Risk Management for Dynamic Metadata Exchange via a Trusted Third Party

Daniela Pöhn
Leibniz Supercomputing Centre, Boltzmannstr. 1, Garching n. Munich, Munich, Germany

Keywords: Federated Identity Management, Metadata, SAML, Metadata Exchange.

Abstract: Inter-organizational access to IT services based on the predominant standard of Federated Identity Management (FIM), the Security Assertion Markup Language (SAML), suffers from scalability issues related to metadata exchange. In order to overcome these issues, an approach for automated metadata exchange between Identity Provider (IDP) and Service Provider (SP) via a Trusted Third Party (TTP) is presented in this article. Based on the architecture, risk management with threats and counter measures is applied by using a risk management template. Special emphasis is put on the secure design of the automated metadata exchange.

1 INTRODUCTION

Medium-sized and large organizations, like universities and companies, typically provide several information and communications technology (ICT) services to their members. These can be, e. g., email, web collaboration tools, and more specific services, like exam management service. In order to authenticate, a technical identifier, commonly referred as username, is assigned to each member. By providing the username and credentials, the user gets access to these services. While the local, normally centralized Identity & Access Management (I&AM) enables organization wide solution for identity management, this becomes more complex when several organization collaborate.

Such a collaboration can be a research project or a combined development of a product, reducing the costs for all participating companies. In order to store and manage the user information only at one place, Federated Identity Management (FIM) was established. It is either based on the trust all comers principle of OAuth (Hardt, 2012) and OpenID Connect (Sakimura et al., 2014), as many web applications do, like Facebook and Google just to name two. The other possibility is the usage of Security Assertion Markup Language (SAML) (Cantor et al., 2005a), which has closed trust boundaries. SAML is used in the Research & Education environment as well as in companies, like in the automotive federation Odette SESAM (Odette, 2009). The home organization of the user is called within SAML-world – as well as in this paper – Identity Provider (IDP), while the provider of the service is referred to as Service Provider (SP). A formally collaboration of IDPs and SPs is called a federation. In research and education, these federations operated by national research and education networks (NRENs) can include hundreds to thousands of universities and research institutions with all their students, staff, and researchers. Examples of those NREN federations are DFN-AAI in Germany (DFN-AAI, 2015) and InCommon in the US (InCommon, 2015).

Although these specific federations by geography and industry-sector are not imposed by FIM technology and protocols, it has become a reality. Most countries and sectors run their own federation. In order to cooperate internationally, so called inter-federations are built, still excluding several potential members. Let's assume a researcher is involved into a research community, also called virtual organization, which provides several services essential for his work. The organizations participating in the community are spread over the world. At the same time, the university of the researcher, also called IDP, is member of a national federation. Other IDPs and SPs are part of this national federation, in order to make use of FIM. As common protocol, they use SAML as it has fixed trust boundaries in comparison to OpenID Connect. In order to know the endpoints and to have a circle of trust, they pre-exchange their metadata (Cantor et al., 2005b). Metadata includes information about the information endpoints, but also contact information, and required attributes. In SAML-world, IDP

Pöhn, D.
Risk Management for Dynamic Metadata Exchange via a Trusted Third Party.
DOI: 10.5220/0005651702270234
In *Proceedings of the 2nd International Conference on Information Systems Security and Privacy (ICISSP 2016)*, pages 227-234
ISBN: 978-989-758-167-0

and SP can only make use of FIM, when they have each others metadata. Although SAML does not explicitly specify the pre-exchange of aggregated metadata, it is current practice. Since the national federation is member of an inter-federation, e. g., eduGAIN, the metadata of all members of the inter-federation is as well aggregated and then distributed. In the case of eduGAIN this comprises 40 federations with more than 2,000 entities (GÉANT, 2015). As a result, services can only be used within these trust boundaries. This also means that the researcher's virtual organizations need to set up their own virtual federation, as not all members are participating in the inter-federation, or it needs to make use of a Homeless IDP, integrating all users from outside the inter-federation.

