# KALMAR UNION, A CONFEDERATION OF NORDIC IDENTITY FEDERATIONS

**Mikael Linden**
CSC - IT Center for Science Ltd, P.O. Box 405, FI-02101 Espoo, Finland
mikael.linden@csc.fi

**David Simonsen**
WAYF-DK - Where Are You From, The Agency for Libraries and Media, H.C. Andersens Boulevard 2, DK-1553 Copenhagen V, Denmark
david@wayf.dk

**Andreas Åkre Solberg**
UNINETT, NO-7465 Trondheim, Norway
andreas.solberg@uninett.no

**Ingrid Melve**
UNINETT, NO-7465 Trondheim, Norway
ingrid.melve@uninett.no

**Walter M. Tveter**
Center for Information Technology, University of Oslo, Oslo, Norway
w.m.tveter@usit.uio.no

## Abstract

This paper reports on Kalmar Union[1], the first effort to cross-link national identity federations for research and education. So far, the participants in the confederation are the academic identity federations in the five Nordic countries: Finland, Norway, Denmark, Sweden and Iceland. Users are able to reuse their login credentials when accessing services across the Nordic countries. Services will more easily be able to expand in the Nordic region and institutions will be able to provide more and better services to their users.

In the Kalmar Union project, policy development was chosen as the task to start with. The focus was on simplicity of entering the confederation, risk adjustment and minimum requirements for identity management and privacy protection. The legal shape of the confederation and its reasoning is presented in this paper.

The technical architecture of Kalmar Union allows interconnecting full mesh Shibboleth federations (Finland, Sweden) with hub-and-spoke federations (Norway, Denmark and Iceland). A simplified profile of SAML 2.0 is used end-to-end, eliminating the need for protocol translating border elements. Systems for automatic aggregation of SAML 2.0 metadata and a new discovery service have been developed. This paper presents also issues for future work, including attribute harmonisation, campus identity management, user experience, SAML 2.0 profile deployment and the federation business models.

The cross-Nordic trust fabric is now strong enough to enable service sharing, as will be shown by the use scenarios. The Kalmar community wishes to contribute to the best practice in the field of identity federation and confederation.

## Keywords

federated identity management, identity federation, confederation, SAML 2.0

[1] http://www.kalmar2.org/

# 1. Introduction and Previous Research

During the last few years, identity federations have been deployed in higher education. An identity federation is an association of organisations that come together to exchange information, as appropriate, about their users and resources in order to enable collaborations and transactions [1]. A federation chooses one or more federated identity management (FIM) protocols, such as Shibboleth or SAML 2.0, and the participants in the federation set up Identity and Service Providers, which are responsible for identification, authentication and authorisation of end users in the federation.

Currently, 17 federations have been identified in higher education around the world [2], many of them already presented to the community [3,4,5,6]. All the federations have had a national scope, and usually they are built around the national education and research network (NREN). However, research and education is inherently global, and needs for a federation of national federations have risen. eduroam confederation [7] is a prominent deployment of policies [8] and technologies [9] bridging national eduroam federations, but scoped only for roaming network access. eduGAIN architecture [10] implemented in GN2/JRA5 project aims at introducing a similar architecture for application access, but covers only the technical parts of a confederation, leaving the policy issues intact. The International Grid Trust Federation (IGTF)[11] has bridged together various grid PKIs in the world, but focuses to the relatively dedicated grid community, whereas ordinary end users have considered the concept of a certificate too difficult [12,13,14:56].

The Nordic countries have a long common history also within academic networking. Since November 1988 [15:62], Nordunet has connected the NRENs in Denmark, Norway, Sweden, Finland and Iceland to the Internet. The Nordic countries also have operational identity federations; FEIDE in Norway, SWAMID in Sweden, Haka in Finland and WAYF in Denmark and Iceland. From the beginning, there has been active co-operation between the federations [16], and the first technical demo of an interconnection was presented in the 23rd Nordunet Networking Conference in 2006 [17]. However, an operational confederation service needs also policies governing the participating federations. A study on related policy issues (such as organisational model, consent, terms of service, liability, subjects and roles in the federation) were presented in TNC2007 [18]. Funded by NordForsk, the second Kalmar Union[2] has been established in 2008, covering both the policy and technical issues of the confederation.

