Project Géant TrustBroker – dynamic identity management across federation borders

Authors: Daniela Pöhn, Stefan Metzger, Wolfgang Hommel

Author affiliations:
Leibniz Supercomputing Centre, Bavarian Academy of Sciences and Humanities
Boltzmannstraße 1, D-85748 Garching n. Munich, Germany
{poehn,metzger,hommel}@lrz.de, +49 (89) 35831-8763

Keywords: Federated Identity Management, Inter-Federation, Shibboleth, SAML, IETF, service provisioning

Abstract:
A growing number of the security assertion markup language (SAML) based national National Research and Education Network (NREN) operated authentication and authorization infrastructures (AAIs) already joined the inter-federation eduGAIN [1]. Other NRENs, e.g., in Australia, Japan, and Estonia [2], are eager to opt-in.
Generally, to participate in an inter-federation, a common technological basis must be established, including:

- **Metadata**: Identity Providers (IDP) and Service Providers (SP) have to know each other's communication endpoints. Therefore all needed information like URLs and server certificates are exchanged. This is done via signed, aggregated metadata within the involved federations, but also via a Metadata Service (MDS) for all the metadata used in an inter-federation.
- **Schema**: IDPs and SPs need a common syntax and semantics of the exchanged user information ("attributes"). On the level of the federation as well as of the inter-federation, a common set of attributes, called a schema, must be established for this purpose.

In consequence, the following drawbacks emerge from the increasing complexity of such full-mesh inter-federations, as shown in Figure 1:

- Aggregated XML-based metadata becomes cumbersome to process and slows down the servers.
- eduGAIN only standardizes the least common denominator regarding attributes, which practically means that certain information about users required by SPs may not be available.
- The setup workflows require manual administrators' work to configure and filter the attribute release as well as to set up inter-federation schema attribute conversion rules.
- Manual work is also required at each SP that is used by at least one user from another federation.
- Users cannot use new SPs before these manual setup tasks have been finished and often loose interest in services due to waiting times and the lack of user-friendliness.

In practice, research communities like CLARIN [3] and DARIAH [4] prefer to found their own federations and run dedicated IDPs in order to provide all the needed user attributes. Therefore, users typically have to manage several identities for their work, which is a contradiction to the single sign-on goal and benefits of Federated Identity Management (FIM). In addition, users from external AAIs, e.g., research project partners from various industry branches, will not be able to get access to an inter-federation service, since the external AAI is not part of the aggregated metadata.

To solve these problems, a complementary approach to eduGAIN has been initiated within Géant as a part of the GN3plus Open Call projects in order to facilitate inter-federation not only based on a minimum schema. Its goal of enabling quick integration of services from other federations by maximizing the degree of automation will support researchers' access to external services and increases their efficiency. Furthermore, functionality to choose between different, also privately used accounts, similar to OpenID's AccountChooser [5], will be integrated to provide users convenience. A proof of concept and pilot projects will be set up in the Géant community.

The project, **Géant-TrustBroker (GNTB)**, will specify the services and protocols required for the solution approach shown in Figure 2: A new inter-federation service, also called Géant-TrustBroker (GNTB), automates *on-demand* metadata exchange between SPs and IDPs across federation borders. GNTB will allow users (not only site administrators) to initiate the first-time contact between service providers (SPs) and the users' identity providers (IDPs) in order to perform the required preparations for identity data exchange based on the technical aspects of "trust". Usually users will trigger the SP metadata registration or its update at GNTB. Afterwards, IDPs are triggered to fetch this SP metadata to auto-generate their

configuration, including the setup of attribute filters and attribute conversions. Through a smart user attribute data conversion rule repository, these rules can be re-used by other IDPs within each federation. In addition, IDPs will be able to retrieve attributes from external sources, i.e., they can perform a recursive Attribute Authority (AA) lookup.

The currently existing SAML-based workflows and protocols will be extended to automate most of the previously manual configuration steps. GNTB can seamlessly be integrated into widely deployed identity federation software packages, such as Shibboleth or simpleSAMLphp. The protocols for accessing GNTB will be submitted for discussion and standardization to the IETF as an important part of the project. A prototype will be implemented based on a Shibboleth testbed.