This example explains the main problems of FIM with SAML. Although FIM is widely used, the coverage and scalability are known issues. The size of the aggregated metadata is increasing, when more federations and providers are participating. The implemented solutions are only sector-wide, e. g., Odette SESAM in the automotive industry, while eduGAIN is used in NREN federations. The approach the inter-federation eduGAIN uses comes to its boundaries, as the approach is not scalable. The aggregators and parsers for the metadata can hardly cope with the increasing amount of data. Since more and more services are offered on-demand, the practical problem and relevant question is, if the SAML metadata, required to make use of FIM, can be exchanged securely on-demand. This article adds security considerations and a risk management based on a template to the GÉANT-TrustBroker approach (Pöhn et al., 2014). The new approach, initiated by the eduGAIN operators (GÉANT project), needs to be as secure as FIM with SAML can be, even though new components and workflows are introduced.

The following section contrasts the architecture of a Trusted Third Party (TTP) for dynamic metadata exchange with current state of the art and practical approaches. Section 3 explains a template for risk management, which is applied to the approach of dynamic metadata exchange via a TTP in the following sections. Section 4 describes possible threats for the TTP, while Section 5 characterizes actors against the TTP. The following Section 6 describes counter measurements, which need to be taken into account during the implementation and the operations. Last but not least, the paper concludes in Section 7 with the results and further research questions.

2 DYNAMIC METADATA EXCHANGE VIA A TTP

In order to help administrators with the management of their metadata, the Swiss federation SwitchAAI was the first NREN federation to develop a web service called Resource Registry. The Resource Registry lets entities register their metadata and update entity information, before the national metadata file is aggregated and distributed, based on all uploaded metadata files. Further NREN federations adapted this solution. A newer practical solution is the Public Endpoint Entities Registry (PEER) by Young et al. (Young and Joie, 2009). The concept of PEER and the implementation called REEP is that any entity, independent of the federation and protocol, can use the registry. Therefore, it shifts from several federations-several tools to one central tool, whereas the metadata is still aggregated by federations and inter-federations. Furthermore, manual steps are required to exchange metadata.

The approach of a TTP for dynamic metadata exchange works similar to PEER, as any entity can register and upload their metadata. Alternatively, they can set a pointer to their local metadata location, which is public. In order to establish technical trust on-demand, the TTP extends a localization 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, the TTP triggers the metadata exchange on-demand. This approach is also described in (Pöhn et al., 2014), where the state of the art, basic concepts, workflows, and database design were explained. As only the necessary metadata is exchanged, this significantly improves the scalability of the metadata exchange, while at the same time avoids performance bottlenecks.

Young submitted an Internet-Draft (I-D) called Metadata Query Protocol (Young, 2015). Another I-D, SAML Profile for the Metadata Query Protocol, describes the profile for SAML. By the Metadata Query Protocol, metadata can be retrieved by simple hypertext transfer protocol (HTTP) GET requests. This theoretically allows dynamic metadata distribution.

The TTP can re-use the Metadata Query Protocol, letting IDPs and SPs query metadata on-demand. Either the TTP knows the metadata location at the entity or it stores it in a metadata repository. The authenticated user triggers the metadata exchange by an extended

IDP discovery workflow based on SAML, as specified in the I-D Dynamic Automated Metadata Exchange (DAME) (Pöhn, 2015a). The TTP orchestrates the metadata exchange, while the exchange itself can be done by the Metadata Query Protocol.