NordForsk is a Nordic research board operating under the Nordic Council of Ministers for Education and Research, responsible for Nordic collaboration in research and research training. The objective for NordForsk’s coordinating activities is to develop the Nordic Research and Innovation Area as a globally leading and attractive region for research and innovation. NordForsk identified an infrastructure for cross-national access control on research and education resources as a tool that supports this goal.

The Nordic Passport Union, established in the 1950s and still in effect alongside the Schengen collaboration, can be seen as a role model for Kalmar Union. The citizens are able to freely cross the Nordic borders without carrying their passports if they can otherwise prove to have Nordic identities. Kalmar Union is moving this collaboration into the digital reality, enabling general trust in users' Nordic electronic identities.

This paper presents the policy and technical foundations of Kalmar Union. The second chapter presents the use scenarios for the confederation. The third chapter explains the confederation's juridical setup and policy. Chapter four presents the technical architecture of the union. Chapter five presents future work items and suggestions for future confederation projects. Chapter six concludes the paper.

# 2. Kalmar Union Use Scenarios

While discussions about how to initiate the Nordic collaboration were ongoing both policywise and technically, several use cases surfaced, four of which are shortly introduced next. They document the need for cross-national trust in digital identities as a natural requirement for extending existing collaboration as well as opening new opportunities.

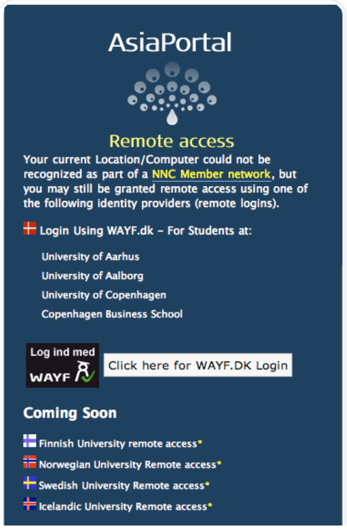
## 2.1. Research Collaboration

Research is often done in international collaboration. The Nordic funding programs also encourage multi-national research projects. In this light it seems obvious to build infrastructures to support these collaborations.

An example of research collaboration is a common effort to pool and share resources for a relatively small area of research: Asian studies. An important task for Nordic Institute for Asian Studies (NIAS) [19] is to provide access to

[2] The first Kalmar Union united the Nordic countries under a single monarchy in 1397–1523.

databases covering Asian politics, literature, news, science, etc. Access control is today based on updated lists of authorised IP-address space, which is still the most used method in the publishing business.



AsiaPortal

Remote access

Your current Location/Computer could not be recognized as part of a NNC Member network, but you may still be granted remote access using one of the following identity providers (remote logins).

Login Using WAYF.dk – For Students at:

University of Aarhus
University of Aalborg
University of Copenhagen
Copenhagen Business School

Click here for WAYF.DK Login

Coming Soon

Finnish University remote access*
Norwegian University Remote access*
Swedish University Remote access*
Icelandic University Remote access*

Figure 1. NIAS has high expectations for Kalmar Union.

To lower the administrative burden, role based access management is preferred and it is exactly what Kalmar Union is paving the way for. Furthermore, NIAS expects guest researchers and exchange students to use their existing usernames and passwords at their home institutions instead of having local accounts created at NIAS.

## 2.2. Research Infrastructure

Setting up and maintaining infrastructure for researchers is expensive. This covers, for instance, tools, systems, software and other equipment that are needed to carry out the studies. If infrastructure costs can be cut the savings can then be reallocated to the research work itself. One way of cutting costs is economics of scale; an investment to research infrastructure can be made available to larger and larger number of researchers even from several countries.

An example of a research infrastructure is SLCS (Short-Lived Credential Service) [20], a service that makes use of federated identity management to provide short-lived certificates to grid users. A researcher uses his or her home institution's username and password to authenticate to a federated service which issues him or her a grid certificate. The service went into production in Switzerland in 2007 and since then several SLCS services have been set up around the world.

It is possible to set up a SLCS service in each Nordic country and register it to the national identity federation. However, the grid community has found that one SLCS installation could easily cover all the Nordic countries. Because of Kalmar Union, one Nordic SLCS service could be done available for all Nordic researchers with their home organisations' usernames and passwords.

