12-03-2015

Open Call Deliverable GÉANT-TrustBroker: Overview of Design and Architecture

Deliverable

Actual Date:	12-03-2015
Grant Agreement No.:	605243
Work Package/Activity:	JRA0
Nature of Deliverable:	R (Report)
Lead Partner:	BADW-LRZ
Document Code:	<Enter the GN3plusYY-nnn-nnn ref for the PDF>
Authors:	Daniela PÖHN

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7 2007–2013) under Grant Agreement No. 605243 (GN3plus).

Abstract

This document gives an overview of the OpenCall Project GÉANT-TrustBroker. It explains the developed service, the design decisions made and the architecture of the GÉANT-TrustBroker service in a short form.

Document Revision History

Version	Date	Description of change	Person
1	12-03-15	First draft issued	D. Pöhn

Table of Contents

Table of Figures

Executive Summary

The GÉANT-TrustBroker OpenCall project enables the fully automated, user-triggered, on-demand establishment of technical trust between service providers (SPs) and identity providers (IDPs) through dynamic automated Security Assertion Markup Language (SAML) metadata exchange (DAME). It includes basic AccountChooser (Where Are You From/WAYF) functionality for users and minimizes the system-administrative workload for IDP administrators by enabling the sharing and re-use of user attribute conversion rules. GÉANT-TrustBroker is intended for scenarios in which the a-priori - e.g. federation- or eduGAIN-based - exchange of SAML metadata is neither practical nor scalable. GÉANT-TrustBroker is not intended for scenarios where a-priori exchange of metadata is mandatory for non-technical aspects, such as contract-based trust building between IDP and SP.

This document is primarily intended to give an overview of the OpenCall project. It therefore describes shortly the GÉANT-TrustBroker, i.e.

- the idea of the project,
- the design of the GNTB service,
- the demonstrator with its setup,
- the design of the protocol DAME used for triggering the metadata exchange, and
- the current status of the Internet-Draft of the protocol.

This deliverable also links to deliverables and milestone documents, which were written during GN3plus.

1 Introduction

The aim of project GÉANT-TrustBroker (GNTB) is the specification of a new service for large-scale authentication and authorization infrastructures, i.e. federations and inter-federations. GNTB allows users to initiate first-time contact between SPs and IDPs to perform required preparations for identity data exchange in a fully automated manner.

Federated access management (FIM) allows users to seamlessly use digital identity information of their home institutions to authenticate against a service provider, but this cannot be used with SPs that are not members of the federation (or inter-federation), as the user's IDP does not know and trust these SPs. Additionally, IDPs needs to know which user attributes are required at the SP's site. To protect user's privacy, IDPs use so called Attribute filters to send only the minimum amount of data. Unfortunately, setting up the technical trust and the IDP-side configuration is usually a manual task. Therefore, GNTB was established. One possible use case is described in the next section.

This deliverable gives an overview of the project GNTB, delivered in GN3plus as an OpenCall project.

- It describes the service itself,
  - the basic design as well as
  - the demonstrator,

  implemented during the project phase.
- The GNTB service uses the DAME protocol to trigger the metadata exchange. The basic design and the current status of the Internet-Draft (I-D) are explained.

GÉANT-TrustBroker was implemented by the GNTB team (Figure 1-1) at the Leibniz Supercomputing Centre (BADW-LRZ).

Figure 1-1: GNTB team at the Leibniz Supercomputing Centre

1.1 Use Case

One possible use case is described in this section and was shown on the demonstrator at the GN3plus Symposium in Athens.

Three organizations - Blue University, Yellow University, and Grey Services - want to cooperate for a fictitious research project “COLORado”. Both universities provide an IDP service (IDP1 at Blue University, IDP2 at Yellow University) and organisation Grey Services runs an SP (SP1). The service provided is a simple project collaboration tool, which allows the usual sharing of project-related files, Wiki web pages, and group calendar. Besides these functions, the collaboration tool provides an integrated online Skype status check plugin, showing all project members along with their Skype-id and current availability status.

We assume that IDP1, IDP2, and SP1 are NOT members of a common federation or inter-federation, so initially they do not have each other’s SAML metadata. For some reasons, they do not want to (or cannot) join a federation that belongs to an inter-federation infrastructure (i.e. eduGAIN). We also assume that both IDPs can provide user information based on the SCHAC attribute schema, but the SP uses a different, proprietary data schema. In order to access the otherwise not directly connected SP of organization Grey Services, the research project wants to use GÉANT-TrustBroker. As a prerequisite, both IDPs and the SP are already registered at GNTB and have the required Shibboleth modifications installed. The extensions to the Shibboleth software for IDP and SP are used to communicate with a central GNTB service.

User Marina from Blue University requests access to the SP of Grey Services. For logging in, Marina chooses “Federated Login”. Because the SP does not know (trusts) her IdP1, its Embedded Discovery Service (EDS) does not allow the selection of IDP1 directly. Because the SP and IdP1 are set up for GÉANT-TrustBroker, the SP’s EDS is configured to allow forwarding the discovery request to the GÉANT-TrustBroker. Marina chooses this option and is presented with a list of all IDPs currently available at the GÉANT-TrustBroker. After selecting her home IDP1 at the GNTB discovery service and subsequently authenticating and authorizing there, Marina will be redirected to the SP. In the background the metadata of her IDP1 and the SP are exchanged and integrated into the local software. After providing user consent using uApprove, Marina will be successfully logged-in to the collaboration tool.

