NAREGI AuthZ Service
- NAREGI's XACML Profile -

Jan 29, 2007
Takuya Mori
NAREGI WP-5 Security / NEC Corporation

abstract

- As part of NAREGI Project, a proto-type AuthZ service is being developed
  - SAML 2.0 & XACML 2.0 based AuthZ service
  - Based on GT4.0 AuthZ Framework
- We defined our Profile for mapping attributes to XACML request context
- We introduce our experience from this proto-type.

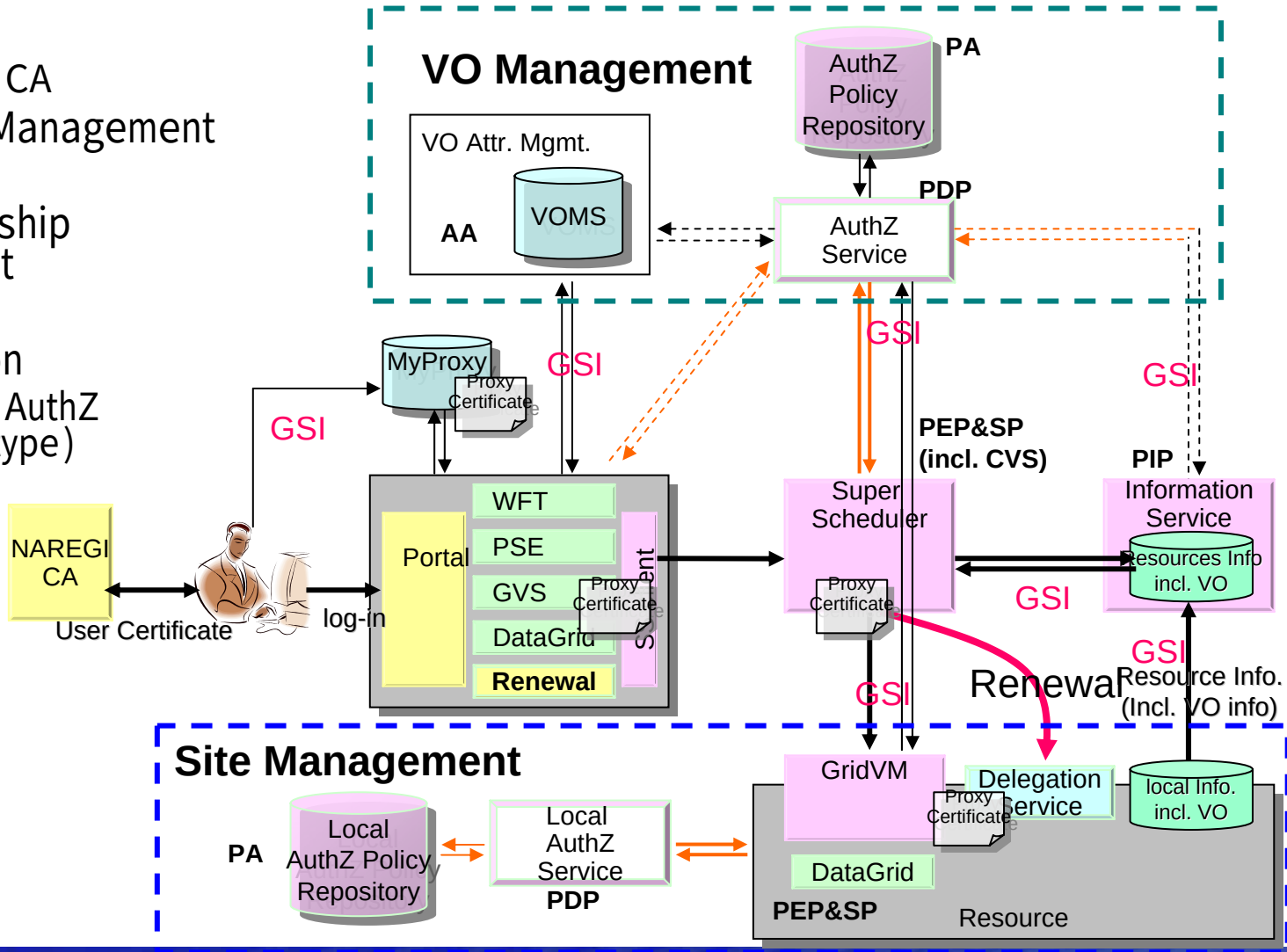
Back ground: Two Profiles

Use of XACML Request Context to access a PDP & Use of WS-Trust and SAML to access a CVS

