GÉANT-TrustBroker project overview

Slides assembled by the Géant-TrustBroker team at Leibniz Supercomputing Centre, Germany for a short presentation by

Licia Florio

at the TF-EMC2 meeting

Zurich, Switzerland February 11th, 2014
Our goal from the user’s perspective:
Let users login to and use federation-external service providers (SPs) by connecting them to their identity provider (IDP) independent of federation borders and without involving manual setup work by SP and IDP admins.

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 when data schemas differ
  - *excluding* organizational aspects such as the need for written contracts between certain (commercial) SPs and IDPs
Background: Where are we today without GNTB?

- Historically, we have two types of federations:
  - National federations operated by NRENs
  - Community federations operated by research communities/projects
- The resulting problem: Users can only access a service when its SP and the user’s IDP are members in the same federation.
- The eduGAIN solution approach: Build a federation-of-federations-style inter-federation.
- eduGAIN is great, but inter-federations bring new issues:
  - Additional contracts increase the overall complexity.
  - The inter-federation schema (i.e., available user attributes) is only the common denominator of NREN federations; thus, eduGAIN SPs may not get all the attributes they require for full service functionality.
  - IDPs still need to set up technical stuff, e.g., attribute filters/release policies, manually. Therefore, users cannot use new SPs immediately.
GÉANT-TrustBroker’s scope

- GNTB is…
  - a metadata registry: SPs and IDPs upload their metadata just like in other federations.
  - a user attribute conversion rule repository: Inter-federation conversion rules can be shared and re-used by other IDPs.
  - a virtual IDP and SP: GNTB seamlessly integrates into standard SAML workflows to “connect” SPs and IDPs on demand. “Connecting” entities includes the exchange of metadata and the automated setup of user attribute conversion rules.
- GNTB automates the technical setup of IDP-SP communication as far as possible. Manual approval steps are optional.
- 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
The GNTB project

GNTB is a GN3+ Open Call project (10/2013 – 03/2015)
A milestone document describing GNTB‘s technical workflows in detail is available on the GN intranet.
GNTB‘s SAML-based core workflow will be submitted as Internet-Draft to the IETF in summer 2014.
We‘re working on a Shibboleth-based prototype.

Pilot operations can hopefully start before summer 2015.

GNTB functionality may be interesting for some other use cases, e.g., rapid provisioning of Shibboleth testbeds (suggested by Moonshot developers).

GNTB includes some more features, such as AccountChooser functionality. Please contact us or check out the GNTB documents for details.
To contact the project team, please email geant-trustbroker@lists.lrz.de