A SAML Metadata Broker for Dynamic Federations and Inter-Federations

Daniela Pöhn, Stefan Metzger, and Wolfgang Hommel
Leibniz Supercomputing Center
Munich Network Management Team
85748 Garching n. Munich, Germany
Email: [poehn,metzger,hommel]@lrz.de

***Abstract*—We present the design and concept for a new service to enable multi-tenant information and communications technology (ICT) service user authentication and authorization (AuthNZ) management in the research and education environment, called Géant-TrustBroker. Géant-TrustBroker complements eduGAIN, an umbrella inter-federation established on top of the national higher education federations in more than 20 countries worldwide by the pan-European research and education network GÉANT. Motivated by real-world limitations of eduGAIN, Géant-TrustBroker enables on-demand establishment of dynamic virtual federations, reducing the manual workload for the participating organisations by a high level of automation. Manual interaction is only necessary when organisational trust-building measures, such as signing a formal contract between providers, are necessary. Furthermore, the efforts of converting user information attributes to the format of a service provider is reduced by a conversion rule repository. We contrast Géant-TrustBroker with other state-of-the-art approaches and present its core workflow and the internal technical architecture.**

Keywords–Federated Identity Management; SAML; Shibboleth; Inter-Federation; Trust-Management.

I. Introduction

Any medium-sized and large organisation, e. g., universities or business companies, provide several ICT services to their employees, students, and also partners and guests. To access, e. g., email, web collaboration and printing services, a unique identifier, usually an username, is assigned to each user. All required information about users is provided by authoritative Lightweight Directory Access Protocol (LDAP) servers or relational database management systems for a centralized Identity & Access Management (I&AM) solution. This allows a simple provisioning procedure for new users and a deprovisioning process in the case of employees leaving a company.

Inter-organisational identity management is necessary when either an organisation's member shall access external services, for example, because a service, such as email, has been outsourced to a third party provider, or when members of several organisations shall work together on a common project, such as a research project, which involves multiple universities and external partners. Existing solutions for authentication and authorisation infrastructures (AAI) are either based on the accept-all-comers concept of OpenID without any formal trust or the rigid bilateral trust model of Security Assertion Markup Language (SAML). Different implementations, like Shibboleth and Identity Federation Framework of the Liberty Alliance, are based on SAML. While many national research and education networks (NRENs) operate large infrastructures for authentication and authorisation based on SAML, many federations in the industrial sectors consist of only very few members. NRENs' AAIs differentiate between organisations providing services for users, i. e., Service Providers (SPs), and home organisations, so called Identity Providers (IDPs). While geographic and industrial-sector-specific borders for federations are not imposed by Federated Identity Management (FIM) technology itself, they have become a reality due to the historic evolution and growth of FIM's use in both industry and higher education institutions. Most sectors and countries run their own federation. For instance, the DFN-AAI [1] interconnects universities and research institutes in Germany. Since research collaborations are not limited to national borders and researchers are professionally mobile, the problem of international and cross-sector collaboration is exacerbated. Neither a researcher from country A nor an employee of an industry partner from country B can access an ICT service operated by a university in country C based on existing national AAIs.

Different ad-hoc approaches exist to handle this problem. Either local user accounts are created for all project participants at each service, which obviously does not scale well for larger projects; or a new federation is set up specific for the given project or community. Either solution increases the overall complexity for IDP and SP operators and their manual working tasks. Also, this compromises user convenience and efficiency because of longer account set-up waiting times and the need to handle separate credentials for each service. Therefore, Inter-FIM is the next evolutionary step and, currently, a still young research discipline. Most conceptual, technical and organisational issues result from two main characteristics of today's federation solutions:

- An organisation's membership in a federation usually requires contracts, e. g., either with all other federation members in an ad-hoc federation or federations with a central operator, which can be either a large company in an hub-and-spoke federation or an independent entity as it can be seen in identity networks. The IDP must, for example, provide high quality user data to avoid SP misuse based on fake accounts, while the SPs must commit themselves to obey privacy and data protection principles.

