Common VO SAML attribute profile

Andrea Ceccanti (INFN)

EMI SAML task force

Common VO attribute profile

- Goal:
  - converge on the definition of SAML VO attributes understood by the three middlewares
- Requirements
  - Simple mapping of SAML to XACML attributes used in policies
  - Use dci-sec registered namespace
    - http://dci-sec.org/
- Attributes
  - VO membership
  - Group membership
  - Role possession

Common VO attribute profile

- The profile is available at
  - http://bit.ly/emi-vo-saml-profile
  - as a WIKI page
  - in EMI technical report format
    - but will need some introductory text to put things in context for people that weren't part of the task force

- VOMS implementation by Dec. 2011
  - current production version implements the straw-man proposal v. 3
    - cosmetic differences

- Interested clients should look at the authorization credential retrieval spec:
  - http://bit.ly/saml-authz-retrieval
  - Currently only the "Self query mode of operation" is supported

Profile adoption roadmap

- The current EMI use case is the integration of the VOMS AA with the UNICORE security stack and the ARGUS authorization service
- Adoption roadmap:
  - UNICORE client can fetch attributes out of VOMS SAML
    - as soon as VOMS SAML implements the latest profile (Dec 2011)
  - UNICORE services can fetch attributes for third parties out of VOMS SAML
    - as soon as VOMS SAML supports third-party queries (EMI 2)
  - UNICORE integrates with Argus
    - as soon as support for extracting attributes out of SAML assertion is implemented in Argus and the SPL is extended to express equality checks among XACML attributes

Links

- The SAML TF wiki page:
  - https://twiki.cern.ch/twiki/bin/view/EMI/EmiJra1T4SAML
- VO Attribute Profile v 1.0.1:
  - http://bit.ly/emi-vo-saml-profile
- Send comments and feedback to
  - emi-jra1-sec-saml@eu-emi.eu

Thank you

EMI is partially funded by the European Commission under Grant Agreement INFSO-RI-261611