Similar to the described TTP, the approach Trust Service Provider (TSP) by Jian Jiang et al. (Jiang et al., 2011) requires each entity to register at the central TSP service. The TSP brokers the trust of two entities during runtime. The metadata is downloaded from the TSP and might be stored in the cache of an entity. If a user wants to make use of a service, the SP needs to query his local cache about the metadata of the IDP. If the SP does not have the needed metadata, it sends a request to the TSP. The IDP is required to send another request, in order to fetch the metadata of the SP. The metadata files have version numbers. If the IDP is outside the federation, the SP of the home federation of the IDP can be used as an IDP-Proxy for indirect authentication. This also means, that the SP needs to cache the assertion of the home IDP and that each SP needs to run an IDP-Proxy. Additionally, the version number is unnecessarily added to the metadata's name.
The TTP, in contrast, does not need version numbers and IDP-Proxys, as every federation and entity can register at the TTP. Furthermore, federations can run a distributed version of the TTPs, which communicate with each other and exchange metadata across TTPs. Therefore, entities do only need to register once. The approach of the TTP automates the technical integration of new metadata on the SP as well as on the IDP side. In order to integrate these information automatically, an extension of existing software is needed. The extension of the software can automate the manual steps by the information already included into the metadata. This eliminates the manual workload for SP and IDP administrators and avoids waiting time for the end users. This is particularly the case as the metadata can be exchanged across current federations' boarders.

The approach Dynamic Identity Federation by Md. Sadek Ferdous and Ron Poet (Ferdous and Poet, 2013) concentrates on the dynamic trust. Dynamic Identity Federation distinguishes between fully trusted, semi-trusted, and untrusted entities. Authenticated users are allowed to add SPs to their IDPs, while SPs add the IDPs to their local trust anchor list (TAL) for further usage. The user establishes the trust by generating a code at his first authentication. He then informs the SP about the code and the EntityID of the IDP. After verification, the SP generates a request with two invisible fields, i. e., MetaAdd and ReturnTo. Both fields are used for the metadata exchange, while the IDP needs to evaluate the value of MetaAdd. When the user gives his consent, the IDP adds the chosen SP to the list of semi-trusted entities. Semi-trusted entities are not allowed to receive sensitive attributes. Untrusted entities are given the National Institute of Standards and Technology (NIST) level of assurance (LoA) 1. If the SP is not known by the IDP, a proxy could be used complicating the trust establishment. The trust establishment via the user generating and forwarding a code is not user friendly, while both invisible fields are not necessary. The fragmentation into trusted, semi-trusted, and untrusted entities as well as the usage of NIST LoA 1 does not reflect real world with its different LoA schemes and the trust relationships. As with the IDP discovery service, all relevant information are integrated within the SAML messages, additional fields are not required. If the user trusts an SP, the SP is added to the IDP's TAL, which consists of all downloaded and integrated metadata. If this fully automated trust is not wanted, the IDP and SP can configure their LoA and the level they want from their counterpart. If, e. g., the IDP matches the level required by the SP, the metadata is exchanged on-demand, while otherwise the administrators and the user are notified. Since many different LoA are used within federations and most NREN federation have around NIST LoA 1 or 2, a more fine-grained LoA schema is needed, which can also map different schemes. Furthermore, a federation administration tool is implemented for additional quality assurance.

Summing up, the TTP is a central service for on-demand metadata exchange for IDPs and SPs. It allows scalable metadata exchange, which is user triggered and based on standard SAML workflows. By software extensions it automates manual workflows and widens the trust boundaries, while, at the same time, providing tools for quality assurance and trust assurance. As the TTP is not an IDP proxy, it is not involved in further communication. This also reduces the likelihood of a bottleneck. Furthermore, it could be operated distributively, as described in (Pöhn, 2015b). The theoretical approach of a TTP is currently implemented and improved for piloting within the project GÉANT, which runs the inter-federation eduGAIN. In order to have a secure implementation and all needed functions, the risk and security management is regarded. While the proof of concept implementation of the TTP is tailored for SAML, the TTP and all its functionalities are generically designed, so it can be adopted to further protocols without changes.

For the researcher described above, it means that his IDP and all the SPs of the community have to reg-

ister at the TTP as a prerequisite. If the researcher wants to use a new service of the community, he is forwarded to the extended discovery service of the TTP. By choosing his IDP, he automatically triggers the metadata exchange between IDP and SP. Since both have configured fully automated metadata exchange and their LoA is high enough, the metadata is exchanged on-demand and directly integrated into the local configuration. The researcher therefore does not have to wait until he can access the service. In order to have the researcher securely access the service, the risk and security of the new components has to be regarded, before it is piloted within the GÉANT project.