- Federations must be built on common technical grounds, i. e., besides the same federation technology, e. g., SAML, the data format used by all IDPs and SPs must be harmonized, resulting in the so-called federation schema. This schema defines the syntax and semantics of information provided by the IDPs about their users. These attributes typically include name, email address and language preferences of the users.

ISBN: 978-1-61208-365-0

One big, world-wide federation is an utopia, because common technology, common membership criteria and one single user data format could not be achieved with thousands of organisations [2]. Instead, existing federations are often integrated into a higher-level umbrella inter-federation. eduGAIN [3] is a successful attempt to span the NRENs' country-specific AAIs across the pan-European research network GÉANT and beyond, including already more than 20 federations. eduGAIN provides the communication endpoints information, which are used to identify and technically trust an entity, i. e., SP or IDP. These so called metadata entries include X.509v3 certificates and other relevant information in Extensible Markup Language (XML) files. Aggregating the metadata of several federations with a Metadata Distribution Service (MDS) [4] results in a huge, in eduGAIN currently around 30.000 lines of code, inter-federation XML metadata file, which significantly slows down processing the metadata at each IDP and SP in practice. Either the slowed down processing must be compensated through new hardware investments or it leads to significantly reduced usability of the end users. Entities establish static bilateral trust relationships, while the Interoperable SAML Profile [5] addresses the exchange of SAML messages. As described above, putting federations under the umbrella of an inter-federation leads to inter-federation data schemas that are the common denominator of all involved federations. In turn SPs, which require certain user attributes not included in the inter-federation data schema, cannot be used with their full functionality. Furthermore, the additional contracts required between federations and their members make the overall inter-federation more complex and cumbersome to manage. With the growth of the inter-federation, the minimalistic data schema, the significant technical effort for each participating organization, and the additional contractual complexity limit the advantages of the concept.

Our new approach, named Géant-TrustBroker (GNTB), is developed as a part of the EC-funded Géant GN3plus research project and shifts from a static, manual model to a more dynamic, fully automated fashion based on SAML, which is used in the research and education communities and is easier to extend. The new, on-demand establishment of trust by dynamic exchange of metadata is more scalable than current approaches. GNTB therefore creates dynamic, virtual federations that overcome many organisational and technical issues of other Inter-FIM approaches. The prototype will be developed based on Shibboleth, the most common implementation of SAML. In Section II, we present the current state of the art and contrast it with the Géant-TrustBroker service described in Section III. Section IV then details GNTB's internally used data model, API calls, and technical details on the conversion rule repository. The paper is concluded by an outlook to how eduGAIN and GNTB will collude and a summary of the results achieved so far.

II. Related Work

As huge metadata files affect performance of the inter-federation, Dynamic SAML [6] simplifies the discovery of other entities. For initial trust establishment, the metadata consumer validates the signature using a root certificate and establishes the trust, though trust continues to lie in pre-established contractual arrangements. Despite the dynamic character, the entities have to manually convert the user information, which are exchanged, or use a data schema that is the common denominator.