The key highlights of the Géant-TrustBroker will be as follows:

- Automates the tedious manual tasks of inter-federation SP-IDP communication setup
- No more waiting times for users before being able to access an federation-external service
- IETF RFC submission of the GNTB protocol
- Prototype implementation for Shibboleth
- Scalability of the on-demand approach compared to full inter-federation metadata aggregation

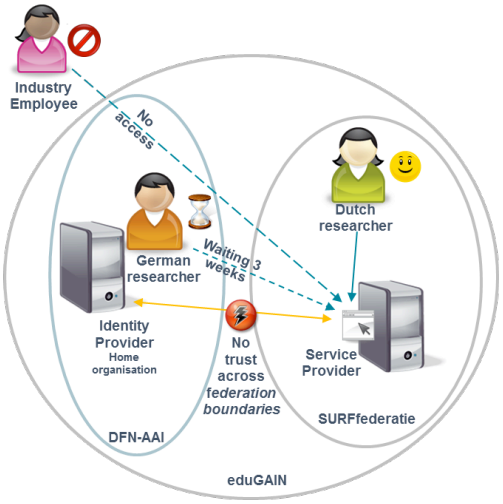

Figure 1: Current situation in inter-federations

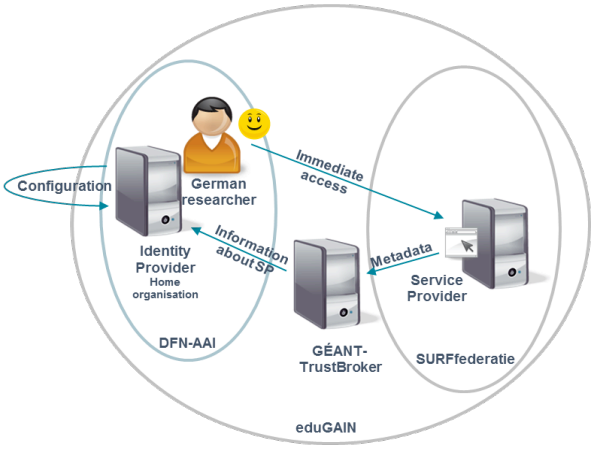

Figure 2: Proposed Approach with GNTB

Full paper: The authors would like to submit a full paper to TNC 2014.

By April, 2014 (full paper submission deadline), the Géant-TrustBroker requirements will have been fully analyzed and will be summarized. We plan to describe the workflows and functionalities of the Géant-TrustBroker and the AccountChooser functionality in more detail from the points of view of a user, an SP and an IDP, and with typical variations, e.g., regarding trust relationships and ways to release attributes. The GNTB protocol specifications, the trust building service, and the smart data conversion rule repository service, based on the defined requirements, will already be specified at an early stage and also outlined. At the conference in May, 2014, we will be able to present the first part of the document intended for IETF submission and hope to get feedback from interested communities and IDP/SP operators.

Acknowledgement: The research leading to these results has received funding from the European Community's Seventh Framework Programme under grant agreement nº 605243 (GN3plus).

References:

[1] Géant: eduGAIN. http://www.geant.net/service/edugain/pages/home.aspx [Online: 11-29-2013]
[2] Géant: eduGAIN technical site. http://www.edugain.org/technical/status.php [Online: 11-29-2013]
[3] CLARIN: CLARIN ERIC. http://www.clarin.eu/ [Online: 11-29-2013]
[4] DARIAH: DARIAH-EU. http://www.dariah.eu/ [Online: 11-29-2013]
[5] OpenID Foundation: Account Chooser. http://accountchooser.net/ [Online: 11-29-2013]

Vitae:

- Daniela PÖHN received a university diploma 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. She is involved in the identity management research activity (JRA3 T1+T2) in Géant3+ since April, 2013.
- Stefan METZGER received a university diploma degree in Computer Science from Technical University Munich. Before he joined LRZ in July 2009 he oversaw diverse risk and compliance management projects as a security consultant. Holding a CISSP certification, his focus as a Ph.D. candidate is on information security as well as identity management in inter-organizational environments.
- Wolfgang HOMMEL is a research group leader at Leibniz Supercomputing Centre. He has a Ph.D. as well as postdoctoral lecture qualification from Ludwig-Maximilians-University, Munich, where he teaches information security lectures and labs. His research focuses on information security, IT service, and network management in complex large-scale and inter-organizational scenarios.