GMAI - General Model for Authorization Information

This information is moved from the old SWAMI web site. SWAMI was an alliance for middleware with members from the Swedish higher educational sector. One of the results from this group was General Model for Authorization Information (GMAI) another was the identity federation SWAMID.

The two extreme approaches to authorization information and authorization are:

1. Give the precise position/role of the user within the organisation and let the authorization system draw the conclusions of what authority this gives.
2. Describe as careful as possible what authorities the user has in a particular system.

This document presents a General Model for Authorization Information, for short GMAI, that can be used for both these cases. The model suggests that most authorization decisions can be based on a tuple with two or more elements of authorization information. The two first elements contain information about Application/Application Area, and Role/User Type respectively. If applicable there may, in addition, be one or more elements defining restrictions on the Scope of Authority. These tuples can be explicitly stored in for example an LDAP directory or generated as requests for authorization information is received.

It is further suggested that for federated authorization within the Swedish higher education sector, the following roles should be used: Self Reporter; Handling Officer; Reviewer; Certifier; Controller; Reader.

These suggestions are based on the result of the work done by a working group in SWAMI - the Swedish Alliance for Middleware Infrastructure, whose task was to suggest a small set of nationally harmonised roles to be used for federated authorization among Swedish higher education institutions. The working group members were selected from both the human resource and IT area, to get a wider perspective.

Further reading and GMAI LDAP schema:

- gmai.pdf
- gmai.ldap.schema

It's possible to store GMAI values in the attribute eduPersonEntitlement but this attribute has no substring matching rules so there is a special attribute swamiGmaiAssertion with substring matching activated. Please use eduPersonEntitlement when you're doing a attribute release in SAML WebSSSO. When sending values via SAML WebSSO the Identity Provider should filter what values are sent to a specific Service Provider due to the risk of security information release based on that most GMAI values is about access control to services.