However, the integrated skype-plugin does not yet contain Marina’s Skype-ID, because the “`skypeID`” attribute could not be created and thus was not transferred. Marina informs her IDP1 administrator that she wants to use the Skype plugin in the collaboration tool. Checking the SP’s metadata, the IdP1 administrator Azuro logs onto the GNTB administration web interface (GNTB-Web) and adds a new conversion rule that derives the “`skypeID`” attribute from “`schacUserPresenceID`”, which he knows is available at his IDP1. With the conversion rule in place, Marina accesses the SP again (a fresh login is required ensure attribute transmission). uApprove pops up and also shows the newly created “`skypeID`”, because the attribute conversion rule added by Azuro in the previous step was installed automatically. Marina confirms the attribute transfer and will be redirected to the secured collaboration tool website. Now the Skype plugin works as expected. The conversion rule can be re-used by IDP2 needing the same attribute conversion rule, when Sunny from Yellow University tries to access the SP.

2 GÉANT-TrustBroker service

This chapter describes the GÉANT-TrustBroker service, which is divided into

- the core service of the trusted third party (TTP),
- the extension of the IDP software,
- the extension of the SP software,
- and an extended Embedded Discovery Service.

The core service is an extension of the Centralized Discovery Service, which is currently used to determine the user's IDP. The central GNTB service extends the Centralized Discovery Service of Shibboleth, in order to facilitate the user-triggered, on-demand exchange of metadata. The extension contains a metadata registry, the logic needed to handle the setup up of the technical trust and the exchange of attribute conversion rules. This functionality is needed for the process of establishing technical trust between Identity Provider and Service Provider via the trusted third party service also referred to as GÉANT-TrustBroker, and to enable user information exchange across traditional identity federations' borders.

Since the EDS is not run by the federation, it includes only the metadata of those IDPs, which are trusted by the SP, via the so called Discovery Feed, and transforms the metadata of the IDPs into a list. The EDS was extended, in order to be able to configure it for the usage with GNTB. If the SP does not know the IDP, the user can trigger the GNTB workflow as EDS can forward the discovery request to the extended Centralized Discovery Service.

The extensions of the IDP and SP software integrate the metadata (and for IDPs the attribute conversion rules) automatically and communicate with the central GNTB service. This results in the automation of previously manual configuration steps.

While the design was done in regard of SAML and its protocols, the demonstrator is based on the often used implementation Shibboleth. Both parts, i.e., the design of the GNTB and the implementation are shortly described in this chapter.

2.1 Getting the source code

All software components of GÉANT-TrustBroker can be downloaded from the subversion (SVN) repository http://svn.geant.net/GEANT/TrustBroker.

It contains the commented source code, archived releases, and detailed installation instructions. The repository is structured as follows (all folders with the exception of the releases folder contain their own SVN directories branches, tags, and trunk):

- **releases:** contains packaged release versions of the extensions that should be used when installing an extension
- **shib-eds-modification:** contains the source code of the modified Shibboleth Embedded Discovery Service
- **shib-idp-dame-extension:** contains the source code of the IDP extension
- **shib-sp-dame-extension:** contains the source code of the SP extension
- **shib-ttp-dame-cds-extension:** contains the source code of the Shibboleth Centralized Discovery Service extension
- **shib-ttp-db-dame-module:** contains the source code for a database module that is used by the IDP and the GNTB extension

2.2 Design of the GNTB service

The design of the GNTB service, i.e.,

- different workflows and
- specification of the core GNTB service,

is described in details in the milestone document M.1.1.1 and the deliverable D.1.1.1.

2.2.1 Workflows

The workflows were designed in milestone document M.1.1.1 [M.1.1.1]. They can be divided into management workflows and core workflows.

The management workflows are established to manage metadata and conversion rules independently from the metadata exchange, which is the technical trust establishment, and can be stated as:

- Management workflow of SP's metadata
- Management workflows of IDPs

- Management workflow of IDP metadata
- Management workflow of conversion rules of IDPs
- Management workflow of SP metadata information for IDPs

The core workflow describes the metadata exchange in different variants:

- Default trust establishment workflow
- Using TrustBroker, if IDP and SP are in the same federation
- Using TrustBroker, if IDPs have to lookup Attribute Authorities (AA)
- Using TrustBroker, if SAML Entity Categories are used
- Using TrustBroker, if attributes are part of SP's metadata information
- Code of Conduct implications using TrustBroker

Furthermore, special cases with options for configurations were stated. The default core workflow is displayed in Figure 2-1 and can be described as:

- The user wants to make use of a service. As his IDP is not known by the SP, the Discovery Service of GNTB is used. The user selects his IDP at the GNTB Discovery Service and triggers the core workflow.
- GNTB informs the SP, which then sends an authentication request. GNTB caches this request, before it sends another authentication request to the user's IDP.
- After the user has been successfully authenticated, the IDP sends the authentication response to the GNTB service.
- GNTB then triggers the IDP to download the SP's metadata. After the successful configuration of the IDP, the SP downloads the IDP's metadata and integrates it into the local configuration.
- GNTB sends the previously cached authentication request to the IDP.
- As the user is already logged in, the IDP sends the assertion with the user information to the SP. If the IDP does not have appropriate conversion rules to convert the user information into the SP's format, it can download conversion rules from the GNTB service.
- The SP then grants the user access to the service.

These core workflows were then used for the protocol, described in Chapter 3.

The requirements on core GNTB service, IDP extension, and SP extension were summarized in milestone document M.1.1.1.

