AuthZ Interop: A common XACML Profile and its current implementation

Oscar Koeroo

Subject attributes

Overview of Subject attributes (0)

- **Subject-id**
  - Type: string
  - Example:
    - /O=dutchgrid/O=users/O=nikhef/CN=Oscar Koeroo
- **Subject-issuer**
  - Type: string
  - Example:
    - /C=NL/O=NIKHEF/CN=NIKHEF medium-security certification auth
- **Subject-serial-number**
  - Type: integer
  - Example:
    - 42

Overview of Subject attributes (1)

- **Subject-vo**
  - Type: string
  - Example:
    - gin.ggf.org
- **Voms-signing-subject**
  - Type: string
  - Example:
    - /O=dutchgrid/O=hosts/OU=nikhef.nl/CN=kuiken.nikhef.nl
- **Voms-signing-issuer**
  - Type: integer
  - Example:
    - /C=NL/O=NIKHEF/CN=NIKHEF medium-security certification auth
- **Voms-dns-port**
  - Type: string
  - Example:
    - kuiken.nikhef.nl:15050

Overview of Subject attributes (2)

- **Voms-fqan**
  - Type: string
  - Example:
    - /gin.ggf.org/APAC/Role=VO-Admin
- **Voms-primary-fqan**
  - Type: integer
  - Example:
    - /gin.ggf.org/APAC/Role=VO-Admin

Overview of Subject attributes (3)

- **CA-serial-number**
  - Type: integer
  - Example:
    - 1
- **Cert-policy-oid**
  - Type: string
  - Example:
    - 1.2.840.113612.5.2.4

Overview of Subject attributes (4)

- **Cert-chain (experimental)**
  - Type: string
  - Example:
    - *MIICbjCCAVagAwIBAgICBNgwDQYJKoZIhvcNAQEEBQAwTDES*
      MBAGA1UEChMJZHV0Y2hncmlkMQ4wDAYDVQQKEwV1c2Vycz
      EPMA0GA1UEChMGbmlraG…(base64)

Obligations

Obligations (0)

- **UIDGID**
  - UID (integer): Unix User ID local to the PEP
  - GID (integer): Unix Group ID local to the PEP
  - Stakeholder: Common
  - Must be consistent with: Username
- **Username**
  - Username (string): Unix username or account name local to the PEP.
  - Stakeholder: VO Services Project
  - Must be consistent with: UIDGID
- **SecondaryGIDs**
  - Complex type solution
    - ListOfGIDs (list of integer): List of secondary Unix Group ID (GID) local to the PEP. Each UID is of type Integer
  - Multi recurrence
    - GID (integer): Unix Group ID local to the PEP
  - Stakeholder: EGEE
  - Needs obligation(s): UIDGID

Obligations (1)

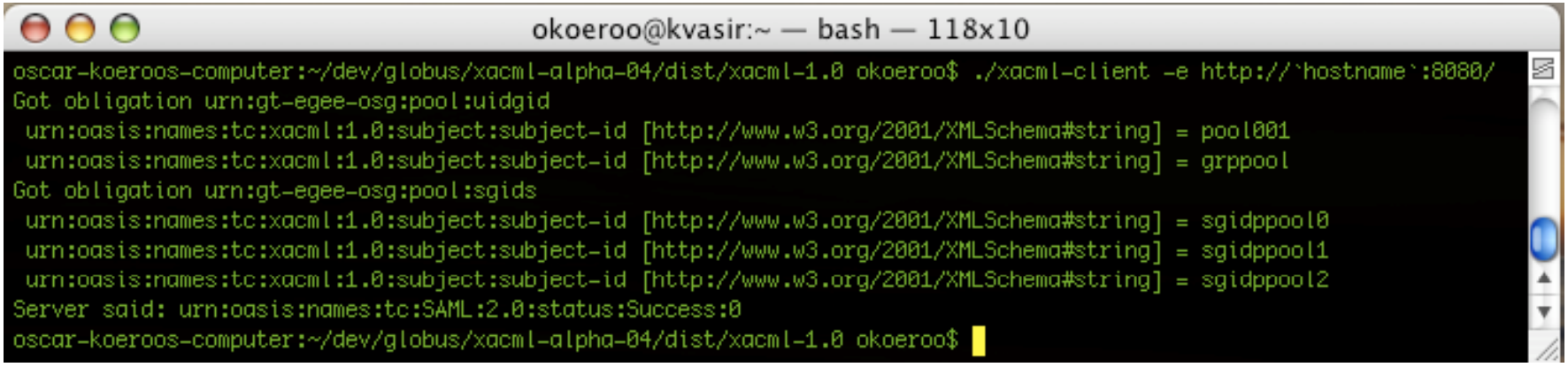
- **AFSToken**
  - AFSToken (string) in base64: AFS Token passed as a string
  - Stakeholder: EGEE
  - Needs obligation(s): UIDGID

Obligations (2)

- **RootAndHomePaths**
  - RootPath (string): this parameter defines a sub-tree of the whole file system available at the PEP. The PEP should mount this sub-tree as the “root” mount point (‘/’) of the execution environment. This is an absolute path.
  - HomePath (string): this parameter defines the path to home areas of the user accessing the PEP. This is a path relative to RootPath.
  - Stakeholder: VO Services Project
  - Needs obligation(s): UIDGID or Username
- **StorageAccessPriority**
  - Priority (integer): an integer number that defines the priority to access storage resources.
  - Stakeholder: VO Services Project
  - Needs obligation(s): UIDGID or Username

The implementation

It works!



- **Code snippets forwarded to Joe**
  - Creation/add/free of an Obligation structure

Still open to C

- **Still open for discussion on the C implementation:**
  - Request send out to be able to handle the SSL/TLS plumbing our selves
    - Joe is investigating
  - Propagation of the understood Obligations from the PEP to the PDP and interacting with that content

Stuff we don't have time for

- **The relationship between:**
  1. the SSL client peer identity
  2. SAML assertion Sender Receiver
  3. SAML-XACML Requester / Responder
  4. XACML <Subject> attributes
  - (not for this discussion) multiple XACML <Subject(s)>

- **Name spaces for the attributes and identifiers in all sections**
  - We may use the registered OID of Nikhef JRA3 Security
    - urn:OID:1.3.6.1.4.1.10434.3.40212:

?