The Swedish Alliance for Middleware Infrastructure

The Swedish Alliance for Middleware Infrastructure, SWAMI, is the organisation for middleware cooperation in the Swedish higher education community. It is financed by its members and by Sunet.

The goal of SWAMI is to build a sustainable organisational framework for, mutually beneficial, cooperation in matters relating to an infrastructure for authentication and authorization within the Swedish higher education community.

Areas of cooperation

In this field there are many areas where cooperation has the potential to be very rewarding for the participating partners. Some of these are

- General sharing of knowledge and experiences through workshops and conferences
- Sharing the costs for development and adaptation of applications and infrastructural systems
- Sharing the costs for examining alternatives in technical choices for common needs
- Running joint services

Actively seeking to create opportunities to cooperate

SWAMI has the ambition to support these and other ways of harvesting the benefits of cooperation. The potential for cooperation to bear fruit is greater when several institutions adopt similar solutions. Therefore, SWAMI develops recommendations for different middleware components and procedures. For the development of joint services and systems, like roaming network access and a national student admittance system, there is a need for harmonising some aspects of identity management and attribute release. Harmonisation issues of this sort are also an area where the SWAMI framework is useful.

Support for developing middleware infrastructure

SWAMI also offers advice and support to institutions that have not yet but are planning to adopt a middleware infrastructure strategy. This support can take the shape of working out recommended roadmaps. Furthermore, SWAMI can, where feasible, fill a function by putting together pre-packaged solutions for integrating some of the most common AAI components.

SWAMI is governed by the SWAMI Council which is advised by the Expert Team. Please visit our website at www.swami.se for further information about SWAMI.

SWUPKI – The PKI for the Swedish higher education community

SWUPKI is the public key infrastructure for the Swedish higher education community. It started as cooperation between Umeå Universitet and Stockholms Universitet. Since then many other universities and other organisations in the education community have joined. SWUPKI has now become a service within SWAMI.

A PKI to stay in control of our infrastructure

The PKI was started because the development of middleware infrastructure created an obvious need to secure and protect the integrity of communication between middleware components and applications. There was the option of using certificates from commercial suppliers. Although these could provide satisfying levels of assurance, the commercial suppliers were not seen to be fully committed to following open standards in their certificates. The prospect of making core middleware communications dependent on proprietary standards was not appealing. Since the costs for starting and maintaining an independent PKI were estimated to not be too overwhelming, SWUPKI was created.

Members run their own CAs under a common policy

SWUPKI operate under a common policy, a common policy CA (Certificate Authority) and policy management authority. The members run their own subsidiary CAs. By running the CAs under the common organisational framework for SWUPKI, we have an infrastructure for protecting the integrity of transactions between the members. The common PKI also allow us to concentrate the knowledge on the use and development of PKI technology at the root level.

Personal certificates around the corner

SWUPKI has so far only issued server certificates, but we are planning to expand the service to include personal certificates. As networked applications become ever more business critical, we want to strengthen the methods of asserting the identities of users. Therefore we want to start to implement authentication with personal certificates and smart cards within the next couple of years.

SWAMID – The identity federation for the Swedish higher education community

SWAMID is SWAMIs identity federation. Our goal with SWAMID is that it shall be the only identity federation needed in the Swedish higher education community for the foreseeable future. SWAMID therefore provides a common infrastructure for federated services with several federation technologies. Initially the identity federation will support CWAA, eduroam and Shibboleth (or SAML). Depending on the demand in the community, more federation technologies will be added to SWAMID.

An organisational framework to build trust between members

An identity federation is an organisational framework designed to make it possible for each of the member organisations to use their own enterprise directory and authentication mechanism for authentication (and possibly attribute release) to services provided by other members of the federation. The organisational framework is based on a policy that determines the principles for the governance of the federation as well as the rules and procedures for membership. The members sign an agreement to comply with the rules and obligations in the policy. The object of the organisational framework is partly to build trust between the members, concerning the practices for authentication and identity management. The object is also to agree on practical matters.

The multitech approach

The norm for identity federations has so far been: one federation for one federation technology. We have chosen a different concept for SWAMID. By including several identity federation technologies under one common organisational framework, we believe we will achieve economies of scale with regards to the number of identity federation technologies provided to the user community. We expect the costs for the central administration of SWAMID to be lower than they would be for several parallel identity federations. We also expect the common identity federation framework to reduce the membership and identity administration costs at the member level.

In our view, the work of organising and maintaining an identity federation is largely independent of the particular federation technologies. For example, one has to decide on procedures for membership applications and so forth. These routines can largely be the same for several federation technologies. Further, the identity management of the identity providers in a federation should meet a common standard. The rules concerning identity management for identity providers in a federation are not necessarily dependent on the federation technology.

To accommodate several federation technologies in SWAMID we have adopted a strategy with one common policy and several technology specific addenda. The common policy mainly focuses on the rules concerning identity management, the governance of the identity federation and routines and procedures concerning membership. The addenda contain technology specific rules. This forms a layered structure of agreements, so it will be possible to join for example the eduroam part of the federation without joining the Shibboleth federation.

The common policy will not restrict membership in SWAMID to organisations in the higher education community. Any organisation that meets the conditions of the common policy and the conditions of at least one addendum can join the SWAMID. The addenda can restrict membership eligibility to certain types of organisations, which for ex. is the case in the eduroam addendum. See http://www.swamid.se for more information.

eduroam in Sweden – Status September 2006

We are in the process of deploying eduroam in Sweden. eduroam is the wireless roaming technology developed cooperatively by some of the european national research networks. It is included in SWAMIs wider federation framework - SWAMID. In May SWAMI and SUNET organised a workshop for those interested in joining eduroam. This well attended event reassured us of the interest in eduroam in the Swedish higher education community.

The national organisation is in place

The work with the organisational framework for SWAMID in general and eduroam in particular, is mostly done. The necessary policy that includes the procedure for membership has been written. We have set up the national radius server for eduroam and are establishing an operational team.

Work to be done for prospective members

The remaining work will mostly be at the level of prospective members. The prospective members have to harmonise their identity management with the SWAMID and eduroam policies. The other main task involved in joining eduroam is to implement a Radius service.

The prospective members themselves can decide which eduroam compliant radius implementation they wish to use. Compared to setting up a Radius service the issue of identity management is in all respects a more complex issue. For the universities that have already deployed, and properly manage, central user accounts it will in most cases not be very demanding to harmonise their practices with the policy for eduroam. For others the deployment hurdle to join eduroam will be higher, since they have to start by introducing central user accounts. SWAMI intends to offer support for the introduction of central identity management. The 20 October another practical eduroam workshop will be organised.

eduroam might become the solution for network logon

The universities joining eduroam have in many cases deployed solutions for authenticating their own users for network access at their own campuses. Joining eduroam means one has to implement an additional solution for network access. When eduroam is fully deployed we believe that many universities will choose to discard their preexisting network logon solutions.

Text: Simon Wiberg