22-04-2016

Deliverable D15.3
Operational GÉANT Trust Broker Pilot Instance

Deliverable D15.3

Contractual Date:	30-04-2016
Actual Date:	22-04-2016
Grant Agreement No.:	691567
Work Package/Activity:	15/JRA3
Task Item:	Task 3
Nature of Deliverable:	O (Other: Software)
Dissemination Level:	PU (Public)
Lead Partner:	SURFnet
Document Code:	GN4-1-16-102E38
Authors:	R. Poortinga-van Wijnen (SURFnet), D. Pöhn (DFN/LRZ)

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 691567 (GN4-1).

Abstract

This document provides high-level background and descriptive information about the GÉANT Trust Broker (GNTB) software release identified as Deliverable D15.3 of GN4-1 Joint Research Activity 3 Trust and Identity Research, Task 3 GÉANT Trust Broker, namely, the operational GNTB pilot instance, which was completed on 22 February 2016. The document covers operational GNTB pilot instance achievements (GNTB enhancements, pilot preparations, standardisation work, dissemination), final pilot instance setup, further information, and conclusions and recommendations.

Table of Contents

Executive Summary 1

1 Introduction 2

2 Operational GNTB Pilot Instance Achievements 4

2.1 GNTB Enhancements 4

2.1.1 Tracking and Monitoring 4

2.1.2 Integration of Other Entities – Attribute Conversion 4

2.1.3 GNTB Out of the Box 5

2.1.4 Shibboleth Upgrade 5

2.1.5 eduGAIN Integration 5

2.2 Pilot Preparations 5

2.3 Standardisation Work 5

2.4 Dissemination 7

3 Final Pilot Instance Setup 9

4 Further Information 10

5 Conclusions and Recommendations 11

References 12

Glossary 13

Table of Figures

Figure 3.1: Pilot setup 9

Table of Tables

Table 2.1: Dissemination activities 8

Executive Summary

This document provides high-level background and descriptive information about the GÉANT Trust Broker (GNTB) software release identified as Deliverable D15.3 of GN4-1 Joint Research Activity 3 Trust and Identity Research, Task 3 GÉANT Trust Broker (JRA3 T3), namely, the operational GNTB pilot instance, which was completed on 22 February 2016.

JRA3 T3 is the continuation of the GÉANT Trust Broker (GNTB) Open Call project in GN3plus, which developed a new protocol and proof-of-concept for dynamically building trust in the research and education community, with the intention of making the current setup of federated access management more dynamic and user-centric, and thereby increasing both ease of use and uptake of the Federation mechanism.

The goal of Task 3 was to build on the results of the GNTB Open Call project in preparation for a pilot to be started after Phase 1 of GN4. This involved further development of the proof-of-concept into a pilot-ready product. The enhancements implemented during GN4-1 to achieve this have included:

- Integration with the live eduGAIN service.
- Introduction of tracking and monitoring functionality.
- Integration of other entities present in the current federated landscape, such as Attribute Authorities, through an enhanced attribute conversion service.
- Providing GNTB “out of the box”, through a Docker image.
- Improvements made while upgrading the Shibboleth IdP.

Work to identify potential pilot users has begun, and, in parallel, outreach activities to disseminate the results of the research and engage with relevant groups have taken place at key events and in key publications.

Developing the operational GNTB pilot instance has led to a new Internet-Draft on Dynamic Automated Metadata Exchange (DAME), which has been submitted to the IETF.

A description of the final pilot instance setup is given in Section 3; further information and resources, including a demonstration video, access to the Internet-Draft and resources for deploying the Docker image, are available on the GNTB wiki pages.

It is recommended that the pilot goes ahead in the next phase of the GÉANT project, with a view to introducing a production service and delivering the benefits of more dynamic and user-centric federated access management in accordance with a schedule that will be defined at the start of the phase.

1 Introduction

GN4-1 Joint Research Activity 3 Trust and Identity Research, Task 3 GÉANT Trust Broker (JRA3 T3) is the continuation of the GÉANT Trust Broker (GNTB) Open Call project in GN3plus, which developed a new protocol and proof-of-concept for dynamically building trust in the research and education community, with the intention of making the current setup of federated access management more dynamic and user-centric, and thereby increasing both ease of use and uptake of the Federation mechanism.