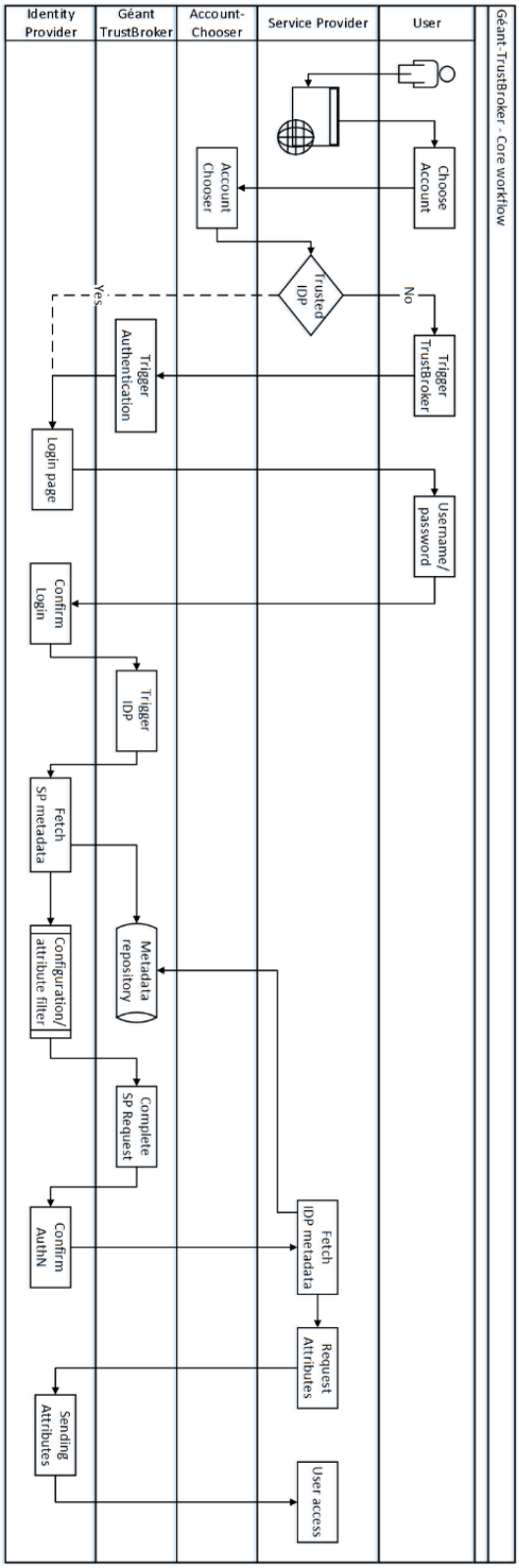

Figure 2-1: GNTB Core Workflow as designed in M.1.1.1

2.2.2 Specification of GNTB

The data model was specified in deliverable D.2.1.1 [D.2.1.1], based on the management and core workflows. The relational database stores, as shown in Figure 2-2, information for the metadata management and conversion rule management. The metadata itself and the conversion rules are saved in a file-based repository as it is difficult to reproduce the extensible Markup Language (XML) content, which can vary, in a relational database. As the XML content is re-used in an untransformed way, a simple storage is more efficient.

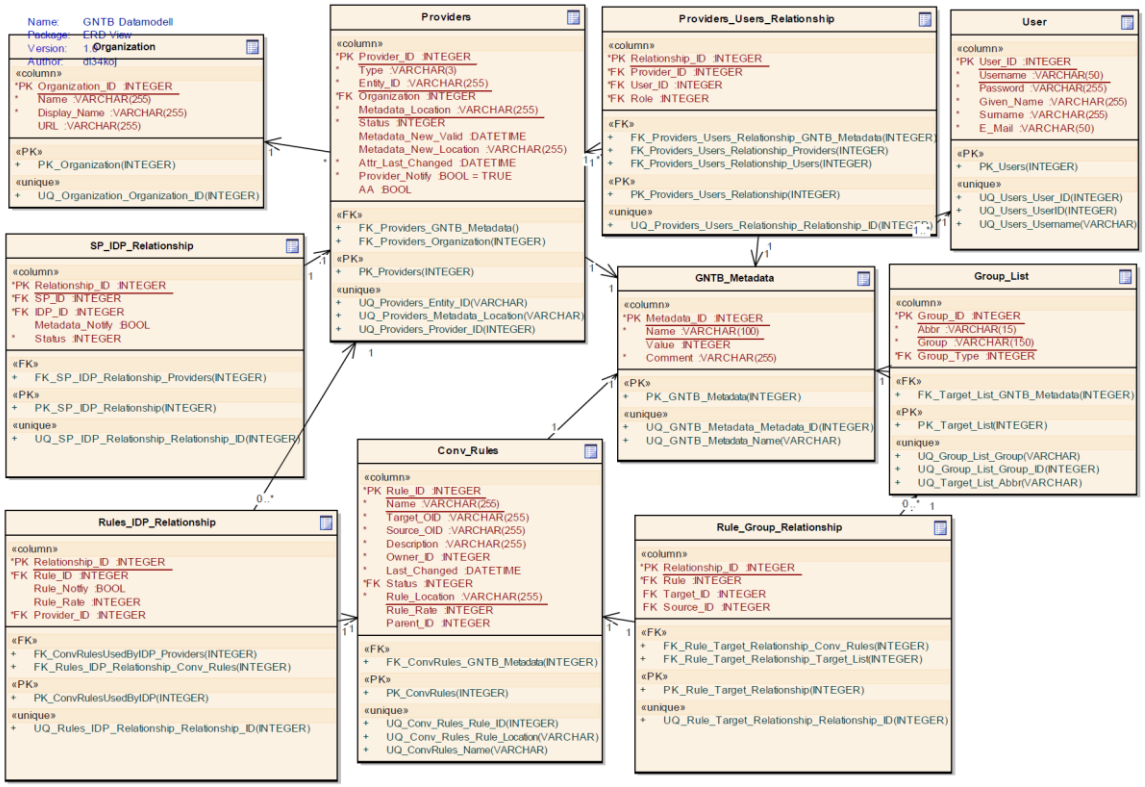

Figure 2-2: Database as designed in D.2.1.1

Also an Application Programming Interface (API) was designed for Account Handling, Entity Handling, and Conversion Rule Handling as described in deliverable D.1.1.1.

