Attribute Authority Collaboration

Kristof Bajnok, NIIF (.HU)
Maarten Kremers, SURFnet (.NL)
Michal Prohazka, CESNET (.CZ)

REFEDs meeting,
18.05.2014, Dublin

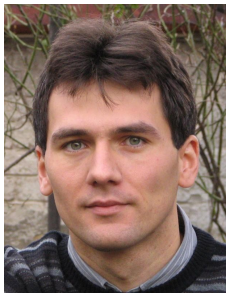
HEXAA

- HiEd eXternal AA – Open Call project
  - MTA SZTAKI + NIIF (Hungary)
- *More Than a Group Manager*
  - VO and a profile management interface that is capable to register any attribute
  - handle consent of attribute release if necessary
  - use SAML2 Attribute Authority
  - support provisioning, etc
- We Are Not Alone

Introducing speakers

Maarten K – ***SURFConext***
- and also GN3+ JRA3T1

Michal P – ***PERUN***



Kristof B – ***HEXAA***

Sources of information

- Why would you need more than one?
  - IdPs can not, should not or don't want to manage it
    - information outside the home institution's context
  - ► ***Virtual Organizations, AA***
    - After receiving an assertion from the IdP, the SP queries another Attribute Authority / group provider
      - eg. VO-managed access control
- Then, why would you need more than ***two***? (Multiple AA-s?)

Use case 1

Global SPs for global projects

- offer services to several projects
- possibly registered in different federations
- delegate access management at VO level

- VO user management must be done in one place
  - at most one VO management platform per project may be used
- Possible examples: e-Science projects (Umbrella, Clarin, ...)

Use case 2

Complex user profiles

- Parts of the user profile might be collected from different attribute providers
  - self-asserted
    - displayName, mail, photo, nick, phone, …
    - X.509 cert, SSH pubkeys, ...
  - VO-asserted
    - status/position in project
    - VO/project name, contact info, ...
  - governmental / value added attribute providers

VO platforms we know

	SAML2 AA	VOOT	GUI API	Attributes / Profile
***Conext**	No	Yes	Grouper	No (not in use)
HEXAA	Yes	No	Yes	Yes
PERUN	Yes	Yes	Yes	Yes
Sympa	Shib IdP	No	No	No
Switch GMT	No	No	No	Group Attributes
CoManage	Through LDAP	Yes	Yes	Yes

Attribute Aggregation

- SP level
  - works for a small number of attribute providers
    - SAML2 Attribute Query, VOOT
    - session initiation can be very long if there are slow / not responding providers
  - AQ works with Shibboleth and SSP (pending patch)
    - Shib creates multi-value attributes if multiple sources resolve to the same attribute
    - SSP has merging options as well (keep/merge/override)

Attribute Aggregation

- Proxy
  - all attributes in a single assertion
  - backend providers are queried in the background by the proxy
    - VOOT (membership + name + email)
    - any protocol (ldap://, sql://, ...)
  - shared (non-targeted) identifier necessary
  - Perun provides AA, if Conext would support SAML2 Attribute Queries, it could be used as an attribtute proxy as well

Group Aggregation

- Aggregation of groups from other VO mgmt tools
- Use of synchronization
  - VOOT
  - happens periodically in the background

Frontend / API

- Normal SP (though needs a shared ID)
- Some SPs want to view/manipulate groups
  - embedded group management in SP (consistent look & feel)
  - export the group information to other SPs
- VO mgmt tool has to provide API for group mgmt
  - VOOT or proprietary
- Perun has support, HEXAA is planning
  - Example: Management of mailing list membership - managed by Perun, but GUI is integrated into the web pages of VO.

Problems

- Attributes flowing here and there: privacy? Consent? → Facebook, Google+
- One AA per VO mgmt tool or per SP?
  - Problems with attribute release policy
- Attribute harmonisation
  - like “give me a name for the user”
    - cn, displayName, “$givenName $sn”, …
- Identifiers
- Who says what?
  - lack of support of 'attribute attributes' or LoA (JRA3-t1)

Consensus

- Protocols
  - keep VOOT simple
    - only group/role membership and basic personal info
  - SAML for accessing complex profiles
- Inter-AA operation
  - groups only (privacy)
- AA consolidation should be a continous joint effort

MTA SZTAKI

Thank you!

HEXAA Project is one of 21 beneficiary projects of the GÉANT Open Call research project initiative, which is part of the wider GÉANT Innovation Programme. The Open Call initiative brings fresh ideas to the GÉANT project and supports new uses of the network.

http://www.geant.net/MediaCentreEvents/news/Pages/GEANT_Open_Call_awards_EC_funding.aspx

GÉANT

Connect | Communicate | Collaborate

www.geant.net

www.twitter.com/GEANTnews | www.facebook.com/GEANTnetwork | www.youtube.com/GEANTtv

SEVENTH FRAMEWORK PROGRAMME