- David Chadwick et al., in 2006
- to specify a protocol to access a PDP and a CVS
- Subject Attribute
  - X509 Subject Name is used for a subject attribute
  - Other attributes are not discussed at this moment
- Resource Attribute
  - wsa:To element value in a SOAP header for urn:oasis:names:tc:xacml:1.0:resource:resource-id
- Action Attribute
  - wsa:Action element value in a SOAP header for urn:oasis:names:tc:xacml:1.0:action:action-id

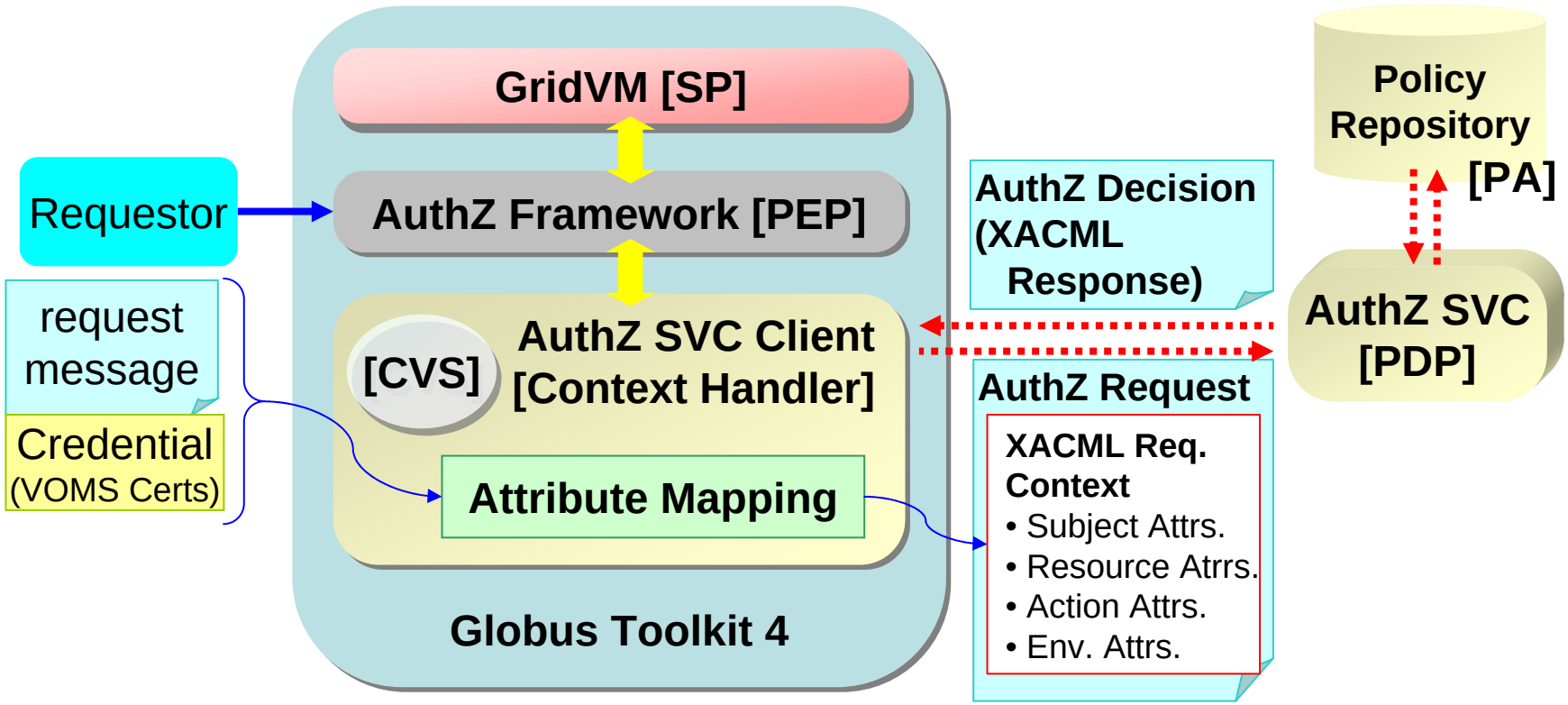
Security Architecture - Overview

- CA
  - NAREGI-CA
- Credential Management
  - MyProxy
- VO Membership Management
  - VOMS
- Authorization
  - NAREGI-AuthZ (Proto-type)



NAREGI AuthZ
- Functional Components -

- SAML 2.0 Profile of XACML 2.0 for AuthZ SVC protocol
- AuthZ SVC Client has an internal Credential Validation Service (CVS)
- XACML 2.0 based policy decision