The Metadata Query Protocol by Young, currently submitted as Internet Engineering Task Force (IETF) Draft [7], suggests how to retrieve metadata from entities using simple Hypertext Transfer Protocol (HTTP) GET requests. Therefore it solves the problem of huge aggregated metadata files, but otherwise has the same drawbacks as Dynamic SAML: manual work for attribute conversion, attribute filter, and the initial trust establishment. The Metadata Query Protocol is one piece of the Metadata Exchange Protocol (MDX), where entities pick a registrar for their metadata and receive attributes from partner entities from one or more aggregators. In analogy to the DNS protocol, the aggregators and registrars are linked in order to exchange metadata with each other. Similar to MDX, the Public Endpoint Entities Registry (PEER) project [8] implemented a public endpoint entities registry supporting both SAML and non-SAML protocols. Though PEER moves from a huge metadata aggregator to a central system, where administrators can register their domain, many manual steps are needed, for example, to generate an attribute filter adjusted to the IDP. The generic framework of Dynamic Identity Management and Discovery System (DIMDS) [9] has the purpose to achieve minor user involvement in the identity management by creating a new DIMDS account. All user attributes are stored unencrypted in a central system, which can affect the privacy of users. Furthermore, DIMDS does not distinguish between IDPs and SPs, though not all IDPs are SPs as well and vice versa. The same problem appears in Federated Attribute Management und Trust Negotiation (FAMTN) [10], where it is assumed that each SP in the federation can act as an IDP. Internal users of the FAMTN system are supposed to perform negotiations by exploiting their single sign-on (SSO) ID without repeating identity verifications, though the SSO ID can be misused for attacks. It might appear that a provider needs less or more attributes, leading to violations of data minimalization or further negotiations between providers. IdMRep [11] shifts from pre-configured cooperations to dynamic trust establishment by a distributed reputation-based mechanism based on local Dynamic Trust Lists (DTLs) [12] and external reputation data. DTLs can, e. g., receive recommendations from other entities, but this mechanism does not work for an entity, which is new in a federation or inter-federation. Because of the amount of data processing required for all external and internal trust information especially in inter-federations, this results in yet another bottleneck in practice. Furthermore, the problem of different attributes, syntax, and semantics is not considered. In contrast, the proposed solution of the Credential Conversion Service for eduGAIN (eCCS) [13] focuses on the conversion of credentials. eCCS makes use of a special credential conversion service, which translates source credentials into target credentials, based on attributes from the SChema for Academia (SCHAC) [14] and eduPerson [15] schemas, which are described in the DAMe project. Though conversion rules within the inter-federation eduGAIN are concurrently written manually, the proposal concentrates on the two schemas SCHAC and eduPerson. The solution is not scalable for more schemas and other attributes, which are needed within certain research communities, like Distributed European Infrastructure for Supercomputing Applications (DEISA) and Partnership for Advanced Computing in Europe (PRACE), and several other inter-organizational projects.

III. Géant-TrustBroker

Put simply, Géant-TrustBroker is an on-demand repository for SP and IDP metadata and conversion rules, which can be re-used by IDPs to fulfill attribute requirements for using a service. GNTB therefore simplifies the discovery of other entities and the establishment of technical trust, while it improves the scalability of metadata release. Furthermore, GNTB provides different means for the creation of dynamic virtual federations. GNTB is currently tailored for SAML, the widespread FIM standard used in R&E federations, but could be extended to support other FIM protocols as well. The GNTB core service enables the exchange of user information across federation borders with the following main characteristics:

- GNTB provides SP and IDP metadata on-demand. As opposed to distributing the complete aggregated metadata of all SPs and IDPs participating in an inter-federation, e. g., eduGAIN, GNTB supplies IDPs only with the metadata of SPs, which are used by at least one of their users and vice versa.
- GNTB automates the technical configuration steps to integrate new metadata when an IDP's user requests a service for the first time.
- Additionally, GNTB enables the re-use of data conversion rules. Instead of supporting only a small common subset of user attributes, the exchange of data conversion rules enables more complex and project-specific data schemas.

Especially the last two characteristics eliminate the previously manual workload for SP and IDP administrators and avoid long waiting times for the end users before they can use the service of a new SP. In general, two different workflow types have to be differentiated:

- The core workflow establishes the technical trust relationship between two entities, i. e., a SP and an IDP, triggered by the users themselves. The workflow is close to the regular SAML workflow in order to seemlessly integrate GNTB in current implementations and federations.
- Management workflows, which allow SPs and IDPs to register, update, and delete their metadata as well as conversion rules. To simplify the design of the core workflow, the metadata registration step is required before the GNTB core service can be used. However, metadata registration could also be integrated in the core workflow in the future.

