The Kalmar eIdentity Union: Facilitating Common eServices in Norden

Mikael Linden, CSC, c/o TTY, PL 692, 33101 Tampere,
Ingrid Melve, UNINETT, Abels gata 5, Teknobyen, N-7465 Trondheim
David Simonsen, WAYF, H.C. Andersens Boulevard 2, 1553 Copenhagen
Torbjörn Wiberg, IT Office, Umeå Universitet, SE 90187 Umeå, Sweden,

Keywords
Identity Federation, Identity Confederation, Identity Management, SAML2, Federation Enabled eServices, Federated eServices

1. EXECUTIVE SUMMERY

The Kalmar e-identity Union builds an infrastructure for exchanging personal information across borders within higher education and research. The goal is to provide users with more and better (electronic) services in order to enhance both education and research within the union. The first Kalmar Union (which lasted 1397-1524) was purely Nordic. This time the starting point (Finland, Norway, Denmark and Sweden) is the same - but not constrained to these four members.

The building blocks of the union are the existing national e-identity federations. The minimal requirements for entering the federations are such that service providers and identity providers (typically institutions) can safely trust the exchanged information about the users, even across bordes.

The technical basis for Kalmar is the SAML2-protocol, building a mesh of service providers and identity providers. Information about these and how to connect is already kept in lists named 'federation metadata' by the national federations. A central task for the Kalmar-group to solve is how to aggregate and manipulate a common set of metadata from distributed sources (federations).

The establishment of the union is funded by NordForsk.

2. INTRODUCTION AND SUMMARY

eID-federations all have a simple goal in common: to provide better and more services to the users. In the countries in Norden, Identity Federations have been set up to serve the academic communities. They make it possible and often even simple
- to introduce single sign-on over the federation for web applications and
- to, in principle, give any user in the federation access to any IT service in the federation.

The basic requirement on an institution for becoming a member of one of these federations is to show that the quality of the identity management process is acceptable. Once an institution has become a member of a federation it is simple and affordable to introduce a new application where every user in the federation is a potential user – the identities are already issued and managed. It is equally simple to offer a shared eScience resource to the same community.

The federations are national, but this promising approach shall of course not be hindered by federation borders but should be used at the next level as well: across borders. This is why the Kalmar (eIdentity) Union is now being set up. The aim is to use and extend the national eID-federations into a new pan-Nordic infrastructure for authentication, attribute release and authorisation of end users. The scope is research and higher education.

Within the Kalmar Union end users in one Nordic country is able to use his/her home institution's username and password to access IT systems, such as research facilities, in other countries within the union. This is made possible by making contractual and technical arrangements between the national federations.

The first Kalmar Union lasted from 1397 to 1524. It consisted of Norway, Sweden (Finland included) and Denmark. The Kalmar Union treaty defined the framework for the economical, political and military cooperation during this period. The second Kalmar Union has more humble goals – it aims at making the usernames, passwords and other eIdentity credentials valid all over the Information System landscape of the union. The technical architecture of the coming Kalmar e-identity Union, initiated by the academic identity federations in Finland, Norway, Sweden and Denmark, was first presented at the NORDUnet conference in September 2006.

The development and deployment of the second Kalmar Union – the Kalmar eIdentity Union – is run as a project during 2008 that is financed by NORDFORSK. The members of the project are the Identity federations HAKA in Finland, Feide in Norway, WAYF in Denmark and SWAMID in Sweden. The plan is that the Kalmar eIdentity Union shall be operational before the end of 2008.

In the next two sections, we note that since the federations are in place, with all services and resources to be shared, one could be fooled into believing that most of the work has been done to se up a union. And it is both rue and false. The task left is to make the federations interoperate. The concept of a federation technology includes some formal way of specifying the metadata of the federation, specifying things like the characteristics of the different services etc. Although it might be true to say that most of the work needed is already done when deploying the national federations, there are lots of interesting decisions involved on the union level. The final section of this paper discusses this and presents the choices we have made so far in the Kalmar Union project.

3. The federations provide the basis for cooperation

The members of an identity federation are organisations that has come together to exchange information about their users in order to be able to share services and in order to simplify collaborations and transactions between the respective member organisations. The goal is to create a structure that makes it possible for a user to get access to a resource in the federation by using the same credentials as she uses in her home organisation. To achieve this sharing of information and services the members are required to provide an Identity Infrastructure for their communities. An Identity Infrastructure, where eIdentities are issued and managed, and that contains an Authentication Service that can verify that a user has at its disposition the necessary credentials associated with the claimed eIdentity.

The setup of the federation further involves choosing one common federation technology, which defines in detail how requests for services and their replies are formulated and packaged. Finally the members have to formally agree on several policy issues including how users are identified and how identities are managed.

All of this basic work has been done by the federations in the respective countries. They may though have chosen different federation technologies, and they most certainly have different policy agreements. How do we proceed to establish the Kalmar union from that point?

The services to be shared – such as various research and collaboration tools, which expect users to authenticate, including grids and support tools for virtual organisations – are mostly already available at the federation level. So what do we have to do to for example make them available to projects with members in several federations – to make them available all over the union.

4. The union as the bridge between federations

The second Kalmar Union can be seen as the next step in a natural development of integrating digital services for researchers: computer networks have been developed and connected internationally over the past 25 years - now the time has come for services and digital identities. But policies, agreement, data semantics etc. have to be defined and this is the true task of establishing the union - all systems deployed in Kalmar will share the same technical interface and the major question is how to implement it in this new configuration with the constraints on the management of electronic identities, that the Kalmar e-identity Union Charter requires.

