UNICORE Security PT

Krzysztof Benedyczak

ICM Warsaw University

Products and elements

- UNICORE Security PT as other UNICORE PTs was greatly refactored.
  - Original division was artificial also there was refactoring in UNICORE core.
- Previous contents:
  - UNICORE Gateway, UVOS, XUUDB.
  - "XACML Entity", "UNICORE authorization data providers" (uas-authz), UNICORE security libs.
- Current contents:
  - UNICORE Gateway, UVOS (UVOS service, UVOS client), XUUDB

Products and elements

- What happened with the rest?
  - Everything in U. Container PT, product UNICORE Services Environment (USE).
  - "XACML Entity" -> XACML PDP (is a separate USE module now)
  - uas-authz -> AIP (Attribute Information Providers, moved to USE)
  - security libraries -> no change. Note: Technically sec. libs are not part of USE (are independent and sometimes used outside of USE). But we didn't want to have product for it due to EMI policies ;-)

Harmonization

- Argus integration
  - Argus PDP - existing. Automated tests, update to the EMI XACML profile.
  - Argus-PAP PDP - new one, will contact Argus PAP and download XACML policies.
    - Faster and Argus-fault resistant.
    - XACML2 evaluation already present for UNICORE.
- STS/AAI related work
  - developing STS client-library useful for all (also not-EMI) UNICORE clients.
  - integration with UCC (helping to).

Harmonization (2)

- Common authentication library
  - taking part in implementation (this PT manpower)
  - **integrating (USE, security libraries)**.
- SAML profile adoption
  - difficult because of backwards compatibility.
- VOMS integration to UNICORE
  - collecting VOMS requirements
  - UNICORE clients - production support for pushing SAML assertions (in fact for getting them - pushing itself is fine).

Evolution

- Optimization of the security stack.
  - Currently security related XML assertions are sent with every request.
  - It's a major overhead for small requests (higher network traffic and *processing*).
  - Security sessions are going to be used, so subsequent messages to the same container need not to repeat assertions.
- Resource sharing (aka team work) support.
  - Allowing small ad-hoc groups of people to share resources: files, jobs, workflows, target systems.