## 2.3. Learning Collaboration

Institutions are now teaming up in special interest groups in order to provide better educational programs. The groups are all the more often crossing also national borders.

For example, the Nordic Master School in Innovative ICT [21] is a network of international ICT master programmes at five scientific universities in the Nordic countries: University of Turku, Åbo Akademi University and Turku School of Economics in Finland, Royal Institute of Technology in Sweden and Technical University of Denmark. Students are able to 'shop' courses across all participating universities and student exchange is made easy.

The use of learning management systems is a natural part of the educational programs and the reuse of the users' familiar authentication mechanisms at their home institutions is a high priority. Kalmar Union helps to simplify the administrative workflow when receiving exchange students - and hereby facilitates ease of movement and course-shopping.

### 2.4. Licensed Contents

Institutions are buying an increasing number of commercial services in order to keep up with the raising demand for support of the daily digital life of students and employees. Users already use services from abroad like Gmail, Twitter, Skype etc. It is essential to be able to sign up also for services provided both in the same country the institution resides in as well as services abroad.

Ordbogen.com [22] is a relatively new company providing online access to dictionaries. In a few years, they have managed to fill in a large part of the Danish market in the sectors for higher education, public agencies, ministries etc. Both Nordic and European expansion is planned. Ordbogen.com is presently migrating to role based access management based on the Danish WAYF federation and sees Kalmar Union as a crucial step for entering the Nordic market. Conversely, institutions in other countries will soon be able to sign up for the electronic dictionaries provided by Ordbogen.com - if quality, price, access management and so forth can compete with existing offers.

## 3. The Legal Shape and Policy of the Confederation

The legal principles of Kalmar Union were laid down in 2007 and presented in TNC2007 [18]. This chapter presents how the principles are put into practice in the Memorandum of Understanding and Charter of Kalmar Union, which forms the policy of the confederation.

### 3.1. Trust Fabric

Kalmar Union is built with a loose legal fabric. In general, each participating federation keeps its own policies. However, a common denominator is agreed on for issues related to privacy and liability and operational issues such as problem management and incident handling.

Each participating federation signs the Memorandum of Understanding and Charter [23] of the confederation. This method of establishing the confederation has been selected to represent a low threshold of legal commitment for the involved parties, which makes entering and leaving the confederation easy. This has been done for three reasons.

First of all, we wanted an organisational model that would allow the national federation to easily enter into Kalmar Union on behalf of their national member organisations. Instead of all Nordic higher education and research institutes, only the five national federations signed the Memorandum of Understanding and Charter. Doing this we could limit negotiations to a handful of entities.

Secondly, we did not wish to go for a full binding and formal legal structure with lots of obligations between the parties. Instead, the confederation is formed by signing a Memorandum of Understanding and Charter. This was because even with the limited number of participating entities a binding contract would have been difficult to accomplish within the given timeframe, if at all. The few questions that had to be hashed out between the parties, when they started involving the respective lawyers, showed with no uncertainty that a complex and untested effort like Kalmar would present an almost unending amount of uncertainties if one were to explore every possibility.

Thirdly, and perhaps most significantly, this was an assessment of risk. On the top level, there are two risk factors that stand out. The first one is what the national federations and their member institutions risk by collaborating in this manner. The other is, given our assessment that a full binding and formal legal structure was not possible, what they risk by not attempting this collaboration. The second seems to outweigh the first. By taking the risk that Kalmar union legal structure is not full binding, the national federations enable new ways of cross-national collaboration whose benefits outweight the risks.

The way we have built Kalmar Union is not necessarily a possibility for all such federations, because it needs both a certain trust and a certain willingness to take a risk from the involved parties. In the Nordic region, these two factors exist. This is partly because of the stability the region has enjoyed since the Second World War and partly because of the solid foundation of Nordic cooperation that exists in a number of areas and that has been in existence since the Nordic countries became modern nations.

From the national federations' and their member institutions' point of view, attempting Kalmar Union is therefore possible without much ado. That leaves protecting the interest of the end users and the Service Providers. This is mainly a question of privacy and security, both of which have a strong focus in the Memorandum of Understanding and Charter. Especially, the ability of end users to access the services through properly informed consent is a key element here. By comparing and making compatible the different national federation’s infrastructure and policies we hope to develop new best practices in these areas.