To explain the GNTB core workflow in further detail, assume that user Alice from IDP I in federation $f1$ wants to make use of a web-based application service from SP S in federation $f2$ as depicted in Figure 1. The authentication form at S presents Alice, as often seen in a FIM scenario, a list of already trusted IDPs. As I and S have no bilateral relationship established yet, Alice cannot choose I from this list directly, but because S is registered at GNTB, Alice can trigger the GNTB core workflow. Using standard SAML mechanisms, Alice is redirected to the GNTB website automatically. From the list of already registered IDPs, Alice has to pick the one she wants to use. GNTB passes the information about the chosen IDP back to S to determine whether an user from IDP I is considered acceptable. If Alice inadvertently, e. g., because she missed it on the list, has chosen an IDP, which S already trusts, a regular FIM authentication workflow is instanced without any further involvement of GNTB. S then sends the initial SAML user authentication request to GNTB, which temporarily stores it. This intermediate step is necessary to authenticate Alice in order to prevent malicious users to add arbitrary IDPs' metadata to any SP and vice versa. GNTB then redirects Alice automatically to her chosen IDP I for authentication. During this step GNTB acts like an SP towards I. Assuming that S is acceptable and Alice has been authenticated successfully, I fetches the metadata for S from GNTB. Based on this kind of information, I can automatically update its metadata configuration, reducing the former manual workload. Because the providers S and I do not belong to the same federation, they usually use different schemas, which requires appropriate attribute conversion. I has to check whether suitable rules are available at GNTB. Based on such rules, I's local attribute resolver configuration has been updated automatically and enables the creation of appropriate attribute filters, i. e., definitions, which user attributes it will sent to S on request; this primarily ensures privacy protection. In the next step, Alice is redirected to GNTB and afterwards back to I to respond to the temporarily stored authentication request of S. Since Alice has already been authenticated, I can immediately send a SAML authentication assertion and Alice's browser is redirected back to S. Because SAML assertions usually have to be signed by the sending entity, S requires and fetches Is metadata from GNTB, which includes the public key(s) in order to verify the signature. For further authentication requests S stores Is metadata to its local configuration. In the last step, S requests a SAML attribute assertion that provides detailed, but filtered user information. After the technical trust establishment, GNTB is not involved anymore and therefore does not interfere with existing entity configuration using other add-ons. However, GNTB supports retrieving updated metadata automatically.

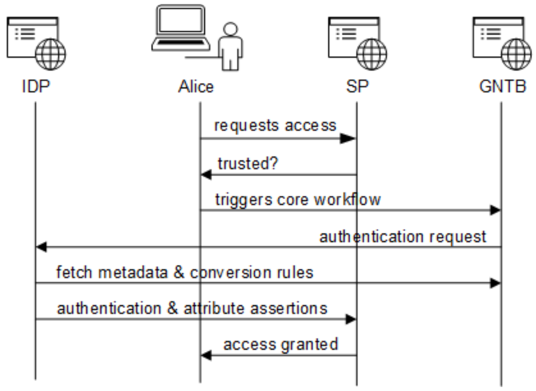

Figure 1. GNTB‘s core workflow.

IV. Brokered Technical Trust in Dynamic Federations

The Géant-TrustBroker service is the central part of our approach and important for establishing technical trust between

Copyright (c) IARIA, 2014. ISBN: 978-1-61208-365-0

two entities and reusing conversion rules. The data model includes a multi-federation namespace that is the basis for registering the list of user attributes required for using the service, while a data access layer facilitates the registration of entities, users, or uploading conversion rules.

A. Géant-TrustBrokers internal data model

As a central point of any Inter-FIM environment, metadata enables exchanging information about the communication endpoints and to ensure the authenticity of the sender. Therefore, this kind of information needs to be stored centrally at GNTB. A technical implementation imposes particular requirements on an interface for up- and downloading signed metadata files, the possibility to extract information from these files, and some kind of version control. We investigated other resource registry solutions for federations different approaches exist, e. g., the

- SwitchAAI Resource Registry tool, which makes use of a relational database management system;
- DFN-AAI, which stores the metadata files directly in the filesystem using PHP- and XSLT processing afterwards; and
- PEER project, which integrated a version control system.