3 RISK MANAGEMENT

In order to achieve a technology readiness level TRL7 and following existing good practices and international standards, e. g., ISO/IEC 27001, a risk assessment takes place. Hommel et. al (Hommel et al., 2015) present a risk management template, which operationalizes and supports the continuous management process. This risk management template was applied to the TTP. As the TTP allows the automated metadata exchange, which possibly leads to the release of personally identifiable information, the critically has to be set to high. Therefore, appropriate security measures have to be implemented.

The first step of risk management is the definition of primary and secondary assets. The secondary assets and the operational risk management are regarded in Section 4. Possible events threatening components of the dynamic metadata exchange are, e. g., flooding the TTP with metadata exchange requests, as described above. Assessing the threat event, the likelihood as well as impact of the example must be seen as high. The high risk value needs further action. To overcome the threat, the TTP requires user authentication before the metadata exchange is triggered. Furthermore, an integrated rate limiter slows down the number of allowed requests sent to the TTP.

All possible risks are regarded, by listing assets, analyzing the risks of all components and the dynamic metadata exchange itself. A wide range of possible risks are shortly explained in the following sections. Based on the risks, possible actor models and counter measurements were inspected. This lead to a protocol, which is as secure as possible, and to a secure designed TTP. In addition, detective and responsive measures need to be established as well. As an example, the local software and the TTP need to be monitored. Further risks can be mitigated by control by federation operators and the use of an assurance frameworks.

4 ASSETS AND THREATS

The first step in risk management requires the definition of primary and secondary assets. While primary assets are usually the core business processes and workflows of an organization, the secondary assets support these processes.

4.1 Assets

In the case of dynamic metadata exchange, the TTP enables the immediate access to online services. Therefore, it can be seen as an enabler and innovator for the collaboration of organizations. The secondary assets are usually categorized as hardware and software, information exchanged and processed by service components. The operational risk management focuses on the technical components of the TTP, i. e., the extension of the entities' software, the TTP itself, including the underlying network infrastructure, and the exchanged data. As the TTP is the main component for the automated metadata exchange, it needs to be highly secure. Therefore, the security of the TTP, respectively distributed TTPs, and the extensions are discussed in this section, followed by counter measures in the following section. First the changes due to the new approach are shown, before all components are regarded. In order to have an overview, different malicious actors are shown afterwards.

Federations and inter-federations currently run metadata aggregators, which aggregate the metadata of all members. In order to obtain and distribute metadata, push and pull mechanisms along with a web tool for metadata management were implemented. Federations normally run centralized discovery services for IDP location. By the approach described in this paper, the following changes appear:

- TTP: instead of a standardized localization service, the localization service is extended with a relational database, an application programming interface (API), a web frontend, and an orchestration service for metadata exchange.
- Federations: federation administrators manage their federations via an administration tool, which is part of the web service of the TTP.
- IDP/SP: IDPs and SPs use an extended software for metadata exchange and integration, while scripts make use of API calls.

- Communication itself: while the discovery workflow of SAML is extended for on-demand metadata exchange, HTTP requests and responses are used for API calls. If the TTPs are distributed, the communicate between TTPs and a register for the TTPs is added.

In principle, the approach consists of server, virtual machine, web server, web application, extension of the software, database, SAML communication, extended communication, and a network of TTPs.

4.2 Threats

A threat scenario template, as described in (Hommel et al., 2015), can be used to point out possible events threatening the TTP. The template characterizes an event by actors, threat type or category, the aim, and the likelihood as well as the impact. Based on the changes, the threats by components, i. e., assets, are shown, before they are explained based on the actors.

The web application of the *TTP* has typical threats, like coding errors and bugs in used software. Furthermore, the registration of a faked entity might lead to a collection of user information or the unauthorized usage of services. The simulation of a higher trust can also lead to the unauthorized usage of services, while malicious code could, e. g., read or change the database underneath or use the web application to spread malware. Also obtaining surreptitiously higher permissions could lead to the exclusion of entities and further misuse. As the extended localization service relies on the integrity and authenticity of the TTP, it is important that the TTP is as secure as possible. Since the localization service let the user trigger the metadata exchange, the availability of the service is crucial. The underlying services and the database also need to be secure and available.

