UNICORE - SAML usage

Krzysztof Benedyczak
ICM, University of Warsaw

UNICORE SAML components

- UVOS - UNICORE VO System. UVOS server provides:
  - SAML Attribute query implementation.
  - SAML Authentication implementation (SOAP and HTTP post bindings)
  - SAML Identity Mapping implementation.
- SAML attribute query clients (used with UVOS) are available:
  - in UNICORE base server container.
  - plugin for UNICORE Rich Client.
- SAML libraries for web portals authentication are also available.

SAML format usage

- SAML as a **format** is widely used in UNICORE.
- In some cases it is (*my private opinion*) overused.
- Standard usage:
  - SAML attribute assertions carrying user's attributes (both pushed by user and pulled by server).
  - SAML authentication assertions are used in some UNICORE related solutions for web portal authentication.

SAML format usage (2)

- Non-standard usage:
  - ETD assertions (encoded as attribute assertions)
  - Gateway-created authentication assertions (encoded as attribute assertions, should be authentication assertions).
  - So called "User assertions" (encoded as attribute assertions).
    - User assertions are created by clients to express wishes about the request (effective user name and others).
- In all cases predefined attributes are used to distinguish special assertions from regular ones.

SAML Protocol usage

- Only when interacting with UVOS:
  - attribute query
  - web portal client authentication
  - identity mapping (not really used anywhere).

Technical aspects

- Only SAML 2 is used.
- Proprietary UNICORE Java library is used.
  - opensaml library is not used as version 2.0 was not available when SAML was introduced in UNICORE.

UVOS

- Some features of UVOS are commonly used in UNICORE.
- Attributes:
  - No FQDN
  - From UVOS perspective all attributes are "generic".
  - There are attribute scopes. I.e. attribute may be valid only in scope a particular group.
- Identities:
  - Multiple formats are supported (DN, certificate, email).
  - Identities may be equivalent.

Attributes encoding

- There are some encoding issues:
  - empty, null and no-val attributes.
  - scoped attributes.
- There was a SAML profile created for defining all those issues.
  - collaboration with SAML-VOMS people (Valerio Venturi) in OMII-Europe.
  - is in quite good shape, however is not implemented anywhere (UVOS implements an earlier draft, SAML-VOMS ??).