



# State of Authorization in HE

# Different arenas

- *From local to global*

- <https://spaces.internet2.edu/display/macepaccman/Access+Management+Recipe++V2>

- *Groups are things you belong to*
  - *A group is a named collection of identities*
- *Roles are things you are*
  - *A collection of entitlements*
  - *implicit role = a role which is not directly assigned, but is implied due to something else.*
- *Entitlements are things you have*
  - *An entitlement is a multivalued attribute that can have zero or more string values . The values of the attribute are indicators of an additional right to a thing, object, or service.*

# AuthR in a federated environment

- *Transition phase*

- *One or more simple attribute values as basis for AuthR decisions*

- *eduPersonAffiliation, ou, o, ...*

- *More complex attribute values*

- *eduPersonEntitlement*

# Entitlements in GMAI

- *General Model for Authorization Information (GMAI)*

- *a tuple with two or more elements of authorization information*

1. *Application/application area*

2. *Role/User type*

3. *additional restrictions*

urn:mace:swami.se:gmai:

`<application>:<role>(:<scopeDenominator>=<scopeValue>)*`

# GMAI use case

- *Uppsala University, Sweden*
- *Used GMAI since 2006 in their identity Management system AKKA.*
- *generalized forms*

urn:mace:swami.se:gmai:{application}:{role}:  
norEduOrgUnitUniqueIdentifier={role organisation}

urn:mace:swami.se:gmai:{application}:{role}:  
swamiCostCenterIdentifier={costcenter code}

urn:mace:swami.se:gmai:{application}:{role}:  
uuLadokInstitutionskod={studentregistry organisational code}

# GMAI@UU.SE

- *Uses GMAI for the Studentportal, TCS Personal (eScience) administration rights, the Swedish admission system, University education catalogue and University webCMS.*
- *Also uses GMAI to describe our users acceptance of our different Acceptable Use Policies (common and application specific). For this we uses two limitations instead of one as above. The AUP acceptance is stored on the form*

urn:mace:swami.se:gmai:AUP:{AUP type}:  
version={versionnumber}:  
timestamp=YYYY-MM-DD TT:MM:SS.

# GMAI@NyaA

- urn:mace:swami.se:gmai:nya-dw:base:o=YY
- urn:mace:swami.se:gmai:nya-dw:  
department:o=YY:norEduOrgUnitUniqueNumber=ZZZZ

# AuthR@UMA

- urn:mace:rediris.es:uma.es:  
    applAccess:{appName}:{applicationDependentData}
- urn:mace:rediris.es:uma.es:  
    applAccessAdmin:{appName}:{applicationDependentData}
- urn:schac:userStatus:service:mail:send:blocked

# 'unsolved' use case (1)

- *A use case not easily supportable today are web portals with proper end-user authentication/authorization for access to third party services behind the web portal ('delegation').*
- *the portal should be able to act on behalf of the user, but the third party service provider wants to verify that the portal is entitled to do so.*
- *Thomas Lenggenhager*

# 'unsolved' use case (2)

- *a French course is being co-taught between a Brown professor and a professor at a French University. Half of the students come from each campus. They are required to access digital resources made available from servers at Brown. Digital work that they do is a part of their grade, so some level of assurance is required.*
- *Steven Carmody*

● *The US NSF has sponsored a Math institute here at Brown (<http://icerm.brown.edu/>). Each semester, and the summer, they bring 50 fellows to the Brown campus to work on a problem; 40% of them come from outside the US. After a group returns to their home campus, there is a strong desire that they continue working together. However, when they leave, their Brown-issued credentials are deactivated, and they must use other credentials to access the collaboration spaces at Brown.*

- *Steven Carmody*



Questions ?