The extension of the *entities' software* enables the automated exchange of metadata and integration into the local configuration, which can be at the same time another threat. As the configuration sets the attribute filter, which is responsible for filtering the user attributes, an inaccurate configuration can lead to the disclosure of user information. On the side of SPs, an erroneous configuration can lead to the use of services, for which users are normally not permitted.

By the automated exchange of metadata, entities can cooperate without being member of the same federation or inter-federation. As a result, the *communication* between entities and TTP is a further risks, given that a man in the middle potentially can listen and change the communication. The authentication and verification of all participants is especially crucial, if the TTPs are distributed (Pöhn, 2015b), since faked TTPs might get registered. These threats can be used to attack the TTP or participating entities by actors with different motivation, origin, knowledge, and traceability.

5 POSSIBLE ACTORS

The different actors are explained in this sections, divided into IDP/SP, user, federation, and external actors.

5.1 Entities as Actors

An IDP or SP might act as an attacker against other *entities* or the *TTP*, if his system was compromised or an administrator misuses his permissions, e. g., as insider threat. One possible motivation to misuse the permissions is to fake identities or increase the trust, in order to use a service. While this is technically possible, the changes are traceable. By getting higher permissions at the TTP, other entities might be excluded or other entities might be registered. Further manipulation, like level of trust, is possible. The efforts are higher than at the first manipulation, though this attack should be traceable by logfiles. By including malicious code, the web application, scripts, the server, or the database might be changed. Different motivations apply for this attack, as by extracting the data, the actor might profit financially, while it is also possible to update entities, permissions or the trust. The traceability for this attack is more difficult, while the ability of the actor varies from the sort of bug. At *communications*, if an administrator tries to hijack a session of another entity, information about the entity, e. g., metadata, and trust level, as well as of the user can be changed. The attack has to be targeted, which means more efforts. At the same time the traceability is less. The information can also be changed for another entity, if social engineering is used to get the account information. IDPs and SPs might try to exchange as many metadata or other data as possible to the TTP, either to attack the TTP itself or one entity, by this denial of service (DoS) attack. This attack is mitigated by the DAME workflow, which requires authentication before the metadata exchange is triggered. Therefore, if not a bug in the implementation let actors exchange data, the attack is traceable. Even though the probability of an attack by an IDP or SP is low, these attacks need to be considered. Attacks by inside threats are the hardest to trace back and protect, while others are mitigated by the design of the workflows and the TTP.

5.2 Users as Actors

Similar to IDP and SP as attackers, the likelihood of an user to become an actor is low. It might the case, if a user wants to harm an entity, to make use of further services, or he wants to test his abilities or his system was compromised. If a user exchanges as many metadata as possible, the DoS attack can slow down a service until it is out of service. Since the user needs to authenticate for the metadata exchange, the traceability is simple. Another possible attack is a masquerade attack, where a user tries to collect accounts. This attack is not TTP-specific, as well as the social engineering, though the impact might increase.

5.3 Federations as Actors

As the *TTP* has an administration tool for federations, this interface can be misused, in order to affect an entity or federation, to gain financial advantage or, if the federation is operator at the same time, to affect entities from specific countries. Equivalent to IDP and SP, the federation administrator can include an entity to attack other entities, to collect user information or to exclude a valid entity. For collecting user information, users have to choose the service and give consent to the data release. These attacks are basically traceable, if not the logfiles are changed. If malicious code or malicious code is used, this seems to be more difficult.

When the federation is also the operator of the TTP, further attack vectors are possible. For example, administrators can misuse the resources, in order to steal or change data, as described beforehand. The infrastructure of the TTP can be attacked by an internal threat. To sum it up, internal threats are hardest to identify, while the technical threats are taken into account.

