Lowering costs of identity proofing by federated identity management

Kristina Leve[1], Valter Nordh[2]

[1] VHS, Box 24070, SE-10450 Stockholm, Sweden, kristina.leve@vhs.se. [2] SWAMI, www.swami.se, Sweden, valter.nordh@gu.se

Keywords
Federated identity management, identity proofing, SAML, Shibboleth, SWAMI

1. EXECUTIVE SUMMARY

Identity proofing is the process of verifying that an electronic user account belongs to a person who really is who she says she is. If you add up the costs of identity proofing for all Swedish universities you will get a considerable cost. Identity proofing is also demanding and time consuming for the students.

1.1. Background

Admission for higher education is nationally coordinated in Sweden. Students apply for higher education courses and programmes at the website studera.nu. At studera.nu the student needs a verified account to see her own credentials and to accept course offers. The identity proofing at studera.nu is done by letting the student enter a PIN-code that has been sent to her national registration address.

1.2. Federated identity management

For some time now, students can log on to studera.nu by using their verified university account. The next step is to let students create verified accounts at their new university, by using their verified studera.nu account. This will be implemented by using the standards-based, open source software Shibboleth within the SWAMID identity federation. At the same time, universities will act as identity providers for each other.

2. Background

2.1. NyA – National admission system

Admission for higher education is nationally coordinated in Sweden. An admission system (NyA) is shared between practically all universities and university colleges.

2.2. studera.nu – National admission website

NyA's student interface is a website (www.studera.nu) where students can search among all the Swedish higher education courses and programmes, submit applications, follow the admission process and accept course offers. It is also possible to apply by sending in a paper application, but 95 % of the applicants apply by the website.

2.3. VHS

The development and maintenance of NyA and studera.nu are managed by the National Agency for Services to Universities and University Colleges (VHS).

2.4. SWAMI

Swedish Alliance for Middleware Infrastructure, SWAMI (www.swami.se), is the virtual organization, with 14 members from the Swedish higher education community, for middleware cooperation in the Swedish higher education community. The commissioning agent of SWAMI is the Swedish national research network SUNET (www.sunet.se). SWAMI is primarily financed by SUNET but every member is providing a small amount of financing (universities 10 000 EUR/year and university colleges 5 000 EUR/year).

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

3. Identity proofing

Identity proofing is the process of verifying that an electronic user account belongs to a person who really is who she says she is. There are different methods of identity proofing and they provide different levels of assurance of the user's real identity. In this paper, a verified account means an account that belongs to a person whose identity has been proved with at least a fair level of assurance. All Swedish citizens have a civic registration number (social security number) as a unique identifier.

At studera.nu the student needs a verified account to see her own qualifications/credentials and to accept course offers. The identity proofing at studera.nu is done by letting the student enter a PIN-code that has been sent to her national registration address.

At the university, the student needs a verified student account. The identity proofing process differs between universities, but can for example be done by the student entering a PIN-code that has been sent to her national registration address or by the student showing her ID card at the university.

Obviously, there are costs connected to the activities of identity proofing, of which the following are some examples:

- About 280 000 PIN-codes are sent per year from VHS / studera.nu, to a cost of about 0.70 EUR per PIN-code. The national admission contact center receives about 20-30 000 e-mails and phone calls per year regarding accounts and PIN-codes, to a cost of about 1.70 EUR per issue.
- At Stockholm University the students receive their account after showing their ID at the student helpdesk. The helpdesk handles 10-15 000 users per year, to an estimated cost of 30-50 EUR per user and year.

- At Uppsala University, the student verifies her identity by entering a PIN-code that has been sent to her national registration address. 10-15 000 PIN-codes are sent by mail each year, to a total cost of about 15 000 EUR per year, and with additional costs of helpdesk etc.

If you add up the costs of identity proofing for all Swedish universities you will get a considerable cost. Identity proofing is also demanding and time consuming for the students.

4. Federated identity management

To reduce the costs and hassle of identity proofing, it is worth striving for having only to verify a student's identity once, either at studera.nu or at *one* of the universities she attends. This can be achieved if organisations in the higher education community join an identity federation, and acts as identity providers for each other.

