Security Session Summary

John White for EMI Security Area

Helsinki Insitute of Physics

Padova, October 19th, 2011

Security Session

https://indico.cern.ch/sessionDisplay.py?sessionId=2&confId=147484#20111017

- Common Authentication Library
  - C, C++, Java
- XACML Profile Document
- SAML Profile Document
- Planned Updates to Argus
- Planned Updates to VOMS
- STS Plans
- EGI Middleware Requirements for Credential Validation
- Delegation

Common Authentication Library

PT "officially" formed (CZ*, UWar, UO). In all cases, effort assigned and working.

- C library :
  - Stubs ready. Provide the as-defined API.
  - Sample client/server available.
  - Working implementation Q4 2011.
- C++ :
  - ARC code being re-used.
  - End of November something to test.
  - **Some complications in certificate extensions*.**
  - **Error messages?**
- Java :
  - **Advanced. Still tbd namespaces/signing policy*.**
  - Test coverage almost there. Re-use of Util-Java.
  - Re-use of VOMS tests

Certificate extensions to be tabulated (ARC, TM).
Common error messages. "Java" set proposed as the basis.
Sensible namespace/signing policy default proposed.
All libraries will be cross-tested.

XACML Profile Document

https://twiki.cern.ch/twiki/bin/view/EMI/EmiJra1T4XACML
http://bit.ly/common-xacml-profile

- v1.1 will be done to add gLExec on CE (and WN).
- Adoption:
  - Argus PAP, PEP Server update (new profile and policies).
  - UNICORE* PDP callouts to Argus PAP.
  - ARC Security Handler callouts to Argus PEP Server. Effort needed.
  - CREAM update/change existing profile. Discuss for EMI-3.
  - WMS - comes along with WMS integration with Argus (EMI-2).

Some discussion needed for the UNICORE policies cases.

SAML Profile Document

http://bit.ly/emi-vo-saml-profile
http://bit.ly/saml-authz-retrieval

- Current target:
  Integration of VOMS with UNICORE security and Argus.
- Roadmap:
- UNICORE client to fetch attributes from VOMS-SAML.
  - → VOMS-SAML implements the latest profile (Dec 2011).
- UNICORE services to fetch attributes for third parties from VOMS-SAML.
  - → VOMS SAML supports third-party queries (EMI-2).
- UNICORE integrates with Argus.
  - → Support for extracting attributes from SAML assertion implemented in Argus.
  - → Argus SPL extended to express equality checks among XACML attributes.

Argus Updates

- SL6* and Debian 6 support.
- Implement the common XACML profile.
- Argus HA/Failover.
- PAP ability to import raw XACML policies.
  No clear requirement, must be discussed in detail.
- New SOAP XACML endpoint in PEP Server.
- Refactoring of the Argus-EES obligation handler.
- EMIR authorization support.
  Needs clarification. Hopefully Tuesday.
- PIP to handle VOMS-SAML assertion.
  Needed by...

VOMS Updates

- For EMI-1 (before end Q4 2011):
  - EMI packaging of NAGIOS probes.
  - VOM(R)S convergence.
    (`http://bit.ly/vomrs-convergence`).
  - Implementation of final version of the EMI VO SAML profile.
  - EPEL compliant packaging of voms-admin client.
- For EMI-2:
  - SL6 and Debian porting
    VOMS needs to be first.
- Longer term:
  - Unify the VOMS and VOMS Admin services codebase.
    Not for EMI.
  - Support for SAML AuthN assertions.

STS Development Plans

- Inputs: X.509, SAML, Kerberos, username/password
- Output: X.509, X.509 proxy, SAML, VOMS-SAML & kerberos
- First version to support ISSUE* operation.
- X.509 generator implemented, CMP protocol for online CA connection.
- Re-use of much OpenSAML3/Shib3. SAML assertion constructed using Shib3 WebFlow.
- Client Toolkit will be Java library to generate security tokens.
- Toolkit utilized in client UI or integrated with services (e.g. portals).
- Shib3: development phase, full functionality Q4 2011, release Q1 2012
  - The most important APIs are already stable.
- HIP 0.6 FTE, SWITCH 0.3 FTE
- First version of STS scheduled for Q2 2012.

EGI MW Reqs for Credential Validation

"EGI Middleware Requirements for Credential Validation"

(Selected) **Wish-list**

- **"Try to prevent spreading of Network Security Service (NSS) library use in m/w."**

(Selected) **Functionality:**

- All proxy certs should have RSA key size >=1024 bits.
  Why 1024? Need to measure performance for 2048?
- Support for OCSP
  A default configuration should be provided.

(Selected) **Compliance:**

- Honour meaning and scope on extensions
  Propose a list of mandatory extensions?
- Allow CRL files to be updated on a file system.
  Already does. Which services do not do this?
- Allow middleware to make authorization decisions based on the certificate policy OID extension.
  Requirement on Argus from EGI carefully expressed.

Delegation TF

- Participation: ARC and gLite, (compute, data and security)
- Demonstration of functional (early) framework for delegation conformancy tests.
- Captured more Compute use-cases (gLite, ARC)
  - Identified areas where gLite and ARC have different usage.
  - No show-stoppers.
- Discussion of limitations of current GDS.
  - No show-stoppers.
- Agreement on going forward with forming the OGF group.
  - Agreement on updating the GDS documentation.
  - Effort coming from ARC and gLite.
  - This will be an OGF document.
- Agreement for a follow-up meeting in ~3 weeks time.
  `https://twiki.cern.ch/twiki/bin/view/EMI/EmiJra1T4DelegationInEmi`

Thank you!

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