5.4 Externals as Actors

Attacks of externals can be targeted to the *TTP*, but also to specific entities. The knowledge ranges from script kiddies to professional hacker. While script kiddies are comparably easy to defend, professional hackers with money and time are a bigger threat. The threat also depends on the entities and federations using the TTP. The localization service and the TTP with its database is especially critical, because of the amount of data and the exposed position. Most likely attacks are:

- Malicious code, in order to collect data, to protocol inputs, to attack specific entities or all users, to name few examples.
- Structured Query Language (SQL) injection, for querying the database or to change data.
- Replay attacks by replaying overheard communication messages with the goal to receive further information about the TTP and the communication.
- DoS and distributed DoS (DDoS) attacks against the availability of the TTP or entities.
- Attacks against the user management.
- Session Hijacking and Single sign-on attacks.

Additionally to the attacks explained beforehand, an external might try to sniff the *communication* between IDP, SP, and TTP, in order to get information, e. g., to gain financial profit. The traceability of this attack is harder. Another possible attack by an external is the registration of a federation, which sounds similar to well-known federations. The aim is to get entities into the federation, receive information, and to harm the known federation. If the actor requires a specific certificate, audit, or payment, the attack has also financial consequences. The attack can be partly traced by the database and log files, though it might be difficult to re-obtain the paid money. With distributed TTPs, an actor might try to set up an own TTP, in order to attack or exclude TTPs. The actor has first to implement an TTP and should understand the communication between different TTPs and entities. If the actor wants to attack TTPs directly, the TTP first needs to be adapted. While the effort is comparably high, the traceability might be difficult. Similar to federations, the actor can register a TTP with a similar name to a well-known TTP. The goal here is to have many entities and federations registered for collecting data and, in the worst case, also to gain financial benefits. External actors normally have different motivation than participants of the TTP, attaching importance to these attack vectors.

6 COUNTER MEASURES

In order to either prevent or detect attacks, different counter measures can be applied. For the components listed in the previous section, important counter measures are the following:

- The web application of the *TTP* has authentication and authorization, validation of input and output, session management, error management, and log files. Additionally, a secure connection to background systems as well as fine grained permissions are implemented. The validation of the registration is checked by certificate, email address

or a specific page on the web server, before an entity can actually let metadata exchange. The localization service only allows metadata exchange for registered entities. The trust is evaluated, while all important actions, like metadata exchanges, are logged. Logging mechanisms are activated at the database, where passwords are hashed and salted, and hashes are used to validate the integrity. Furthermore, all components of the TTP are monitored. *Federations* can additionally verify entities.

- The implementation of the *IDP/SP software extension* has to be as secure as possible, in order to prevent the leakage of personal information. The administrators can configure the trust and assurance as well as the degree of automation. Furthermore, users have to authenticate before metadata can be exchanged, while, at the same time, signatures, IDs for messages, and a short validation time for asseverations are used.
- The *communication* is secured either by Secure Sockets Layer (SSL) or Transport Layer Security (TLS). Distributed TTPs are registered with a certificate for validation with at least Domain Name System Security Extensions (DNSSEC) or, preferably, DNS-based Authentication of Named Entities (DANE). Certificate transparency can be added.

Counter measures can be distinguished between organizational and technical measures as well as between preventive, detective, and responsive measures.

6.1 Organizational and Technical Measures

Organizational measures regulate, who has which permissions for rooms and servers and how log files are going to be evaluated. An additional security incident response process can help to find threats, analyze an attack, re-establish the target stage, and to document. In order to make use of LoA, the local LoA has to be measured or the requirements need to be estimated.

Technical measures help to prevent and detect attacks. Random numbers as session ID, tokens, and session timeouts need to be considered during design and implementation as well as a validation of the entity by certificate, email address or a specific page on the web server. IDPs and SPs should use either tokens or FIM to authenticate at the TTP. Another example for technical measures is the authentication of the user, before the actual metadata exchange.

6.2 Preventive, Detective, and Responsive Measures

A different classification divides the measures into preventive, detective, and responsive. Preventive measures for the dynamic metadata exchange via a TTP include all measures, which need to be taken before a possible attack can occur. Examples are technical measures, like firewalls and salted passwords at the TTP, as well as the usage of tokens and session IDs during the communication. Detective measures observe an attack, which could be done by monitoring systems, such as an intrusion detection system. Last but not least, responsive measures include security incident response process, the automatic reconfiguration, audits, and backups. These measures and threats were taken into account at the risk management, helping to secure the design, extensions, and the implementation.