The core of the GNTB proposal was the specification of a new automated metadata exchange service for large-scale authentication and authorisation infrastructures (i.e. federations and inter-federations such as eduGAIN). With GNTB, users can initiate the first-time contact between service providers (SPs) and identity providers (IdPs) to perform the required preparations for identity data exchange in a fully automated manner. The resulting benefits of this include a more dynamic trust model, the ability to reuse data conversion rules and automation of most of the previously manual configuration steps.

The goal of Task 3 was to build on the results of the GNTB Open Call project in preparation for a pilot to be started after Phase 1 of GN4. This involved further development of the proof-of-concept into a pilot-ready product. Enhancements identified at the start of the project as being required included:

- **Integration with the live eduGAIN service** (in collaboration with GN4-1 Service Activity 5 Trust and Identity Service Development (SA5)), in order to allow "live" testing in the pilot phase.
- **Introduction of tracking and monitoring functionality**, to gather the relevant statistics needed for evaluating pilot use.
- **Integration of other entities present in the current federated landscape**, such as Attribute Authorities e.g. Higher Education External Attribute Authority (HEXAA), etc.
- **Exploration of a "GNTB out of the box"** concept, in order to speed up introduction and setup of virtual federations.

This document provides high-level background and descriptive information about the GNTB software release identified as Deliverable D15.3 of JRA3 T3, namely, the operational GNTB pilot instance, which was completed on 22 February 2016. The document covers the following aspects:

- Operational GNTB Pilot Instance Achievements.
  - GNTB enhancements.
  - Pilot preparations.

    - Standardisation work.
    - Dissemination.
- Final pilot instance setup.
- Further information.
- Conclusions and Recommendations.

2 Operational GNTB Pilot Instance Achievements

This section summarises the key achievements attained in delivering the operational GÉANT Trust Broker (GNTB) pilot instance in the areas of enhancements, pilot preparation, standardisation work, further information and dissemination.

2.1 GNTB Enhancements

A number of enhancements were added to the GÉANT Trust Broker functionalities during GN4-1, both minor, such as automatic refresh (of conversion rules, for example) without a restart, and major, namely: tracking and monitoring, attribute conversion, GNTB out of the box, and Shibboleth upgrade. The major enhancements are described in more detail below.

2.1.1 Tracking and Monitoring

Useful metrics for statistics and monitoring were identified, and methods of collecting, aggregating and displaying those statistics for IdPs, SPs and federations were designed. The results can, for example, help the providers and federations determine which attributes are commonly requested, and which IdPs and SPs are regularly used together and form clusters, as well as identify which foreign countries a federation, IdP or SP collaborates with most.

2.1.2 Integration of Other Entities – Attribute Conversion

As part of the move away from basing the TrustBroker service on the Shibboleth CDS (see Section 2.1.4), the attribute conversion service was developed as a standalone server application. This application is based on the Tornado-JSON framework to build a scalable REST API for querying attribute conversion rules. The rules themselves are improved by defining a generic conversion rule format based on JSON. This format can then be used to generate application-specific versions of the conversion rules. This allows one rule to be used across multiple SAML implementations such as Shibboleth, SimpleSAMLphp or pySAML2. The generic format currently supports the merging, splitting and scoping of attributes. Advanced operations such as custom scripts cannot be translated across the different SAML implementations. Nevertheless, the GNTB approach for sharing implementation-based conversion rules can still be used in those cases.

2.1.3 GNTB Out of the Box

In order to ease the deployment and setup of GNTB at potential pilot institutions – and for subsequent use in the production environment – a Docker image containing the TrustBroker service was created. This image can be used to quickly evaluate the potential benefits of using GNTB.

2.1.4 Shibboleth Upgrade

GNTB makes extensive use of the standards-based, open source login and authentication software Shibboleth. With the end-of-life of the Shibboleth IdP version 2, the GNTB IdP plugin was adapted to the current Shibboleth IdP version 3. The adaptations needed were quite extensive, as much of the underlying architecture changed. This provided a good opportunity to improve the overall code quality and reliability of the plugin prototype implementation. In addition, the implementation of the core TrustBroker service itself was improved. However, during the course of GN4-1 it was announced that the Shibboleth Centralised Discovery Service (CDS), on which the TrustBroker service is based, will not be supported or updated from mid-2016 onwards; alternative systems were therefore explored. The best solution was determined to be rewriting the TrustBroker service as a standalone application using the pySAML implementation and a Python web framework such as Tornado (see also 2.1.2).