The goal of Kalmar Union was to get the confederation up and working. Achieving this means not only getting users to access cross-federation services (thus also getting services to open up for users) but to build the trust fabric from the voluntary participation in such a venture. In the future projects, other organisational models may be chosen. On the other hand, if the trust fabric that is woven by Kalmar Union is strong enough, other organisational models may not be needed, except for scalability issues.

## 3.2. Campus Identity Management

A common denominator for the Nordic academic identity federations is respect for a high quality of identity management in the home organisations. The national federations' policies impose minimum requirements for end user's identities; how initial proof of identity is done and how the freshness of identity data is ensured as the end users' roles in their home organisations change over time.

As campus identity management in the participating federations was considered important in Kalmar Union, related requirements were placed in the Memorandum of Understanding and Charter of the confederation. Information about the requirements for the campus identity management procedures is provided by each participating federation, and must be available in English. When a new national federation joins the confederation, the current members must accept the new member unanimously. This covers studying the new member's policy on campus identity management, as well.

Recently, a lot of discussion has taken place on the Level of Assurance for authentication and identity data. Several frameworks for assessing the Level of Assurance have been proposed, such as NIST SP 800-63 [24] and IDABC eID Interoperability [25]. In Kalmar Union, there is currently only one basic level of assurance for identity, authentication or attributes, and the participating federations have been willing to accept each other's basic assurance level.

## 3.3. Privacy Policy and Consent Management

According to the EU data protection directive, processing personal data is based either on an end user's consent or a necessity [26]. In many cases, processing end user's personal data in a Service Provider may be based on necessity, but to ensure being always in the safe side, many federations have deployed a practice where the end user must always consent to the attribute release to a new Service Provider. Typically, it is the Identity Provider that asks for the end user's consent before releasing his or her personal data to the Service Provider.

In Kalmar Union, consent management at the Identity Provider is handled within each federation. WAYF and FEIDE have central consent management services, as well as integration of consent into the first login with a Service Provider. Haka presents this information to the end users at each Identity Provider. The important factor for the cross-federation is that informed consent is available for the whole user population, even if user interfaces and implementations vary.

Furthermore, according to the European data protection legislation, the consent must be informed. The data subject must be informed on how and for which purposes his or her personal data is processed. Services providing access across national borders have stronger requirements for consent and consent management than services within a country, or indeed within a single security domain. In order to give informed consent, the user must be informed about what he is consenting to. On the Internet, a convenient way for doing this is providing the end user the privacy policy of the service.

A link to the privacy policy can be available for the end user in the service before she or he logs in, so that he or she is able to read it before the service starts to process his or her personal data. In the participating federations, Haka federation has taken one step further to enforce the practice and considers the privacy policy URL as part of the federation metadata. When a new service is registered to the federation, the Service Provider needs to register the privacy policy URL to the federation operator. The Identity Providers, in turn, must provide an end user the opportunity to click the Service Provider's privacy policy URL when consenting to the attribute release.

## 3.4. User experience

From an end user perspective, Kalmar Union does not introduce anything fundamental. In Kalmar Union, the end user is redirected to his or her home organisation's Identity Provider for login, and he or she sees the familiar user interfaces for login, logout, consent and privacy information.

The Discovery Service function, redirecting the end user to his or her own home organisation for login, is the only new element seen from the end user. The first time an end user logs in to a Kalmar Union Service Provider, there is a choice presented with various home organisations, including pointers to the foreign home organisations (or federations). Background technical interaction with the Discovery Service ensures that this information is minimised. A Discovery Service could show the local Identity Providers and the national flag from the foreign Identity Providers. An example of the Service Provider side Discovery Service is shown in the use case from the Nordic Institute for Asian Studies (Figure 1).

# 4. Technical

Complementary to the policy, this section presents the confederation's technical architecture and its reasoning.

## 4.1. Architecture

The eduGAIN architecture [10] designed by the Joint Research Activity 5 of the GEANT2 project (GN2/JRA5) has been so far the most notable confederation architecture in higher education. In short, eduGAIN architecture introduces protocol gateways, at least one in each participating federation, which is an element bridging the federation to the others in the confederation. The bridging element makes necessary protocol and attribute conversions and is a trusted entity for both the Identity and Service Providers in the transaction. Similar architectures have been presented in the telecommunications industry [27] and in the European public administration [28].

