

Authentication & Authorisation (AA) Framework



With the support of:

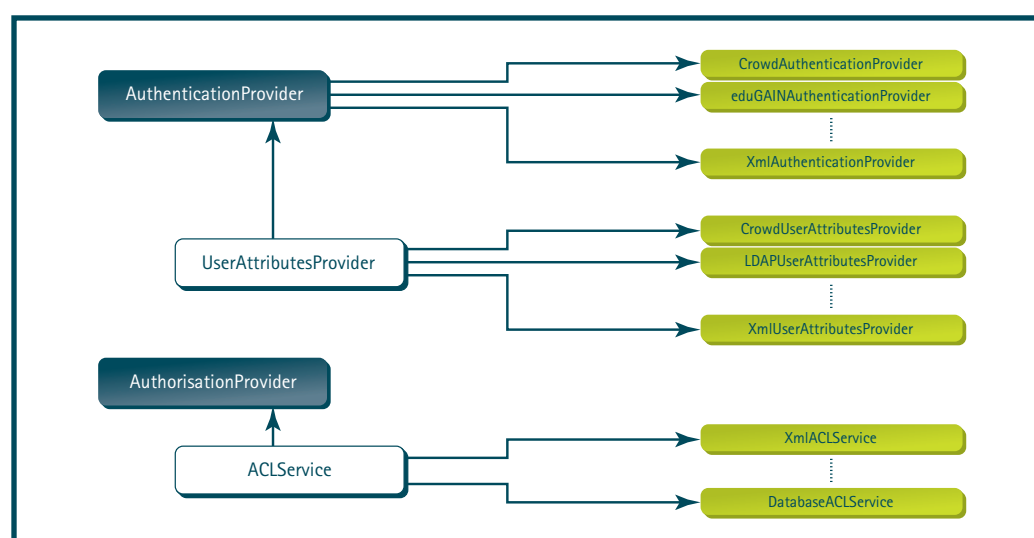


1 Motivation

- To provide a common and flexible AA solution for various GÉANT multi-domain network services in the GÉANT Service Area.
- To provide maximum control over authorisation decisions (Attribute/Role entitlements) to web resource provider.
- Facilitate use of available AA solutions for developers.
- Simplify eduGAIN integration.

2 Architecture

- Plug-in based extensible architecture
- Use existing frameworks, industry standards and best practices.
- Configurable Authentication Providers, User Attributes Providers and ACL services
- Technologies used include JAVA, Spring Security Framework, Crowd Integration library, OIOSAML.java library and Maven.



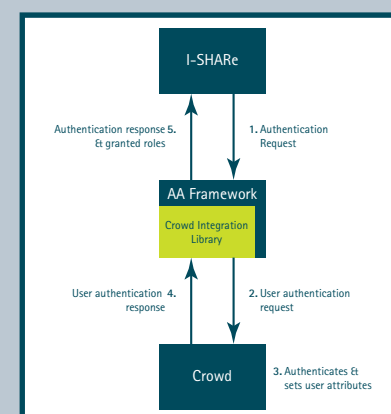
3 Features

- The current implementation provides following options:

	Authentication Provider	User Attributes Provider	ACL Services
Atlassian Crowd	✓	✓	N.A.
eduGAIN	✓		N.A.
LDAP	✓	✓	N.A.
Relational Databases	✓	✓	✓
XML	✓	✓	✓

4 Framework Users

- **Existing users:**
 - AutoBAHN (XML based)
 - I-SHARe (Crowd based)
- **Potential users:**
 - cNIS
 - perfSONAR
 - LHCOPN Portal
 - GÉANT Mail Archives, Tools Portal



5 Cross Activity Collaboration

- Collaboration with eduGAIN identified the use of **TLS with client certificates** as the optimal solution for securing web applications and services.
- Collaborating with eduPKI to set up Certification Authority for all GEANT Multi-Domain Network Services.

6 Future Work

- Implement web service support
- Upgrade to Spring 3.0
- Extend framework for perfSONAR requirements
- Provide UI for editing user attributes.

Forge Space – <http://aai.forge.geant.net/>