Procedures and functions were developed for clean-up and schema validation.

2.3 Demonstrator

Based on the design of the GNTB service, the demonstrator was implemented. The implementation is described in the milestone document M.4.1.1 and the deliverable D.4.1.1 and consists of the following parts:

- The core GNTB service, extending the Shibboleth Centralized Discovery Service
- Extension of the Shibboleth IDP Software
- Extension of the Shibboleth SP Software
- Extension of the Shibboleth EDS

In this section, first the setup of the demonstrator is described, before the implementation of the core GNTB service, divided into web-frontend and backend, is described in short. Last but not least, the extensions for IDP and SP are mentioned.

2.3.1 Setup

The successful implementation of GNTB was shown in the following setup, described as use case in 1.1, at the GN3plus Symposium 2015 in Athens and in the deliverable D.4.1.1 [D.4.1.1]:

- The TTP GNTB implements the DAME-based SAML metadata exchange, described in Chapter 3, and facilitates the sharing and re-use of user attribute conversion rules.
- Two IDPs: Blue University and Yellow University have never cooperated before, but are partners in the COLORado project now. They are not members of a common federation
- One SP: Grey Services provides a collaboration platform both universities would like to use to manage their project; it has never cooperated with either IDP before and does not share any federation membership with the IDPs.

The setup is visualized in **Fehler! Verweisquelle konnte nicht gefunden werden.**:

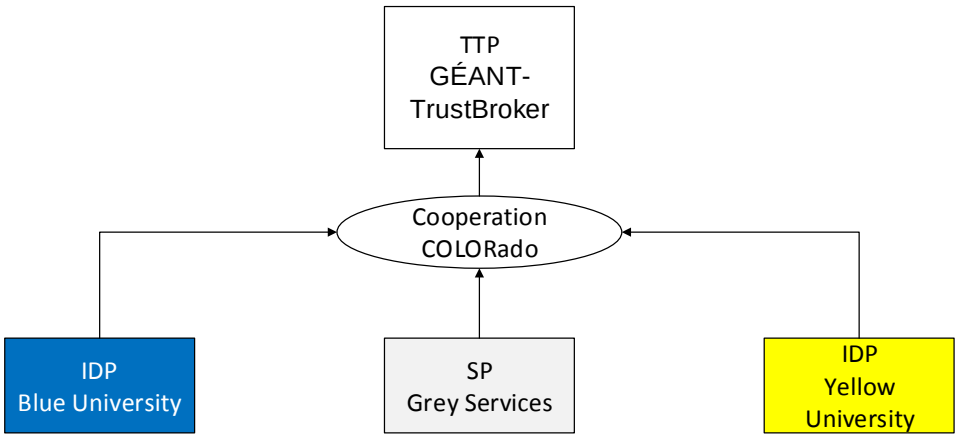

Figure 2-3: GNTB setup of the demonstrator as described in D.4.1.1

2.3.2 Central GNTB Service

The demonstrator for the central GNTB consists of the following parts, described in details in milestone document M.4.1.1 [M4.1.1.]:

- Backend, which is a web service running on the web server Tomcat and stores relevant information in a database and a file-based repository.
- Web frontend as a user interface, which has all relevant functionalities.
- Scripts for testing the web services and providing workflow automation in the future.

While the scripts for testing can be found in M.4.1.1, a short description of the GNTB web-frontend and the GNTB backend follows.

2.3.2.1 *GNTB Web-Frontend*

The web interface can be accessed at:

http://gntb08.srv.lrz.de:8080/discovery/ttp/index.jsp

The demonstrator's web frontend is implemented by

- Tomcat Servlets,
- Java Server Pages (JSP),
- the bootstrap framework,
- and Cascading Stylesheets (CSS).

The underlying functionality is partly implemented as servlets, which run on the web server. Based on the URL pattern, derived from the API, the relevant servlet is chosen, as displayed in Figure 2-4:

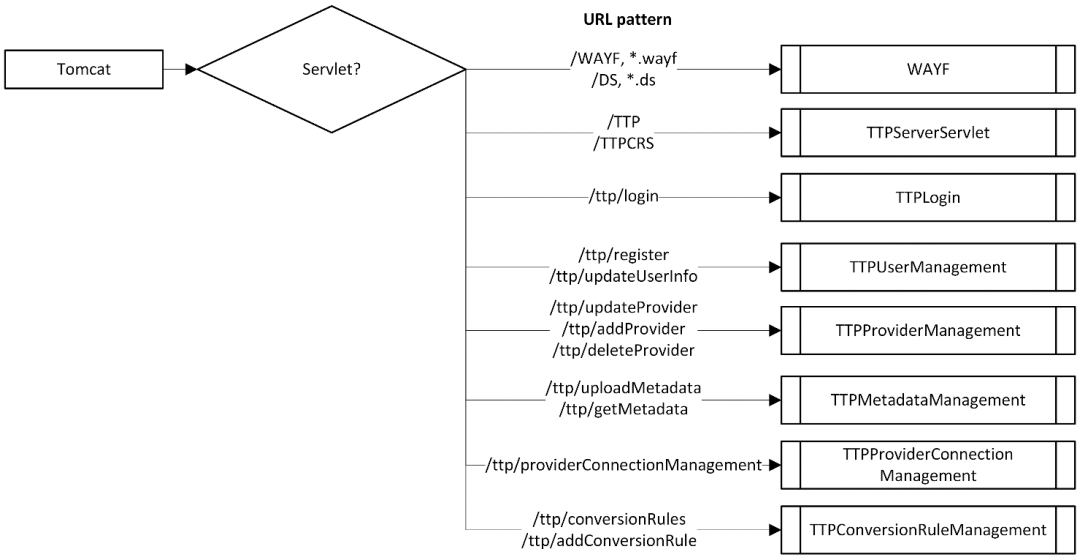

Figure 2-4: URL patterns for servlets

2.3.2.2 *GNTB Backend*

The backend consists of a file-based repository for conversion rules and metadata as well as of a MySQL database.