Unlike the eduGAIN architecture, Kalmar Union does not utilise any bridging elements or other protocol gateways. Instead, Kalmar makes the Identity and Service Providers communicate directly with each other, using the SAML 2.0 protocol end-to-end.

The federations connected in Kalmar are based on three different architectures. Haka is a classic Shibboleth full mesh, FEIDE has a centralised structure with one Identity Provider (with multiple Authentication Points) and WAYF follows a hybrid model with some central functionality and local Identity Providers. The Kalmar Union architecture accommodates various federation architectures, as long as the protocol support is available in the participating federations.

In Kalmar Union project, bridging elements were considered as unnecessary gateways. As a generic rule of thumb, protocol gateways never enhance the quality of the communication but merely loose information in translation. Furthermore, they become single points of failure, which everyone needs to trust. They are also suspicious from the privacy perspective, because they see all end user's attributes and are able to monitor all the Service Providers to which an end user signs in.

As a result of the general convergence towards SAML 2.0 protocol, in Kalmar Union, the protocol gateways were dropped and SAML 2.0 used end-to-end, instead. The Kalmar Union environment consists of a full mesh of all the Identity and Service Providers that each participating federation shares in Kalmar Union (Figure 2). All the participating Service Providers are visible to all the Identity Providers in the confederation.

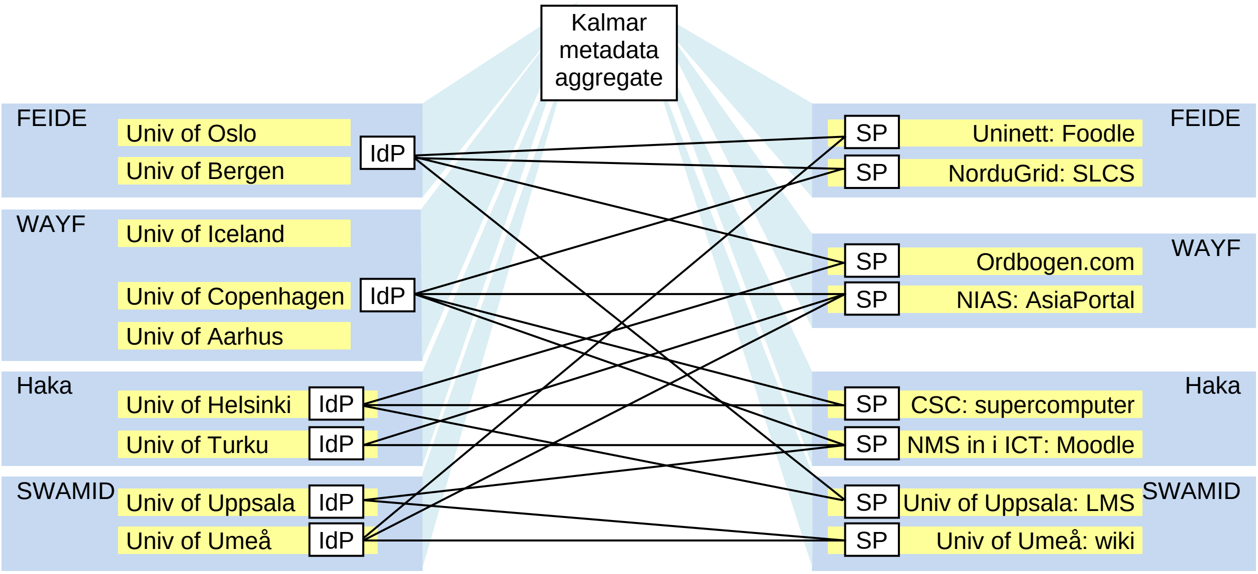


Figure 2. Kalmar Union is a full mesh of Identity Providers (IdP) and Service Providers (SP) registered to the participating federations.

The Kalmar Union setup is managed by aggregating and sharing SAML 2.0 metadata. SAML 2.0 metadata, as specified in [29], is a signed XML document containing a list of Identity and Service Providers (called entities in the specification), their unique names (entityIDs), addresses (SAML 2.0 endpoints), public keys and the other properties their peer Provider needs to know. Participating national federations continue maintaining the metadata for their own national Identity and Service Providers. Additionally, the metadata is shared with other participating federations in Kalmar Union.