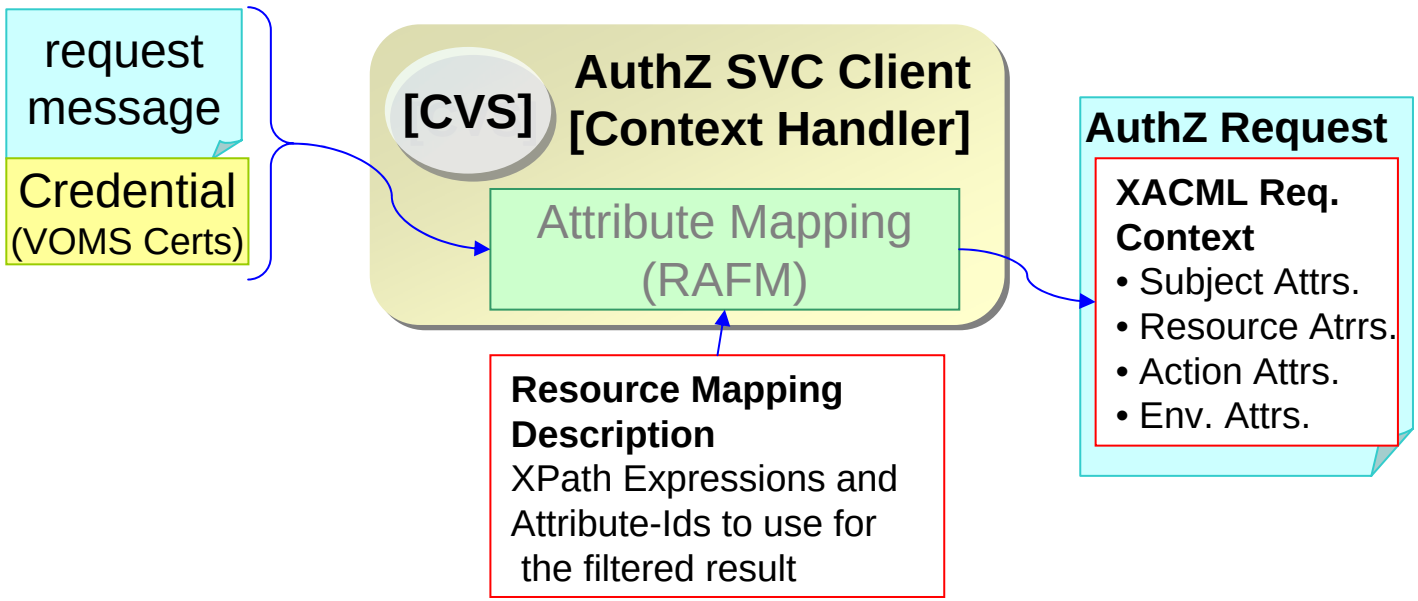
Subject Attribute

- Attributes are retrieved from a VOMS Attribute Certificate
- UserDN:
  - ID: “naregi:vo:userDN”
  - Value: User Globus ID (in String format)
- VO Name:
  - ID: “naregi:vo:voName”
  - Value: VO Name (in URI format)
- Group:
  - ID: “naregi:vo:group”
  - Value: Group Name (in String format)
- Role:
  - ID: “naregi:vo:role”
  - Value: Role Name (in String format)
- Capability:
  - ID: “naregi:vo:capability”
  - Value: Capability Name (in String format)

Note: the IDs described in this “Mapping” are tentative

Resource Attribute

- Attributes are retrieved by Resource Attribute Filtering Mechanism (RAFM)
  - RAFM (an XPath filter) retrieves resource attributes from the request SOAP message
  - RAFM allows a service provider to select attributes to use for AuthZ decision
  - RAFM allows the AuthZ service to make AuthZ Decision based on the message content of the request to the SP



Action Attribute Mapping

- Action Attribute is retrieved from the action property of the Message Context on GT4.0 AuthZ Framework
  - ID: “naregi:action”
  - Value: the value of action property
- wsa:Action may also work well (we used the action property because it is easily available)

Experiences we've got

- NAREGI's XACML profile
  - Subject Attributes:
    - Maps of VOMS attributes in XACLM Subject Attributes
    - Needs standardized attribute IDs for well-known types of credentials such as VOMS attribute certificate
  - Resource Attributes:
    - RAFM enables flexible resource attribute retrieval from the request message content to SP
    - To support for authorization for WS-Resource or finer-grained resource, this kind of mechanisms is needed
  - Action Attributes:
    - Maps GT4.0 AuthZ Framework Property to an XACML Action Attribute
    - wsa:Action may also work well

The End

Future Plan

- support for Environment Attribute
  - what are requirements?
  - what are use cases?
- support for Obligation
  - what are requirements?
  - what are use cases?
- policy management mechanism
  - need DBMS to manage policies
- support for NAREGI Information Service for better information retrieval
  - attribute retrieval method