The XML-based metadata information of a provider entity and the XSLT-based conversion rule definitions are stored directly as files in the file system of the TTP in the following two directories:

- `ttpMetadataStorageDirectory`
- `ttpConversionRuleStorageDirectory`

The exact path in the file system is defined as parameter in the `web.xml` file. The location of an entity's information will be referenced by the location parameters in the `GNTB_Metadata` and the `Conv_Rules` tables in the database.

Differing from the data model specified in deliverable document D.2.1.1, we added or adapted some tables in the GNTB core service database in order to improve the GNTB quality:

- `User`: the columns *salt* and *validated* are added. The *salt* increases the difficulty to discover the user's password. The *validated* parameter denotes, if the user account has been activated by a GNTB administrator.
- `Organization`: a column *description* has been added.
- `Providers`: information about the provider's metadata are now stored in the table `GNTB_Metadata`
- `ProviderWhitelist` and `ProviderBlacklist`: whitelists and blacklists for IDPs and SPs allows explicitly to block or allow the automatic metadata exchange between specific providers. These tables have references to the `provider` table (not shown in the figure above).
- `GNTB_Metadata`: some meta-information about the entity's metadata. This table stores the *entityID*, the *location* of the metadata file in the file system-based repository. The parent entry allows referencing

another metadata information from which the metadata are derived. This allows to store more than one metadata information of an entity, e.g. in the case of renewing a contained certificate.

- `Attributes`: Table to store information (*name*, *nameFormat,* and *friendlyName*) of an attribute
- `Conv_Rules`: Table to store information about the attribute conversion rules. The columns, *source_OID* and *Rule_Rate*, specified in D.2.1.1 are moved to new tables (`RuleDependencies`, `RuleScores`)
- `RuleDependencies`: Stores the source attributes (reference to the `attributes` table) required by a conversion rule to build the specified target attribute.
- `RuleScores`: Stores user-specific rating information about the quality of a conversion rule. References the tables `User` and `Conv_Rules`.
- `AttributeReleasePolicy`: overview of all attribute release policies between an IDP and SP pair. IDPs can select attributes they do not want to release

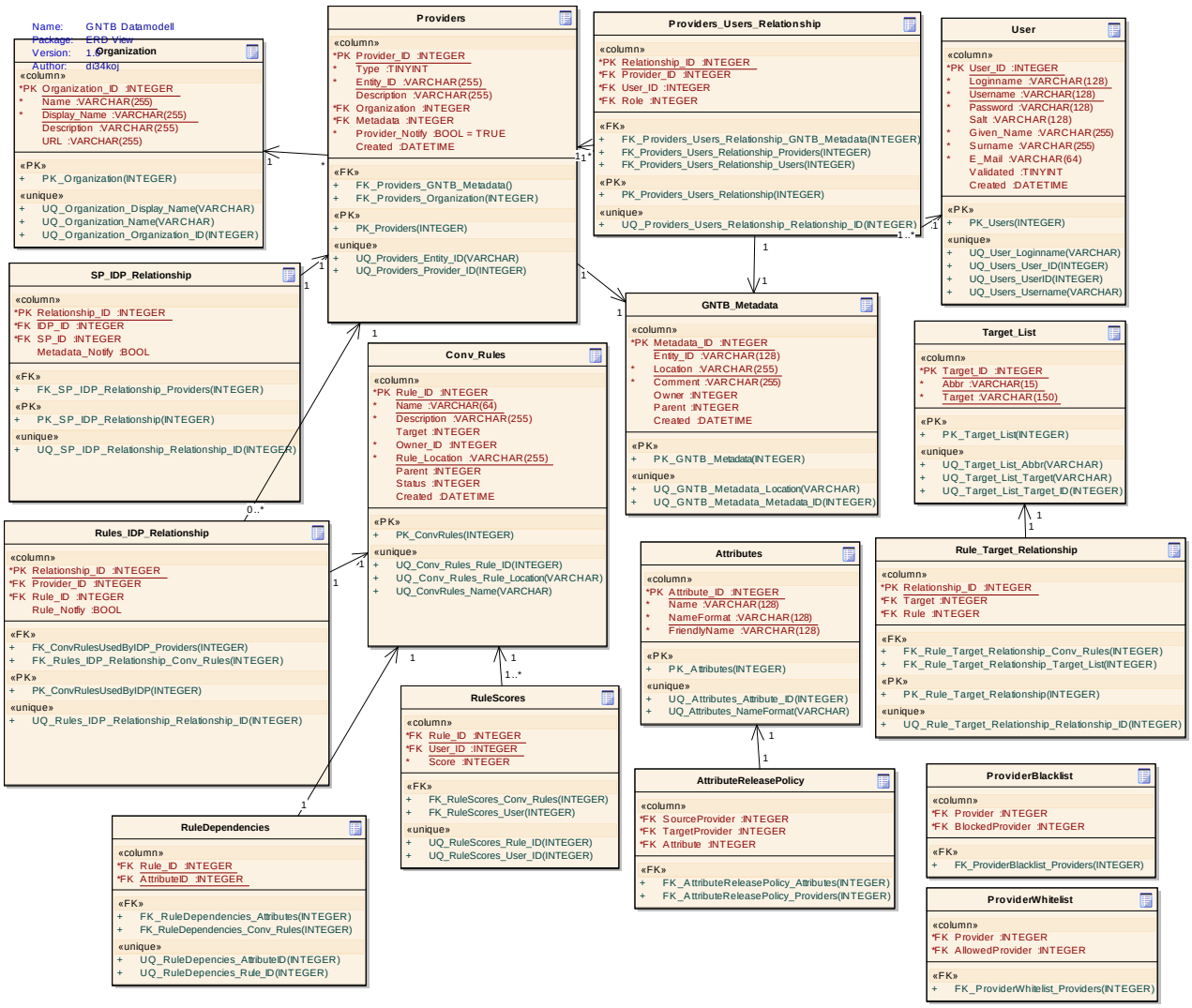

Figure 2-5: Data model as implemented

2.3.3 GNTB extension for IDP software

The extension for the Shibboleth IDP basically adds two new features, which have, like the IDP itself, been implemented in Java. These features are