Currently, Identity and Service Providers in the national federations must opt-in for being in Kalmar Union. That is desirable at least as long as all the Providers (for instance, Shibboleth 1.3 installations) in the national federations do not support SAML 2.0. Furthermore, there are several Service Providers that are intended for national use only, and at least require modifications in their access control model when Kalmar Union starts to bring in end users from the other countries. Later, when Kalmar Union is well established, we may consider if this principle will be revised and Identity and Service Providers in participating federations made automatically visible also in Kalmar Union.

## 4.2. SAML 2.0 Metadata Management

Each national federation provides a national aggregate of all entities that are exposed in Kalmar Union. These entities are presented in a signed SAML 2.0 metadata document in a well-known URL made available to a central Kalmar Union metadata aggregate service. The metadata files are only valid for a pre-defined time (as expressed in the validUntil attribute). The URL to the document and the signing public key is configured in the metadata aggregate service.

All entities exposed in the national aggregates must be configured to consume Kalmar metadata from the central metadata aggregate (see Figure 2). As long as the national federations have Providers which do not belong to Kalmar Union, all providers need to continue consuming the national federation's metadata, as well. This leads to the situation where a national Service Provider may be visible to the Identity Provider both in the national metadata and in the Kalmar Metadata, which could be solved by preferring the national metadata since this is in the same security domain.

In order to avoid conflicting names for Identity and Service Providers, each participating federation ensures that all participating entities have its SAML 2.0 EntityID in a controlled namespace, which can be either a URN or a URL. For example, a university that uses a URL as entityID must use a domain name that the university or the federation controls. If there are Providers which are registered to more than one participating federation, the duplicates must be excluded from the aggregated Kalmar Union metadata. Typically, cross-national content providers, such as library content providers or Microsoft DreamSpark, are registered to several national federations.

Scoping of identities is fundamental to the security model in a full-mesh-federation, where the Identity and Service Providers communicate directly. Scoping ensures that only the Identity Provider of CSC is able to assert an identity for end user “mlinden@csc.fi”. Otherwise, an attacker needs to compromise just one Identity Provider in the federation to impersonate any end user in any of the Identity Providers. To enforce scope checks, a Service Provider needs to have a list of the scopes that each Identity Provider is allowed to assert.

Shibboleth software makes use of a proprietary extension element in the SAML 2.0 metadata to express the list of scopes allowed for each Identity Provider. The extension element is used in the Kalmar Union metadata, as well. The list of scopes is included for all Identity Providers in the metadata. Regular expressions are not used in the scope element.

SAML 2.0 deployments often use public key cryptography to ensure the confidentiality and integrity of the message exchange between an Identity and Service Provider, and their public keys are typically placed in the SAML 2.0 metadata. In Kalmar Union, all Identity Providers entities must have an embedded signing certificate in the metadata. If the Service Providers' SAML 2.0 endpoints are not available on HTTPS, all Service Provider entities must have an embedded encryption certificate, as well. Without an embedded certificate it is not possible to encrypt the XML messages sent to the Service Provider. In Kalmar Union, embedding keys in metadata follows the guidelines in the SAML v2.0 metadata interoperability profile draft [30].

SAML 2.0 metadata contains also name and description elements for the entities. In the metadata, Identity and Service Providers must support multi-lingual names, and supply at least their name in English. Service Providers must also have a multi-lingual description of the service, describing the purpose of the service. This information is used for the informed consent and the consent management. Technical and administrative contacts must both be provided, as well. Without technical and administrative contacts, solving operational issues (bug tracing, performance issues, missing user accounts, etc) is impossible.

## 4.3. Identity Provider Discovery

Services connected to Kalmar Union are responsible for handling the user interface for selecting which Identity Provider to login to. Kalmar recommends using the OASIS draft Identity Provider Discovery Service Protocol and Profile [31] and offers a central discovery service supporting it. The Kalmar central metadata aggregate is also configured to work as a central discovery service. However, using the central discovery service is optional.

