Géant-TrustBroker
Dynamic inter-federation identity management

Daniela Pöhn
TNC2014

Dublin, Ireland
May 19th, 2014
Agenda

- Introduction
- Motivation
- GNTB Overview
- GNTB in Details
  - Workflow
  - Initiation of GNTB Workflow
  - Metadata Registry
  - Feature Attribute Repository
- Conclusion
GNTB Introduction

• Géant-TrustBroker (GNTB):
  • Dynamic establishment of technical trust between Identity Provider (IDP) and Service Provider (SP)
  • Dynamic metadata exchange
  • First time contact initiated by the user
• GN3+ Open Call project (10/2013 – 03/2015)
• Internet-Draft to IETF in summer 2014
• Shibboleth-based prototype
GNTB Motivation

Current situation:

- Two types of federations:
  - National federations operated by NRENs
  - Community federations operated by research communities / projects
- Inter-federations, e.g., eduGAIN

Source: eduGAIN membership status
GNTB Motivation

The resulting problem:
SP and the user’s IDP need to be in **same federation** or inter-federation.

→ Communities need to participate in national federations or
→ need to join eduGAIN as a federation.
→ IDPs/SPs might need to join several federations.
→ Research partners outside eduGAIN / national federation cannot make use of Federated Identity Management.
Further Issues:

**Initial efforts**
- **Complexity**: Additional contracts increase the overall complexity for IDPs and SPs.
- **Manual work**: IDPs need to set up configuration, e.g., attribute filters / release policies, manually.
  → *Users may have to wait.*
- **Trust**: IDPs have to trust SPs.
  → *SPs may not get all required attributes.*

**Limitation** through schema: Inter-federation schema is only the common denominator of NREN federations.
→ *SPs may not get all required attributes.*
Agenda

- Introduction
- Motivation
- **GNTB Overview**
- GNTB in Details
  - Workflow
  - Initiation of GNTB Workflow
  - Metadata Registry
  - Feature Attribute Repository
- Conclusion
Our goal:

- SPs connected to user’s IDPs.
- Independent of federation borders.
- Dynamic establishing technical trust and automated configuration.
**GNTB Overview**

**Basic function:** Automate established workflows
- No manual setup work for IDPs
- No waiting time for users

**Features:** Attribute Conversion Rule Repository + Account Choosing
- Re-use of attribute conversion rules
- One rule for all

- Only needed: registration + plugin
- Complements existing approaches
Agenda

• Introduction
• Motivation
• GNTB Overview
• GNTB in Details
  • Workflow
  • Initiation of GNTB Workflow
  • Metadata Registry
  • Attribute Repository
• Conclusion
1. Researcher R wants to use a service at SP. R chooses her IDP at GNTB.
2. a) R triggers the technical setup. b) SP has to register at GNTB.
3. GNTB redirects R to his IDP for authentication.
4. a) IDP fetches metadata of SP. b) Configuration is automatically updated. IDP looks for attribute conversion rules.
5. IDP sends assertion to SP. R gets access to service at SP.
User R wants to make use of a service. Since he cannot find his IDP in the list, he chooses GNTB.
User R chooses his IDP at GNTB.

Welcome to Géant-TrustBroker's AccountChooser!

Choose an account

Daniela Pöhn
@gmail.com

Choose from registered IDPs

Learn more>

DFN-AAI - Leibniz-Rechenzentrum (LRZ)
Login via Shibboleth >
User R is redirected to his IDP for authentication.

Shibboleth Web Login

Account/Kennung:
Password:

[ ] Show me the data transmitted / Übertragene Daten anzeigen
Login

Weitere Informationen:

- Falls Sie noch keine LRZ-Kennung haben, orientieren Sie sich bitte an diesen Informationen.
- Zur Nutzung des von Ihnen angeforderten Dienstes "TERENA Service Provider Proxy" und weiterer im Rahmen der DFN-AAI und TUM, müssen Sie die entsprechende Loginmaske Ihrer Hematechnologie verwenden (betrifft insbesondere Studenten und Mitarbeiter von LMU): A.nicht möglich oder sehr stark eingeschränkt.
- Für Rückfragen kontaktieren Sie bitte den LRZ Servicedesk.
Agenda

- Introduction
- Motivation
- GNTB Overview
- GNTB in Details
  - Workflow
  - Initiation of GNTB Workflow
  - Metadata Registry
    - Attribute Repository
- Conclusion
GNTB Metadata Registry

- IDP/SP first needs to register at GNTB and install the plugin.
- Ownership and metadata are validated.

- Exchange of metadata on demand.
  → Automatically added to the local configuration.
  → Technical trust relationship established.
Agenda

• Introduction
• Motivation
• GNTB Overview
• GNTB in Details
  • Workflow
  • Initiation of GNTB Workflow
  • Metadata Registry
  • Attribute Repository
• Conclusion
Typical conversion rules:

- **Renaming:**
  attribute is named differently, e.g., Gecos → displayName

- **Transforming:**
  attribute transformed into another format, e.g., using yyyymmdd instead of dd.mm.yyyy

- **Splitting / Merging:**
  - source attribute needs to be split by a regex, e.g., attribute role (“Administrator”) of a given DN entry “cn=Administrator, ou=Groups, ou=application, o=lrz, c=de”
  - Merging two source attributes, e.g., givenName and surname, into a new one, e.g., commonName.
GNTB Attribute Repository

- Rules can be searched and re-used, e.g., within a federation
- Rules can be fetched by API calls by plugins
- Rule automatically added to local configuration

→ Only one IDP has to create rule
→ SPs receive all requested attributes
→ Rules could be used by other services, e.g., Attribute Authorities
Possible Administration Interface for managing conversion rules

Administration Interface for IDPs at Géant-TrustBroker

Manage own conversion rules
New conversion rules?
- Upload
Change or delete existing rules
Name of rule | Action
--- | ---
Service4all | Change > | Delete >

Conversion rules of other IDPs
Find suitable conversion rules
Géant-TrustBroker allows you to reuse conversion rules for service x.
- Name of rule | Action
Leibniz Supercomputing Center | Change >

Get notification of changed conversion rules
- Name of rule | Action
GlobalServ | Change >
Advantages of GNTB:

- **Metadata registry:**
  SPs and IDPs can download metadata.

- **User attribute conversion rule repository:**
  IDPs can share and re-use conversion rules.
  → Reduces manual work of IDPs.
  → Conversion rules automated integrated into local configuration.

- **Virtual IDP and SP:**
  GNTB workflow seamlessly integrates into standard SAML workflows to “connect” SPs and IDPs on demand.
  → SPs / IDPs only need a plugin.
GNTB Conclusion

• Shibboleth-based prototype
• Further development of GNTB in GN4
• Pilot operations hopefully start in GN4

• What have we done so far:
  • Workflows and Requirements
  • Data Model and Data Access Layer
  • Started with Protocols

• What we still need to do:
  • Protocols
  • Implementation
  • Internet-Draft to IETF in summer 2014
  • Documentation
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

géant-trustbroker@lists.lrz.de