1. a metadata provider that is able to provision the other components of the IDP with the metadata that was transmitted by the DAME TTP, and
2. two handlers that can be used by the GNTB core service to synchronize metadata and conversion rules.

Both components are implemented in their respective Java classes `TTPMetadataProvider` and `TTPMetadataSyncServlet`.

2.3.4 GNTB extension for SP software

The Shibboleth SP and the extension are implemented in C/C++. The extension basically has the same functionality as the IDP extension with the exception that the SP does not need conversion rule synchronization and application, as this is only done on the IDP side. But as SAML sessions, according to the SAML 2.0 Web Browser SSO Profile, are initiated by the SP, a special `SessionInitiator` element is needed.

More information on the implementation can be found in the deliverable D.4.1.1 and the documentation of the code.

Though the GNTB team implemented a running demonstrator, the implementation needs to be improved for the pilot phase. Therefore, in GN4 Phase 1 additional features will be implemented, e.g.,

- possibilities to configure the automation of the metadata exchange and addition of conversion rules.
- functionalities for statistics and monitoring.
- more funtctionalities for deleting and updating information.
- improved interface for Attribute Authorities (AAs) to re-use conversion rules.

GÉANT-TrustBroker will be a distinct task in the Joint Research Activity (JRA) 3 during GN4 Phase 1.

3 DAME Protocol

The DAME Protocol [DAME] describes the core workflow, i.e., triggering the metadata exchange, as already shown in 2.2.1. The metadata exchange itself is out of scope and can be done by the Metadata Query Protocol [MDQ]

The roadmap of standardization for the DAME protocol was described in milestone document M.1.2.1 [M.1.2.1] standardization roadmap. The decision was made for the standardization organization Internet Engineering Task Force (IETF), though SAML was standardized by Organization for the Advancement of Structured Information Standards (OASIS). The reasons, herefore, are that

- IETF seems to be more active,
- contact persons in IETF groups are known,
- and no fee respectively membership is required.

The core protocol specification was defined in the next step, before the IETF guidelines for Independent submissions [Independent] were applied.

In this chapter, the design of the DAME protocol is first shortly explained, before the current status of the I-D is shown.

3.1 Design of the DAME Protocol

The DAME Protocol was designed based on the IDP Discovery Workflow, shown in Figure 3-1. The GNTB workflow is similar to the workflow of the IDP Discovery Profile and extends the SAML2 Web Browser SSO Profile.

As it is based on the standard IDP Discovery Workflow, it uses the following Hypertext Transfer Protocol (HTTP) messages:

- HTTP GET requests, coloured grey in the figure
- HTTP POST messages coloured purple
- HTTP 302 (Redirect) messages coloured green

