Pöhn, D.: Géant-TrustBroker: Dynamic, Scalable Management of SAML-Based Inter-federation Authentication and Authorization Infrastructures. ICT Systems Security and Privacy Protection, Springer Berlin Heidelberg (2014)

[4] Young, I., Ed.: Metadata Query Protocol - draft-young-md-query. http://datatracker.ietf.org/doc/draft-young-md-query/ [Online; 12.01.2016]

[5] Pöhn, D.: Dynamic Automated Metadata Exchange - draft-poehn-dame. https://datatracker.ietf.org/doc/draft-poehn-dame/ [Online, 12.01.2016]

[6] Hegering, H.-G., Abeck, S. and Neumair, B.: Integrated Management of Networked Systems - Concepts, Architectures, and Their Operational Application. Morgan Kaufmann Publishers (1999)

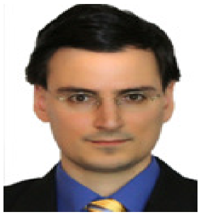
[7] Garschhammer, M., Hauck, R. and Hegering, H.-G. et al.: Towards generic Service Management Concepts - A Service Model Based Approach. Proceedings of the 7th International IFIP/IEEE Symposium on Integrated Management (IM 2001)

[8] Garschhammer, M., Hauck, R. and Kempter B. et al.: The MNM Service Model - Refined Views on Generic Service Management. IEEE Journal of Communications and Networks, vol. 3, no. 4, pp 297-306 (2001)

[9] Garschhammer, M., Hauck, R. and Hegering, H.-G. et al.: A Case-Driven Methodology for Applying the MNM Service Model. Proceedings of the 8th International IFIP/IEEE Network Operations and Management Symposium (NOMS 2002)

AUTHORS

Daniela PÖHN received a university master degree in Computer Science from the University of Hagen, Germany, in 2012. She was engaged in the IT industry as a full-time software developer during her studies, before she joined LRZ as a Ph.D. candidate in September 2012. Her main research focus is on identity management.



Wolfgang HOMMEL has a Ph.D. as he teaches information security lectures and labs. His research focuses on information security and IT service management in complex large-scale and inter-organizational scenarios.