Géant-TrustBroker Project Overview

Leibniz Supercomputing Centre of the Bavarian Academy of Sciences and Humanities

Daniela Pöhn
7th FIM4R meeting

Frascati, Italy April 24th, 2014
Géant-TrustBroker [GNTB]:
The basic idea

Our goal (SP perspective):

- SPs connected to user’s identity provider (IDP)
- Independent of federation borders
- Establishing technical trust and configuration
- Without involving manual setup work by SP and IDP admins
Géant-TrustBroker [GNTB]:
The basic idea

More technical:

- GNTB facilitates the user-triggered, on-demand exchange of IDP and SP metadata as basis for SAML-based AuthNZ
- GNTB therefore *complements* existing
  - NREN and community federations
  - inter-federations (e.g., eduGAIN)
- GNTB will automate the setup of IDP-SP communication
  - *including* user attribute conversion
  - *excluding* organizational aspects
- GNTB will extend Shibboleth by IDP/SP plugins in order to
  - integrate the central metadata repository automatically
  - use attribute conversion rules
  - update the configurations of IDPs/SPs
Background:
Where are we today without GNTB?

Current situation:

• Two types of federations:
  • National federations operated by NRENs
  • Community federations operated by research communities / projects

• The resulting problem:
  SP and the user’s IDP need to be members of the same federation (or inter-federation)
Background: Where are we today without GNTB?

Current situation:

- **eduGAIN approach:** federation-of-federations-style inter-federation

- **Issues:**
  - Additional contracts increase the overall complexity.
  - Inter-federation schema is only the common denominator of NREN federations → SPs may not get all required attributes
  - Set up technical stuff, e.g., attribute filters/release policies, manually.
  - IDPs have to trust SPs → SPs might not get all required attributes
Géant-TrustBroker’s scope

GNTB is…

- a metadata registry: SPs and IDPs upload their metadata.
- a user attribute conversion rule repository: conversion rules can be shared and re-used by other IDPs.
- a virtual IDP and SP: The GNTB workflow seamlessly integrates into standard SAML workflows to “connect” SPs and IDPs on demand.
Géant-TrustBroker’s scope

- GNTB automates the technical setup of IDP-SP communication as far as possible.
- GNTB does not handle organizational aspects, such as the demand for written contracts with commercial SPs.
- eduGAIN and GNTB complement each other:
  - eduGAIN is the organizationally profound, long-term solution
  - GNTB allows for the quick setup of all technical aspects
Géant-TrustBroker’s workflow

GNTB workflows:
• Management workflows:
  – IDP/SP metadata
  – conversion rules
• Core workflow: technical trust establishment
The GNTB project

- GN3+ Open Call project (10/2013 – 03/2015)
- Internet-Draft to IETF in summer 2014
- Shibboleth-based prototype
- Pilot operations hopefully start early 2015
The GNTB project

• A milestone document describing GNTB’s technical workflows available on the GN intranet.

• Presenting GNTB at TNC2014

• GNTB
  • includes some more features, such as AccountChooser functionality.
  • May be interesting for other use cases, e.g., rapid provisioning.
  • Please contact us or check out the GNTB documents for details.
For more details, please see the documents published on TrustBroker’s Géant Intranet website:

https://intranet.geant.net/JRA0/GEANT-TrustBroker

To contact the project team, please email

geant-trustbroker@lists.lrz.de