Alternatively, a high-performance XML database, e. g., eXist would be an option. As GNTB should provide its service to different federations and communities, the metadata content varies, making the sole usage of a relational or XML database too complicated for reproducing metadata in a simple, efficient way. On the other hand, a version control system adds additional value to the service. Thus, we combine both approaches – a relational database and a versioning file system – because GNTB needs further information about an entity, e. g., to which organization a provider entity belongs to, in which repository container its metadata file is stored, or to record its current status. Additionally, to ensure that only authenticated and authorized administrators can manage their metadata or uploaded conversion rules, a simple GNTB user management is implemented. The database schema consists of the following information:

- Organizations: Each organization consists of one or more IDP or SP entities.
- Providers: Besides its unique name (entity_ID), entity type (i. e., IDP, SP) and its current status (e. g., valid, invalid, deactivated) information about the last attribute change and the location of the metadata file are stored.
- Users: Information about the authorized users, like username, hashed password, given name, surname, and email address of the contact person and their technical role.
- Conversion rules: Metadata about conversion rules, like description, its owner (e. g., the IDP, which uploads the rule), timestamp of the last change, status, and location of the rule file.
- Groups: Communities and federations, which can be the target or source group for conversion rules. Target means that the conversion rule can be re-used by one or several groups of IDPs or, respectively, one single IDP. Source is the opposite: the conversion rule was written for the needs of one specific SP or group of SPs, which all require identical attributes. One entity could be member of several groups, e. g., one federation, one inter-federation, and several projects.
- Relationships between a) IDPs and SPs, b) IDPs and conversion rules, c) rules and groups. The relationship between an IDP and an SP indicates a successful technical trust establishment using the GNTB core workflow described above and has to be stored at GNTBs database. This and analogous the information about the IDP and conversion rule relationship enable to notify administrators about metadata or rule changes. The last table contains information about a specific rule and by which target (single entity or group of entities) it is re-used. Thus we have to store only one copy of a conversion rule in the repository.

B. Géant-TrustBroker's data access layer

The database tables are filled up by different application programming interface (API) functions provided by GNTB data access layer (GNTB API). These functions can be split into three categories: account handling, provider entity handling, and conversion rule handling.

1) Account handling: As GNTB requires authentication of users as a precondition before any metadata or rule related configuration is possible, to prevent successful malicious intent of the user, some kind of user management is essential. For Géant-TrustBroker a basic access authentication (HTTP authentication) based on username and password, as often seen in FIM scenarios, is acceptable from a security perspective. But to avoid plain-text credentials in IDP- or SP-located scripts, a certificate based authentication method can also be used. User management provides the required functions to support the generally known lifecycle phases (e. g., creation, update, and deletion) of a GNTB account. API functions can be used to add, update, or delete the $username$, $password$ (i. e., its hash value) and the optionally stored $given\_Name$, $surname$ and $emailaddress$ entries of the entity administrator to the database.

2) Provider entity handling: At the first time contact between an entity and GNTB, metadata information is usually not yet registered, except if it has been automatically taken over from a federation or inter-federation, e. g., by a central Metadata Distribution Service, as it could be an option in the inter-federation eduGAIN. The registration procedure is possible either Uniform Resource Locator (URL) or file-based. In the first case, an entity is registered by providing a metadataURL to fetch a metadata XML file from there; otherwise, an entity provider uploads this file manually. The uploaded metadata is validated by specific XML Schema Definition (XSD) files, which validates the structure of the XML file. The ownership can be confirmed by HTTP validation, i. e., creating a resource in the root of the HTTP service for the domain with the name of a random parameter string given by GNTB, certificate validation of the uploaded metadata or by simply verifying educational domain names by email. As described

ISBN: 978-1-61208-365-0

in the core workflow above, a SP typically checks its trust relationship to the IDP chosen by the user. The API provides an appropriate *gntb_Ent_CheckTrustToIdp(Entity_ID[SP], Entity_ID[IDP])* function for this purpose. If an IDP is considered acceptable, the core workflow continues to establish the technical trust by invoking the API function *gntb_Ent_EstabTrust(Entity_ID[SP, Entity_ID[IDP])*. The administrators can set up further options, like notification of changed metadata and certificate expiration, update its metadata and delete technical trust relationships.