2.1.5 eduGAIN Integration

Integration with eduGAIN, one of the four main enhancements identified at the start of the project as being required (these are listed in Section 1), was not undertaken after all. The original goal was to improve the setup process for providers joining TrustBroker by allowing the import of whole federations into the TrustBroker database. However, during discussions at various meetings it was determined that the level of automation TrustBroker offers as it is was already a concern for providers, thus this feature was omitted in favour of other activities. As of now, each provider that wants to participate in GNTB has to register with the TrustBroker service manually (though a bulk import function is available).

2.2 Pilot Preparations

Potential pilot users were identified and contacted, a process that will continue until the pilot itself starts, in order to achieve the most diverse set of pilot users. Several providers have expressed an interest in participating in the pilot, including EGI. One confirmed pilot user is CLARIN within the next phase of the Authentication and Authorisation for Research and Collaboration project (AARC2).

2.3 Standardisation Work

The core GNTB workflow was defined, based on the specification for the initial metadata exchange, as Internet-Draft (I-D) Dynamic Automated Metadata Exchange (DAME) [DAMEDraft] and submitted

to the IETF. The I-D was further improved and discussed at the 93rd IETF Meeting in Prague, 19–24 July 2015.

2.4 Dissemination

Outreach has been an important aspect of the work of the GÉANT Trust Broker Task. The outreach activities carried out were mostly in two areas: dissemination of the research work results and engagement with relevant groups. The Trust Broker approach was presented at the REFEDS meeting in Porto during TNC2015, at the EWTI 2015 in Vienna, and at a German meeting of IdP administrators (ZKI Verzeichnisdienste Herbsttreffen) in Heidelberg. Furthermore, the research work was discussed at the conferences OID2015 and ICISSP2016, while the approach is also described in an IARIA journal paper. Details are provided in Table 2.1 below.

Type	Title	Event	Location	Date	Link
Presentation	GÉANT Trust Broker	REFEDS	Porto	14-06-2015	https://refeds.org/meetings/29th-meeting-june-2015
Demonstration	GÉANT Trust Broker	TNC2015	Porto	16-06-2015	https://tnc15.terena.org/core/event/26
Presentation	GÉANT Trust Broker	ZKI Verzeichnisdienste Herbsttreffen	Heidelberg	01-10-2015	https://www.zki.de/arbeitskreise/verzeichnisdienste/protokolle/zki-arbeitskreistreffen-am-01-und-02-oktober-2015-in-heidelberg/
Journal Paper	DAME: On-demand Internet-scale SAML Metadata Exchange	–	–	–	International Journal On Advances in Systems and Measurements, v 8 n 3&4 2015
Presentation	Topology of Dynamic Metadata Exchange via a Trusted Third Party	OID2015/ISSE2015	Berlin	10-11-2015	https://www.openidentity.eu/fileadmin/openidentity-files/pub/GNTB_OID.pdf (also appears in proceedings for OID2015)
Poster presentation	Risk Management for Dynamic Metadata Exchange via a Trusted Third Party	ICISSP2016	Rome	20-02-2016	http://www.icissp.org/TechnicalProgram/View/sessions.aspx

Type	Title	Event	Location	Date	Link
Presentation	Dynamic scalable metadata exchange	European Workshop for Trust and Identity (EWTI 2015)	Vienna	2–3 December 2015	https://identityworkshop.eu/
Presentation	OIDC federation	European Workshop for Trust and Identity (EWTI 2015)	Vienna	2–3 December 2015	https://identityworkshop.eu/

Table 2.1: Dissemination activities

3 Final Pilot Instance Setup

The final pilot instance, which has been shown at multiple demonstrations and presentations (see Section 2.4), consists of two identity providers (IdPs) and one service provider (SP) as well as the TrustBroker instance itself, as shown in Figure 3.1. The setup also contains additional non-permanent providers in order to test providers joining and leaving virtual federations within the TrustBroker network. Those non-permanent providers are not displayed in Figure 3.1.

This setup features the different versions 2 and 3 for the Shibboleth IdP to represent the real world more closely and to prove that the new version of the TrustBroker extension for IdP version 3 is compatible with the older version.

