EMI project combines ARC, gLite and UNICORE stacks.
  - Security models are similar not identical.
    - gLite, ARC based on X.509 credentials for AuthN/AuthZ \(^1\).
    - UNICORE uses X.509 for AuthN, SAML attributes internally.

- Opportunity to improve the inter-operation.
- Unify and simplify the user credential handling.
- Provide common profiles and libraries for uniform operation.
  - Simplified credential handling
  - Common SAML profile
  - Common XACML profile
  - Common Authentication Libraries
  - Common Delegation method
  - Argus-EES.

- The Security Area developments follow these directions.

---

\(^1\) AuthN - Authentication (who you are)
AuthZ - Authorization (what you can(not) do)
Credential Handling

- Security Token Service “authenticates and authorizes” users based on security tokens.  
- Aggregates the required information from external sources.
  - eg. The Identity Provider (IdP)
- Establishes a trust relationship between different security/application domains.
  - eg. Institute login → VO VOMS.
- First STS version will support the ISSUE operation that transforms an incoming security token into another security token.
  - Incoming formats: X.509, X.509 Proxy, SAML, Kerberos
  - Outgoing formats: X.509, using external online CA X.509 Proxy, exploiting VOMS SAML Kerberos

- See next talk.

---

2 Security token: a collection of statements (or claims) about a user or resource, in this case: X.509 certificate, SAML assertion, Kerberos ticket, Username/Password
Common SAML profile
Common SAML profile

- Common user attribute schema for AuthZ/AuthN.
- Currently integrating UNICORE security with VOMS-SAML and Argus.
- UNICORE client fetches attributes from VOMS-SAML.
  - → Latest VOMS-SAML implements the profile.
- UNICORE services to fetch attributes for third parties from VOMS-SAML.
  - → VOMS-SAML to support 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.

Common XACML profile

- Allows to write standard AuthZ schemes for services.
- Adoption:
  - Argus PAP, PEP Server update (new profile and policies).
  - UNICORE* PDP callouts to Argus PAP.
  - ARC Security Handler callouts to Argus PEP Server.
  - CREAM update/change existing profile. Discuss for EMI-3.
  - WMS - comes along with WMS integration with Argus (EMI-2).

https://twiki.cern.ch/twiki/bin/view/EMI/EmiJra1T4XACML
Common Authentication Libraries

VO services
- Information System
- File Catalogue

common services
- VOMS (1 per VO)
- SLCS
- MyProxy
- WMS

SAML / VOMS
- SAML Kerb.
- IdP
- AAI Login

CA

Delegation
- proxy cert
- renewal of expiring cert. (through WMS)

UI

AAMI interop

SE
- proxy X.509 (DN tied to user name)
- delegates
- authZ
- authZ

Argus
- Resource(s) (CE, SE...)
- AuthZ OK
- AuthZ

Resource(s)
- authN (of presented X.509)
- authN (of presented X.509)

Sandbox

Delegation
- access to data

All Services: authN Lib.
Common Authentication Libraries

Provide a uniform layer for AuthN decisions.

- C library:
  - Delivered. EMI-2
  - Sample client/server available.

- C++:
  - Library delivered.
  - Still some details being worked out.

- Java:
  - Delivered.
  - Test coverage, Re-use of gLite Util-Java and VOMS tests.
  - Delivered with standards testing

Common error messages. “Java” set proposed as the basis. Libraries will be cross-tested. Adoption by services in EMI-2.
Common Delegation Method

- Participation: ARC and gLite, (compute, data and security)
  - Captured more Compute use-cases (gLite, ARC)
  - Identified areas where gLite and ARC have different usage.
  - Functional framework for delegation conformancy tests.
- No show-stoppers.
- Delegation agreement at:
  https://discordia.desy.de:2880/paul/Delegation/
- Will proceed to form an OGF group.

https://twiki.cern.ch/twiki/bin/view/EMI/EmiJra1T4DelegationInEmi
Argus EES

- “An obligation transformer used to ensure that an appropriate site-specific execution environment is procured based on the site-agnostic obligations and input attributes”.
- A service that may co-exist with Argus to start VMs or send jobs to a Cloud*.
  - Argus-EES ready for EMI-2.
  - Tested with Argus. (PEPd)
  - OpenNebula will come as update for EMI-2
- No show-stoppers.

http://www.eu-emi.eu/products/-/asset_publisher/z2MT/content/argus-ees
Argus EES

► “An obligation transformer used to ensure that an appropriate site-specific execution environment is procured based on the site-agnostic obligations and input attributes”.
► A service that may co-exist with Argus to start VMs or send jobs to a Cloud*.
  ► Argus-EES ready for EMI-2.
  ► Tested with Argus. (PEPd)
  ► OpenNebula will come as update for EMI-2
► No show-stoppers.

http://www.eu-emi.eu/products/-/asset_publisher/z2MT/content/argus-ees
Thank you!

EMI is partially funded by the European Commission under Grant Agreement RI-261611
First workshop (AAI). EGI Amsterdam 2010.
https://twiki.cern.ch/twiki/bin/view/EMI/EmiJra1T4AAI

Common SAML profile
https://twiki.cern.ch/twiki/bin/view/EMI/EmiJra1T4SAML

Common XACML profile
https://twiki.cern.ch/twiki/bin/view/EMI/EmiJra1T4XACML

Common Authentication Libraries
https://twiki.cern.ch/twiki/bin/view/EMI/EmiJra1T4SecurityCommonAuthNLib

Common Delegation method
https://twiki.cern.ch/twiki/bin/view/EMI/EmiJra1T4DelegationInEmi