Currently, the identity federations in Nordic countries are national. The early Kalmar trials demonstrated the feasibility of crossfederating several national identity federations, but were only the first, and arguably easiest, step towards the ambitious goal: establishment of a formalised, international cooperation around services and electronic identities between the national identity federations.

In the middleage, politics was at the heart of the union - and so it remains today: cooperation between Nordic researchers is politically seen as a necessity to keep up with the international competition in higher education and research.

National identity federations pave the way for sharing of resources, and thereby also division of labour, and having better and more useful electronic identities. As the identity federations have already proved useful it only seems natural to extend the cooperation to the international level. The sharing of electronic resources of many kinds across both institutions and national borders will make cooperation between researchers easier and thereby strengthen the Nordic research community. Already the Nordic Master School is planning to build courses on the Kalmar union providing Finish eScience resources to Danish students.

Please note that the Kalmar Union is not (this time) necessarily a priori confined to be 'Nordic'.

5. Different federation architechtures meet on common ground (SAML2)

The flow of information about the individual users differs in the Nordic eIDfederations. Norway and Denmark have established centralized structures, where all user information is passed through a single 'identity hub' or 'identity provider' (IdP) (see figure 1). This implies that services always recieve user-information from the same logical point which in turn may be connected to multiple data sources (institutions). This way services reach a broad user base through a single technical connection - and vice verca: the users of an institution may reach multiple services though a similar technical connection. In Figure 1 the data flow goes from the institutions, over the IdP to the services. The central IdP may manipulate the data flow on behalf of the connected institutions if needed. Agreements between services and institutions may be needed i.e. for services which involves accounting.

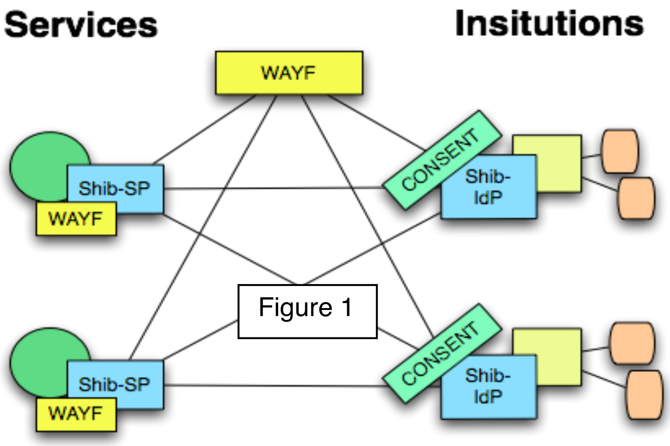

Figure 1

Finland and Sweden have established decentral eIDfederations in which all service providers must recieve user information from the institutions directly, see Figure 2. The architechture therefore is a true many-to-many relation, which is only indirectly true in the case of Figure 1. When redirecting users to login at the institutions, services may keep track of their business relations setting up their own Where Are You From (WAYF)-service - or they might point to the federations' central WAYF-service which keeps a list of all member institutions. Also in Figure 2 the data flow goes from right to left. Any required manipulation of the passed data must be done at each institution (IdP).

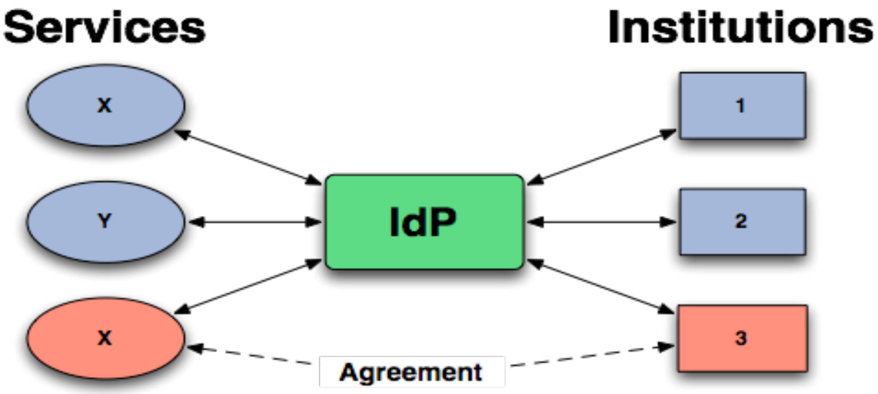

Figure 2

The technical definition of the eIDfederations, regardless of which of the above architechtures is used, is a simple list (xml) describing all federation members (service providers and identity providers). The list is cryptographically signed by the federation's authority and can therefore also be trusted. It may (not) be publicly available but should not contain sensitive data. The list consists of a structured set of identifyers, descriptions, members' cryptographic keys, attribute release policies for services etc. - everything needed in order to contact either a service provider or an IdP (central or decentral).

Many good systems and protocols could be used to support the task - but all seem to converge towards a single dominant standard: Security Assertion Markup Language version 2 (SAML2). It therefore seems obvious to choose SAML2 as the 'lingua franca' in the Kalmar eIdentity union even though not all Nordic federations support SAML2 at the time of writing. All other options would be more complex and not scale in the longer run, and they would be incompatible with many related government projects which have chosen SAML2 based solutions.

Having a common language to describe the national federations also makes it possible to merge metadata and thereby make services from one federation available in other federations - which is exactly what Kalmar intent to do. This is possible if, and only if the formal policies are aligned with regard to the various minimal requirements for entering the national federations. If not - the trust will not extend to the federations with the lower bar. To distribute the metadata (automatically) between several federations has not been tried before and is therefore and area of investigation before the Kalmar Union will become reality.

Acknowledgement
This work would not have been possible without the generous financial support from NordForsk – an independent Nordic research institution under the Nordic Council of Ministers for Education and Research. See http://www.nordforsk.org/ for more information