- HTTP 200 OK messages coloured pink

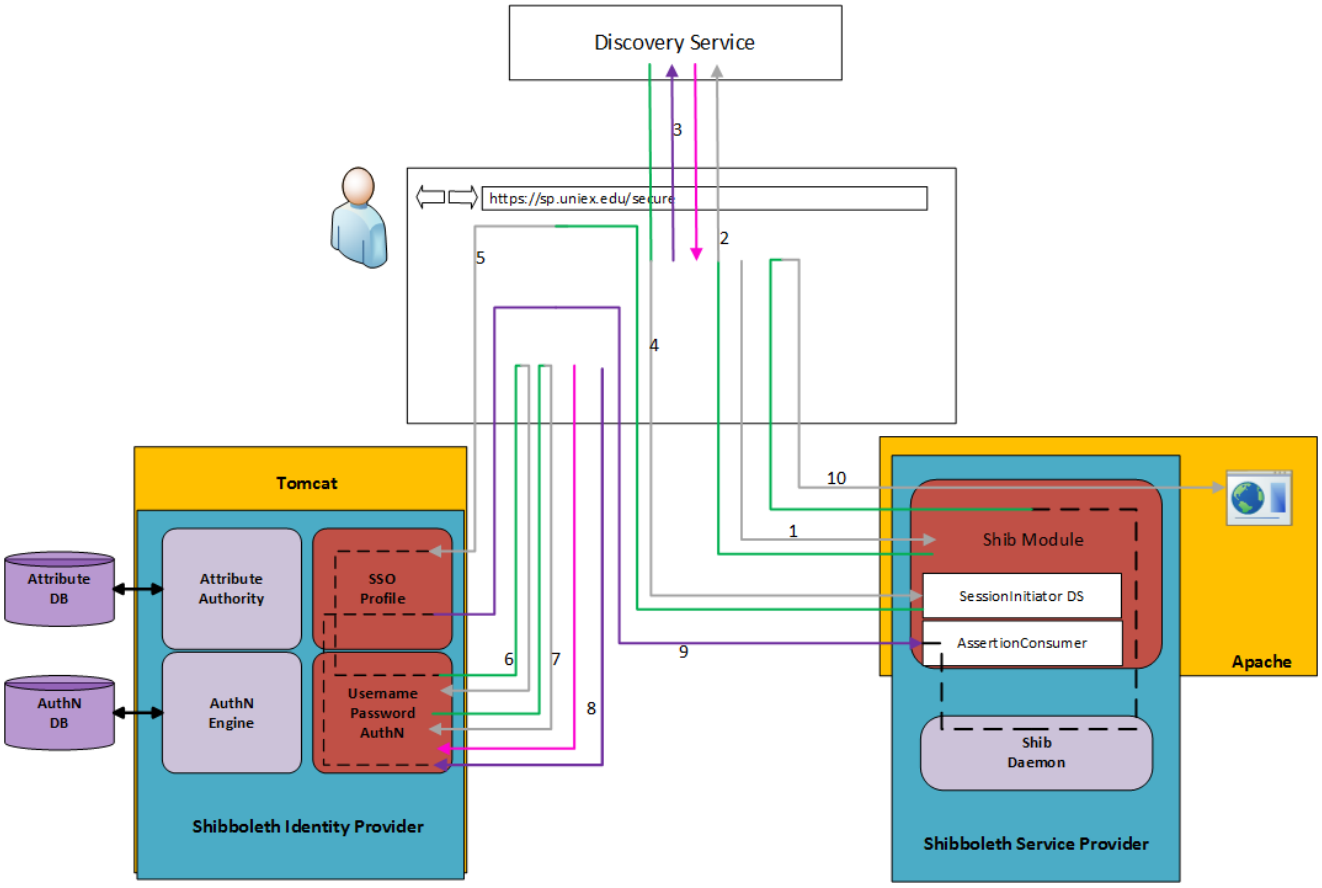

Figure 3-1: IDP Discovery Workflow

The first drafts (versions 00 and 01) of the I-D were explained in the milestone document M.2.2.1 [M.2.2.1].

As described before, the DAME protocol specifies the core workflow of GNTB, i.e., the metadata exchange between IDP and SP via a TTP called GNTB. The complete workflow is visualized in Figure 3-2. It comprises the following steps:

1. The user wants to make use of a service. As his IDP is not known by the SP, the Discovery Service of GNTB is used.
2. The user selects his IDP at the GNTB Discovery Service and triggers the core workflow.
3. GNTB informs the SP, which then sends an authentication request. GNTB caches this request, before it sends
4. Another authentication request to the user's IDP.
5. After the user has been successfully authenticated, the IDP sends the authentication response to the GNTB service.
6. GNTB then triggers the IDP to download the SP's metadata.

7. After the successful configuration of the IDP, the SP downloads the IDP's metadata and integrates it into the local configuration.
8. GNTB sends the previously cached authentication request to the IDP.
9. As the user is already logged in, the IDP sends the assertion with the user information to the SP.
10. The SP then grants the user access to the service.

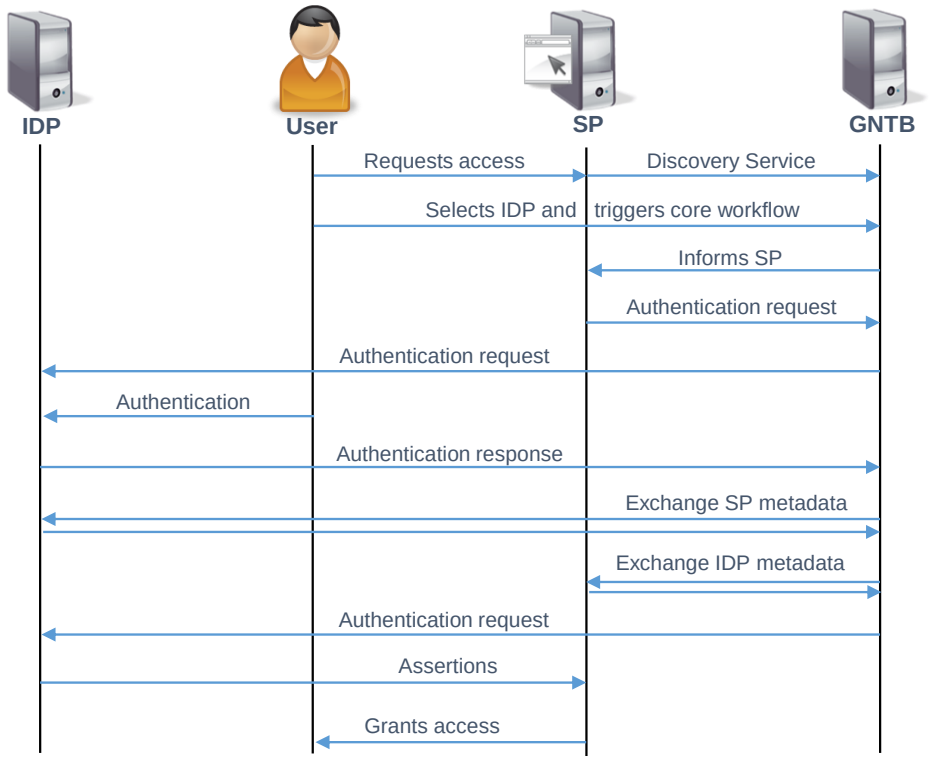

Figure 3-2: DAME Core Workflow

The I-D describes the workflow in a technical way, e.g., which HTTP messages have to be send by which party.

3.2 Current Status of the Internet-Draft

The current status of the I-D is explained in details in deliverable D.2.2.1 [D.2.2.1]. The document history is also visualized in Figure 3-3.

The drafts 01 and 02 were sent to the Research and Education Federations (REFEDS) mailing list and to researchers in GÉANT JRA3 and Service Activity (SA) 5. Furthermore, the I-D was presented at the 90th IETF meeting in Toronto by Stefan Metzger and at the European Workshop on Identity and Trust in Vienna by Daniela Pöhn.