3) Conversion rule handling: Service providers may expect attributes, which may not be part of the IDP's schema, i. e., the IDP cannot provide these attributes out of the box. In order to send them, IDP administrators utilize so called user attribute data conversion rules, which will be used to extend the local attribute-resolver.xml definition. In the first step, raw attributes are pulled by a DataConnector from an IDP-internal data store, e. g., LDAP server or user management database, and then prepared for release in an attribute definition consisting of the definition of the attribute itself and the so called conversion rules. Typical attribute conversions encompass

- renaming: the attribute is used with the same format, but another name. A simple example of renaming a source attribute *gecos* to a new *displayName* attribute would look like this:

```
<resolver:AttributeDefinition id="displayName"
  xsi:type="Simple" xmlns="urn:mace:[...]"
  sourceAttributeID="gecos">

 <resolver:AttributeEncoder [...]
   name="urn:mace:dir::displayName" />

 <resolver:AttributeEncoder [...]
  name="urn:oid:2.16.840.1.113730.3.1.241"
  friendlyName="displayName" />

</resolver:AttributeDefinition>
```

- transforming: this is typically used for timestamps or dates, if the internally format is different from that of the SP;
- splitting: regular expression can be used to extract partial information from an attribute;
- merging: inter-connects two source attributes, e. g., givenName and surname, into a new one, e. g., commonName.

These conversion functions can be cascaded, i. e., one rule to prepare the attribute for internal use, then another one referencing the internal rule for the federational or communities schema, which can afterwards have a dependency to another schema. Administrators can re-use those conversion rules by utilizing the GNTB conversion rule repository. These XML files can be uploaded and should be searchable as well as re-usable by other IDPs. The data access layer provides the function *gntb_Conv_FetchRule(Name)* to download an appropriate conversion rule. The definitions within the rule are added to the local configuration (metadata-resolver.xml) by scripts. Due to the fact that XML include tags would not work according to [16], as XInclude requires schema support in the original schema to mark where things can be included, and we want to reduce the manual work for administrators, local assembling of configuration files is reasonable. We define source groups, which is one SP or a group of SPs needing specific attributes. The target group is one IDP or a group of IDPs, that can use this conversion rule. As mentioned above, conversion rules can be applied to different sources and targets, if a rule is applicable for different groups, i. e., federations, communities or project partners as well. For example, one conversion rule named 01203_2.xml was written from an IDP I belonging to the federation $DFN - AAI$, which is an example for a target group. If the source of this rule was SP B in the federation $SWITCH - AAI$, an IDP C in the Austrian federation $ACOnet$, noticing that the rule 01203_2.xml can be used for their federation as well, can fetch the rule, updated its configuration and therefore this Austrian IDP C applies rule 01203_2.xml for the Austrian federation.

V. Conclusion and Future Work

Géant-TrustBroker enables the on-demand, user-triggered exchange of metadata and user attribute data conversion rules across identity federations' borders. Concurrently the scalability of the metadata exchange in federations and inter-federations is improved. GNTB supports the fully automated technical setup of FIM-based AuthNZ data exchange and therefore increases the automation of the former manual implementation efforts required by administrators of SPs and IDPs. Consequently, users can immediately start using a new service outside of their federation and have no waiting time until the administrators have finished the manual setup process.

The Géant-TrustBroker core workflow, which is based on the IDP Discovery Protocol and Profile [17], will be formally specified as an IETF Internet-Draft and submitted for standardisation as IETF Request for Comments (RFC). The GNTB prototype and implementation of the workflows for the FIM software package Shibboleth will be made availabe as open source and used for pilot operations in 2016.

Further research questions relate to the combination of technical and behavioural trust for the establishment of dynamic virtual federations as well as to quality assurance, i. e., measure for Level of Assurance (LoA) guarantees, of entities in the dynamic virtual federations, which will be focused in 2015 during GN4 phase 1.

Acknowledgment

The research leading to these results has received funding from the European Communitys Seventh Framework Programme under grant agreement no 605243 (Multi-gigabit European Research and Education Network and Associated Services - GÉANT).