7 CONCLUSIONS

The automated SAML metadata exchange enables user-triggered exchange of 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 necessary metadata is exchanged. The approach of dynamic metadata exchange via a TTP supports the fully automated technical setup of FIM-based authentication and authorization data exchange. It therefore increases the automation and scalability of former manual implementation steps by administrators. Consequently, the users can immediately use a new service.

In order to have a secure service, which is important for the acceptance, the risk management was applied and taken into account. The risk management was initiated by the description and the application of a risk management template. First, the assets and the differences to current FIM was explained. Based on the differences, the vulnerabilities and threats were discussed, before possible actors against the TTP were shown. This analysis show, that the TTP is the biggest target in this setup and therefore has to be secure. At the same time, as it is only involved during the metadata exchange and a distributed setup can be operated, the probability of a bottleneck is reduced. Counter measures, divided into the different classification, demonstrated possibilities to overcome the threats. These threats and counter measures need to be taken into account for the improved implementation, before it can be piloted.

Further research topics relate to the level of assurance respectively 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.

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

Cantor, S., Kemp, J., Philpott, R., and Maler, E. (2005a). Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0. Technical report, OASIS.

Cantor, S., Moreh, J., Philpott, R., and Maler, E. (2005b). Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0. Technical report, OASIS.

DFN-AAI (2015). DFN-AAI – Authentication and authorization infrastructure. https://www.aai.dfn.de/en/ [accessed: 2015-11-30].

Ferdous, M. S. and Poet, R. (2013). Dynamic identity federation using security assertion markup language (saml). In *Policies and Research in Identity Management*, pages 131–146. Springer Berlin Heidelberg.

GÉANT (2015). edugain membership status. https://technical.edugain.org/status.php [accessed: 2015-11-30].

Hardt, D. (2012). The OAuth 2.0 Authorization Framework. Rfc6749, IETF.

Hommel, W., Metzger, S., and Steinke, M. (2015). Information Security Risk Management in Higher Education Institutions: From Processes to Operationalization. In *Proceedings of the 21th congress of the European University Information Systems Organisation*, pages 190–201. EUNIS.

InCommon (2015). About InCommon. http://www.incommonfederation.org/about.html [accessed: 2015-11-30].

Jiang, J., Duan, H., Lin, T., Qin, F., and Hong, Z. (2011). A federated identity management system with centralized trust and unified single sign-on. In *Communications and Networking in China (CHINACOM), 2011 6th International ICST Conference on*, pages 785–789. IEEE.

Odette (2009). Odette sesam specification for building up federated single-sign-on (sso) scenarios between companies in the automotive sector – draft of 15.07.2009. Technical report, Odette.

Pöhn, D. (2015a). Dynamic automated metadata exchange – draft-pohn-dame-03. Work in Progress.

Pöhn, D. (2015b). Topology of Dynamic Metadata Exchange via a Trusted Third Party. In *GI-Edition 251 - Open Identity Summit 2015*. GI.

Pöhn, D., Metzger, S., and Hommel, W. (2014). Géant-TrustBroker: Dynamic, Scalable Management of SAML-Based Inter-federation Authentication and Authorization Infrastructures. In *ICT Systems Security and Privacy Protection*, pages 307–320. Springer Berlin Heidelberg.

Sakimura, N., Bradley, J., Jones, M., de Medeiros, B., and Mortimore, C. (2014). OpenID Connect Core 1.0. Technical report, OpenID Foundation.

Young, I. A. (2015). Metadata Query Protocol – draft-young-md-query-05. Work in Progress.

Young, I. A. and Joie, C. L. (2009). Interfederation and metadata exchange: Concepts and methods. http://iay.org.uk/blog/2009/05/concepts-v1.10.pdf [accessed: 2015-11-30].