The concept of federated identity management is to share digital identities with trusted partners. It allows users to use the same username, password or other ID to gain access to affiliated but separate websites or networks within the federation. The term identity provider refers to the organisation (or actually software running at the organisation) that has users wishing to access a restricted service. The organisation (or actually software running at the organisation) that provides a restricted service is called a service provider.

Applied to the identity proofing problem, the idea is to give a student with a verified account at identity provider A, a new, verified account at service provider B. The student logs on to B via the existing account at A, and the student is then sent back to B together with her civic registration number (social security number). B can then establish a new, verified account for the student. The student can start using the restricted services of B immediately, for example register at a course. The next time the student logs on, she logs on directly to her new account at B. Both A and B can be either a university or the national admission website studera.nu.

Partially, this has been possible for over a year now. Students can log on to studera.nu by using their verified university account. This is implemented with a framework called CWAA, a technology developed by SWAMI. About 57 % of the Swedish users at studera.nu log on via their university.

The next step is to let students create verified accounts at their new university by using their verified studera.nu account. This will be implemented by using the standards-based, open source software Shibboleth within the SWAMID (SWAMI Identity Federation) identity federation. One pilot university will offer its students Shibboleth login via studera.nu from June 2008. From January 2009, all universities will be given the possibility to use studera.nu as an identity provider. Parallel to this, an ongoing effort is made within SWAMID, to make the universities act as identity providers for each other.

4.1. SWAMID / SAML

SWAMI Identity Federation, SWAMID (www.swamid.se) is the identity federation for the Swedish higher education community and is governed by SWAMI. The most common way to implement federations in higher education is to have multiple technology federations but SWAMID has the unusual approach with an identity federation together with multiple technology addendums, or technology federations.

The purpose of SWAMID is to make it possible for service providers to provide services to end users in the federation. This is accomplished by making infrastructures for federated identification and authentication available to the higher education and research community in Sweden and by inviting its service providers to become members of the federation.

Identity management is the process by which identity providers make claims of identity for subjects (e.g. individuals, resources and other objects). A claim of identity is an electronic representation, using a specific identity management technology, of a set of attributes identifying a subject. Each federation technology used in SWAMID employs a separate implementation of the principle of federated identification of subjects. Hence the common set of procedures and practices described in the federation policy applies equally to all federation technologies, regardless of the means by which identification and attribute release is implemented.

A SWAMID federation technology offers authentication service for entities and may offer release of attributes containing unique assertions of identity. It is expected that in order to support authentication, SWAMID Federation Members must implement identity management solutions which are able to support a wide range of federation technologies. At present there are two federation technologies, SAML2 and eduroam (www.eduroam.se), that is used in SWAMID. The use case with studera.nu that is described in this paper uses the SAML2 federation with a Shibboleth scope extension.

4.2. What's next?

Within a couple of years, studera.nu will phase out CWAA and replace it with SAML/Shibboleth. Shibboleth is standards-based and continuously developed, while CWAA is "deprecated" and will eventually no longer be supported by SWAMI.

National electronic citizen ID (eID) is an interesting alternative to PIN-codes and ID card-checks, as a means of identity proofing. The usage of eIDs in Sweden is far higher than elsewhere. The implementation of eID at studera.nu will be evaluated in the near future. Issues to consider are the costs of being the first eID service for many people (few services are aimed at 19 year olds today) and the development of the eID technology (there are indications of cheaper eID implementations in the future).

On a more visionary level, European confederations (federations of identity federations) could be the basis for new services to students and help facilitate student mobility. A discussion on this topic at the EUNIS conference would be very interesting.

5. REFERENCES

Forrester website (2008). *Government eID Projects Need Private Sector Initiative And Support For Broader Success*. Retrieved May 15, 2008, from: http://www.forrester.com/Research/Document/Excerpt/0,7211,45644,00.html.

Internet2 Shibboleth website (2008). *Shibboleth*. Retrieved May 15, 2008, from: http://shibboleth.internet2.edu/.

SWAMI website (2008). *SWAMI*. Retrieved May 15, 2008, from: http://www.swami.se

SWAMID website (2008). *SWAMID*. Retrieved May 15, 2008, from: http://www.swamid.se