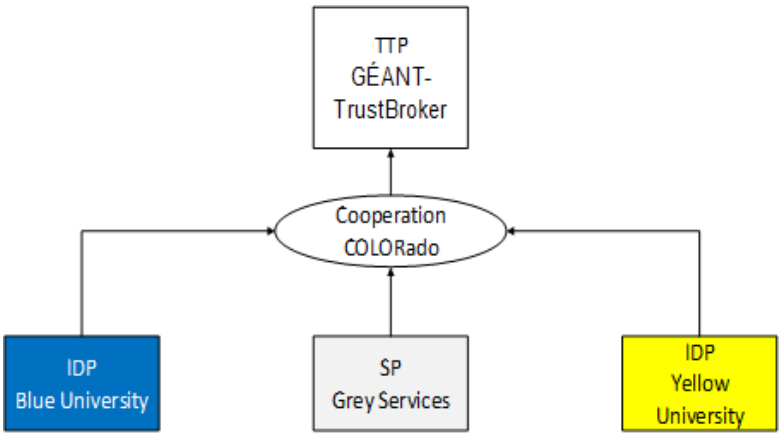

Figure 3.1: Pilot setup

4 Further Information

Further information and resources about GNTB is available on the GNTB Wiki pages [GNTBWiki], including:

- Flyer.
- Overview document.
- Presentation given at REFEDS meeting 14 June 2015.
- Demonstration video.
- Internet-Draft.
- Information and resources for Docker deployment.

5 Conclusions and Recommendations

During GN4-1, JRA3 Task 3 has achieved its goal of building on the results of the GN3plus GÉANT Trust Broker Open Call project to deliver an operational GNTB pilot instance. It has implemented most of the enhancements identified at the start of the project – namely, introduction of tracking and monitoring functionality, integration of other entities such as Attribute Authorities, and exploration of a "GNTB out of the box" concept – as well as applying others, capitalising on the opportunity for improvement afforded by applying a Shibboleth upgrade. In acknowledgement of providers' feedback, a decision was made not to undertake integration with the live eduGAIN service as part of the pilot.

Work to identify potential pilot users has begun – one confirmed pilot user is CLARIN within the AARC2 project – and, in parallel, outreach activities to disseminate the results of the research and engage with relevant groups have taken place at key events and in key publications.

Developing the operational GNTB pilot instance has led to a new Internet-Draft on Dynamic Automated Metadata Exchange (DAME), which has been submitted to the IETF.

It is recommended that testing of GNTB, based on the operational pilot instance delivered by JRA3 T3, should go ahead in the next phase of the GÉANT project, with a view to introducing a production service and delivering the benefits of more dynamic and user-centric federated access management in accordance with a schedule that will be defined at the start of the phase.

References

[DAMEDraft] D. Pöhn, S. Metzger, W. Hommel, M. Grabatin, *Integration of Dynamic Automated Metadata Exchange into the SAML 2.0 Web Browser SSO Profile*, draft-poehn-dame-04, December 7, 2015
https://datatracker.ietf.org/doc/draft-poehn-dame/

[GNTBWiki] https://wiki.geant.org/pages/viewpage.action?pageId=45844180

Glossary

AARC2	Authentication and Authorisation for Research and Collaboration
API	Application Programming Interface
CDS	Centralised Discovery Service
CLARIN	Common Language Resources and Technology Infrastructure
DAME	Dynamic Automated Metadata Exchange
eduGAIN	EDUcation Global Authentication Infrastructure. An initiative that interconnects research and education identity federations around the world, enabling the trustworthy exchange of information between service providers and research and education institutions or other identity providers.
EGI	European Grid Infrastructure
EWTI	European Workshop for Trust and Identity
GNTB	GÉANT Trust Broker
HEXAA	Higher Education External Attribute Authority
I-D	Internet-Draft
IARIA	International Academy, Research, and Industry Association
ICISSP	International Conference on Information Systems Security and Privacy
IdP	Identity Provider
IETF	Internet Engineering Task Force
JRA	Joint Research Activity
JRA3	GN4-1 Joint Research Activity 3 Trust and Identity Research
JSON	JavaScript Object Notation
OID	Open Identity
OIDC	OpenID Connect
REFEDS	Research and Education Federations
REST	Representational State Transfer
SA	Service Activity
SA5	GN4-1 Service Activity 5 Trust and Identity Service Development
SAML	Security Assertion Markup Language
SP	Service Provider
SSO	Single Sign-On
T	Task
T3	Task 3 GÉANT Trust Broker
TNC	The Networking Conference
ZKI	Centres for Communication and Information Processing (Zentren für Kommunikation und Informationsverarbeitung e.V.)