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-Universitt München, Technische Universitt München, the University of the Federal Armed Forces, and the Leibniz Supercomputing Centre of the Bavarian Academy of Sciences and Humanities.

References

[1] "DFN-AAI – Authentication and authorization infrastructure," 2014, URL: https://www.aai.dfn.de/en/ [accessed: 2014-03-04].

[2] "Interfederation and Metadata Exchange: Concepts and Methods," 2009, URL: http://iay.org.uk/blog/2009/05/concepts-v1.10.pdf [accessed: 2014-03-04].

[3] "Géant: eduGAIN Homepage," 2014, URL: http://www.geant.net/service/eduGAIN/Pages/home.aspx [accessed: 2014-03-04].

[4] "mds.edugain.org," 2014, URL: http://mds.edugain.org/ [accessed: 2014-03-04].

[5] "Interoperable SAML 2.0 Web Browser SSO Deployment Profile," 2009, URL: http://saml2int.org/profile/current [accessed: 2014-03-05].

[6] P. Harding, L. Johansson, and N. Klingenstein, Dynamic Security Assertion Markup Language. IEEE, 2008.

[7] "Metadata Query Protocol - draft-young-md-query-01," 2013, URL: http://datatracker.ietf.org/doc/draft-young-md-query/?include_text=1 [accessed: 2014-03-05].

[8] "PEER 0.11.0: Python Package Index," 2013, URL: https://pypi.python.org/pypi/peer/0.11.0 [accessed: 2014-03-05].

[9] K. Lampropoulos and S. Denazis, "DIMDS: A Dynamic Identity Management and Discovery System," in Proceedings of the INFOCOMP Workshop 2009, IEEE, Rio de Janeiro, Brasil. IEEE, 2009, pp. 1–2, ISBN: 978-1-4244-3968-3.

[10] A. Bhargav-Spantzel, A. C. Squicciarini, and E. Bertino, "Trust Negotiation in Identity Management," IEEE Security and Privacy, vol. 5, no. 2, Mar. 2007, pp. 55–63. [Online]. Available: http://dx.doi.org/10.1109/MSP.2007.46

[11] P. AriasCabarcos, F. Almenárez, F. GómezMármol, and A. Marín, "To Federate or Not To Federate: A Reputation-Based Mechanism to Dynamize Cooperation in Identity Management," Wireless Personal Communications, 2013, pp. 1–18. [Online]. Available: http://dx.doi.org/10.1007/s11277-013-1338-y

[12] F. Almenárez, P. Arias, A. Marín, and D. Díaz, "Towards Dynamic Trust Establishment for Identity Federation," in Proceedings of the 2009 Euro American Conference on Telematics and Information Systems: New Opportunities to Increase Digital Citizenship, ser. EATIS '09. ACM, 2009, pp. 25:1–25:4. [Online]. Available: http://doi.acm.org/10.1145/1551722.1551747

[13] G. López, O. Cánovas, D. Lopez, and A. Gómez-Skarmeta, "Extending the Common Services of eduGAIN with a Credential Conversion Service," in Computer Security – ESORICS 2007, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2007, vol. 4734, pp. 501–514. [Online]. Available: http://dx.doi.org/10.1007/978-3-540-74835-9_33

[14] "Download SCHAC Releases," 2011, URL: http://www.terena.org/activities/tf-emc2/schacreleases.html [accessed: 2014-03-05].

[15] "LDIFs - MACE-Dir: eduPerson/eduOrg LDIFs," 2012, URL: https://spaces.internet2.edu/display/macedir/LDIFs [accessed: 2014-03-05].

[16] "Shibboleth – Users – include files for xml config," 2011, URL: http://shibboleth.1660669.n2.nabble.com/include-files-for-xml-config-td6206245.html [accessed: 2014-03-13].

[17] "Identity Provider Discovery Service Protocol and Profile - Committee Specification 01," 2008, URL: http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-idp-discovery.pdf [accessed: 2014-05-08].

ISBN: 978-1-61208-365-0