Date	Version	By	Text
2014-12-16	02	Daniela Poehn	New version available: draft-poehn-dame-02.txt (diff from previous)
2014-07-08	01	Nevil Brownlee	ISE state changed to **Submission Received**
2014-07-08	01	Nevil Brownlee	Intended Status changed to **Informational** from None
2014-07-08	01	Nevil Brownlee	Stream changed to **ISE** from None
2014-07-03	01	Daniela Poehn	New version available: draft-poehn-dame-01.txt (diff from previous)
2014-06-18	00	Daniela Poehn	New version available: draft-poehn-dame-00.txt

Figure 3-3: Document history of the I-D

Based on the feedback we received and project-internal discussions, the following changes are scheduled for the 03 version of the DAME Internet-Draft (sorted by priority):

- Clarifications on the workflow, if one half of the metadata is already exchanged and if lazy sessions are used. At this point, the usage of the parameter `isPassive=true` and the Artifact Binding are reconsidered.
- Clarification on inappropriate usage scenarios that the user authentication steps protects against.
- Revision of security considerations on Secure Hash Algorithm (SHA)-1 in relation to SAML Artifact Binding.
- Publishing the I-D as an official Request for Change (RFC) within the Independent Submission Editor's stream or aiming for acceptance of the I-D as a working group document.

Version 03 with the changes listed above is planned to be submitted in May 2015. This is already part of JRA3 T3 in GN4 Phase 1. The received feedback for draft 03 can hopefully be included before the following IETF meeting in July. Though the main focus is on the preparations for the pilot operations of GNTB in GN4 Phase 2, the Internet-Draft still needs to be improved in order to become an official RFC within the Independent Submissions Editor (ISE). Therefore, the contact with REFEDS and IETF will be deepened.

4 Conclusions

This deliverable describes in a short form the design, conception and the implementation of the GÉANT-TrustBroker service, including the core GNTB service at the TTP, the SP extension, and the IDP extension. Furthermore, the design and current status of the DAME protocol, describing the initiation of the metadata exchange, is shown.

The dissemination of GNTB includes a TERENA Networking Conference (TNC) paper and a International Federation for Information Processing (IFIP) SEC paper, but is not limited to those two publications, as further scientific paper were published. The results of GNTB have been discussed at different workshops and meetings, including the 90th IETF meeting in Toronto and the European Workshop on Identity and Trust.

In order to have a fully working pilot, the demonstrator will be further improved during GN4 Phase 1. At the same time, the I-D will be improved as well in order to become an official RFC within the ISE.

References

[D.2.1.1]	D. Pöhn, S. Metzger, and W. Hommel: GÉANT-TrustBroker Specification. GÉANT Intranet.
[D.2.2.1]	D. Pöhn, S. Metzger, and W. Hommel: GÉANT-TrustBroker protocol specification. GÉANT Intranet.
[D.4.1.1]	D. Pöhn, M. Grabatin, S. Metzger, D. Schmitz, and W. Hommel: GÉANT-TrustBroker implementation with documentation. GÉANT Intranet.
[DAME]	D. Poehn, S. Metzger, and W. Hommel: Integration of Dynamic Automated Metadata Exchange into the SAML 2.0 Web Browser SSO ProfileL – work in progress. http://datatracker.ietf.org/doc/draft-poehn-dame/
[Independent]	RFC Editor, "Independent Submission" http://www.rfc-editor.org/indsubs.html
[M.1.1.1]	D. Pöhn, S. Metzger, and W. Hommel: Requirements analysis of GÉANT-TrustBroker. GÉANT Intranet.
[M.1.2.1]	D. Pöhn, S. Metzger, and W. Hommel: GÉANT-TrustBroker standardisation roadmap. GÉANT Intranet.
[M.2.1.1]	D. Pöhn, S. Metzger, and W. Hommel: GÉANT-TrustBroker protocol specification written. GÉANT Intranet.
[M.3.1.1]	D. Pöhn, S. Metzger, and W. Hommel: Project Géant-TrustBroker – dynamic identity management across federation borders. GÉANT Intranet.
[M.3.2.1]	D. Pöhn, S. Metzger, and W. Hommel: Géant-TrustBroker: Dynamic, scalable management of SAML-based inter-federation authentication and authorization infrastructures. GÉANT Intranet.
[M.4.1.1]	D. Pöhn, S. Metzger, and W. Hommel: TrustBroker service demonstrator. GÉANT Intranet.
[MDQ]	I. Young: Metadata Query Protocol – work in progress. http://datatracker.ietf.org/doc/draft-young-md-query/

Glossary

AA	Attribute Authority
API	Application Programming Interface
CSS	Cascading Stylesheets
DAME	Dynamic Automated Metadata Exchange
EDS	Embedded Discovery Service
FIM	Federated Identity Management
GNTB	Géant-TrustBroker
HTTP	Hypertext Transfer Protocol
I-D	Internet-Draft
IDP	Identity Provider
IETF	Internet Engineering Task Force
IFIP	International Federation for Information Processing
ISE	Independent Submissions Editor
JRA	Joint Research Activity
JSP	Java Server Pages
LRZ	Leibniz Supercomputing Centre
OASIS	Organization for the Advancement of Structured Information Standards
REFEDS	Research and Education Federations
RFC	Request for Change
SA	Service Activity
SAML	Security Assertion Markup Language
SHA	Secure Hash Algorithm
SP	Service Provider
SQL	Structured Query Language
SSO	Single Sign-On
SVN	Subversion
TNC	TERENA Networking Conference
TTP	Trusted Third Party
URL	Uniform Resource Locator
WAYF	Where are you from
XML	Extensible Markup Language
XSL	Extensible Stylesheet Languag
XSLT	XSL Transformation