EUDAT Federated AAI TF
(Authentication Authorization Infrastructure Task Force)

EUDAT WP5

Slides by Jens Jensen+AAITF
Presented by Claudio Cacciari (c.cacciari@cineca.it)

Date: 2012/03/08
Outline

- Background
- Task force work plan
- Community’s benefits & issues
- Authentication and Authorization process
  - Actors
  - General overview
- Options
- Challenges
Background

New communities

Scientific Institutes

Universities

Homeless Scientists

Citizen Scientists
A task force dedicated to AA has been created to:
- Provide expertise
- Design the AA infrastructure

**2012**
- Task force start

**February**
- Pilot deployments

**May**
- Integration into core services

**August**
- **First phase (Feb-Aug)**
  - Starting with internal EUDAT core communities (ENES and CLARIN) 01.05.2012
  - Starting with most mature services (internal collaboration services, data transfer services) 31.07.2012

- **Second phase (Aug)**
  - Extending the interaction to all interested communities
  - Involving a wider range of services
Community’s benefits & issues

• Expected benefits of a federated AA infrastructure:
  – access to a wider range of services and increased collaboration opportunities.
  – decrease the cost associated to the user account management.
  – increase the level of security (establishing Level of Assurance, network of trusted IdPs …).

• Potential issues:
  – change of the policy to consider identity federation.
  – user’s sensitive attributes could be required.
AA process’ actors

1. Federations
2. Multiple IdPs (e.g. home institute IdP)
   - Provision for supporting “homeless” users, cf SWITCH
   - Attributes from home institute
   - Technology – IdPs should use the same technology
3. Attribute authorities
   - Attributes relating to collaborations/communities (e.g. roles, memberships)
   - Each community should be prepared to manage and publish the user attributes
4. Multiple service providers
   - All consuming the same identities and attributes
   - Single Sign on: single IdP
EUDAT High Level Organization

IdP A
IdP B
IdP #
Community IdP

IdP and AtP for homeless and Citizen Scientists

EUDAT
Federated AtP

Central Policy Rule registry

Service Provider A
Service Provider B
Service Provider #
Federations

• Policies: practices for participants
  – Who can be a member
  – Levels of assurance
  – PII
• Directory/information: who’s who
• Roots of trust
• Processes for adding/removing participants
• Support
• Monitoring/statistics
• Other federation level services (e.g. credential conversion, accounting, fed. level attrs.)
Identity Provider Requirements

- Identifiers MUST be personal
  - Attributes assigned to identity = individual
- MUST provide persistent identifiers
  - E.g. DN, eduPersonTargetedID
  - No recycling of IDs: MUST be allocated uniquely
Attribute Authority

• Run for/by communities
  – Scope = communities
  – IGTF best practices for AA

• Personal attributes
  – Data protection rules
  – User acceptance (once?)
  – Tied to identity

• The meaning of attributes
  – Not necessarily consistent across federations, or even within a fed, or even in a single AA 😞
  – Future work...
AA process: general overview

Some steps are of course optional

Technology

• Within the federation
  – Shibboleth (Web), Moonshot (Non Web)
  – eduRoam (based on RADIUS: Remote Authentication Dial-In User Service)
  – User certificates, OpenId
  – XACML (eXtensible Access Control Markup Language)
  – Oauth2 (Google, Facebook, Microsoft)

• Outside the federation
  – Credential conversion: special SP to create “external” credential
Options

• Join one or more existing federation(s)
  – Must comply with fed policies
  – Not always easy beyond national level
• Use IdPs from one (or more) existing federations
  – No control over IdPs, but they comply with known policies
  – Lowest common denominator problem
• Superfederate (cf. eduGain): WFAYF (Which Federation Are You From)
  – Baseline may be quite low
Challenges

• Leveraging existing identification systems

• Establishing a network of trust among the AA actors: IdPs, SPs, Attribute Authorities, Federations

• Attributes harmonization: it is necessary to agree on a common way to interpret different set of attributes.
Proposal 1

- Use WFAYF to Shibboleth federations
  - Use fed portal for initial login
  - SWITCH-type homeless IdP
  - Ignore policy requirements in short term?
- Optional: create certificates on-the-fly
  - Hidden from users, obviously
  - Needs fed level services, but ties into things-that-use-certs
  - Needs delegation mechanism, about ~4 options
Proposal 2

- Consume multiple credentials in front end
  - Support both portal and CLI
  - OpenID supported (ENES-friendly)
- Create credentials on the fly (cf Contrail)
- Fed-level attributes (only) initially
  - But can ingest from other sources
Additional Activities

• Track attribute (non-)harmonisation efforts
  – E.g. attribute translation matrix
  – Or genuinely deliver core attributes (e.g. nailed down subset of eduPerson – but you may not get it from IdPs)
  – Nail down attributes between communities – which is possibly possible

• Track related technology
  – E.g. Moonshot

• And Federations at the right scope
  – eduGain, eduRoam, ...
Additional Activities

• LoA
• Performance/scalability testing
• Determine (super)federation baseline policies
  – And whether they match requirements
  – Can we work around it when not?
• Test with Real Users(tm)