Using the central discovery service is convenient for services that are only connected to Kalmar Union. However, if Service Providers are also connected to the national federations, the setup becomes more complicated as the Service Providers probably have legitimate end user from those national Identity Providers who are not registered to Kalmar Union. In that case, the Service Provider is advised to have both the national discovery service and the Kalmar discovery service available for the end users.

The discovery service can be used in two ways, either in an active or a passive mode. In the active mode, the Kalmar discovery service presents a dialogue asking the user to indicate where he or she comes from. In the passive mode, the central domain name is only used for storing and retrieving Identity Provider selection in a common central domain by using a cookie.

Kalmar testing has led to a proposal for a new protocol extension to the Identity Provider Discovery Service Protocol that allows the Service Provider to send an Identity Provider preference to the Kalmar discovery service. The Kalmar discovery service user interface then presents the Identity Provider as a pre-selected one to the end user. This nicely combines the requirements for a Service Provider styled discovery service with the feature of a preselected Identity Provider that you obtain by having a centralised discovery service. The details of the Extended IdP Discovery Service Protocol are presented in [32].

## 4.4. SAML 2.0 WebSSO Protocol Profile

The entities in Kalmar Union must support SAML 2.0 as specified by OASIS. However, SAML 2.0 is a versatile specification, containing several optional and alternative features. A SAML 2.0 deployment, such as a federation utilising several software products, needs to agree on the subset i.e. a profile of SAML 2.0 that is specific enough to make an Identity and Service Provider interoperable.

Kalmar Union uses a deployment profile [33] that specifies how to configure the SAML 2.0 entities in Kalmar. A participating federation may use the profile also internally in the national level, but Kalmar Union puts no requirements or restrictions on the local federation, only between entities that participate in Kalmar Union.

According to the profile, each Identity and Service Provider must support at least the Authentication Request protocol with the HTTP redirect binding in the request and the POST binding in the response. The authentication response must be signed but the request need not to. In the authentication response, the Identity Provider releases also the necessary attributes to the Service Provider. The Service Provider's AttributeConsumingService element in the SAML 2.0 metadata includes a list of the attributes the Service Provider requires from an Identity Provider.

The SAML 2.0 specification has a Single logout protocol for Identity or Service Provider initiated global logout. However, the feasibility of logout has faced skepticism [34]. In Kalmar Union, supporting single logout is optional. If an Identity or a Service Provider supports logout, it manifests a SingleLogoutService endpoint in its metadata. HTTP redirect binding is used for both the LogoutRequest and the LogoutResponse. The receiver of a logout request is expected to respect the IsPassive flag, if it is set in the request.

SAML 2.0 specification specifies various formats for an end user's unique identifier (NameID). In Kalmar Union, transient NameIDs are used as a default. In Kalmar Union metadata, a Service Provider may optionally include a NameIDFormat specification.

## 4.5. Attribute Management

In European data protection legislation, processing unnecessary personal data is not allowed. All participating federations respect this by supporting the release of only necessary attributes from an Identity Provider to the Service Provider. For instance, the Finnish Haka federation maintains a Shibboleth attribute filter policy file that allows attribute release for only necessary attributes, which differ Service Provider by Service Provider.

The SAML 2.0 metadata specification supports a list of requested attributes for a Service Provider element. In Kalmar Union, all Service Provider entities must make use of the RequestedAttribute element in the metadata to include a list of requested attributes. Although the official and authoritative information about attribute release policy is included using

RequestedAttribute elements, Kalmar metadata aggregate service provides also Shibboleth specific attribute filter policy XML documents for convenience to the Identity Providers running the Shibboleth software.

In Kalmar Union, the attribute name format must be a URI. All attributes transferred in Kalmar use the OID formatting of attribute names, as suggested by SAML 2.0 profiles specification [35] and the MACE-dir group of Internet2.

Each participating federation has a different specification for the attributes and the mandatory attributes vary federation by federation. In Kalmar Union, our approach has been to assess the differences in the attributes openly and provide comparisons. However, all participants must as a minimum support the schema defined in eduPerson. Other schemas supported include Schac, funetEduPerson, norEduPerson, eduOrg, norEduOrg and norEduOrgUnit. In Kalmar Union, it is up to the Service Providers to adapt to the varying attributes.

# 5. Future Work

In the Kalmar Union project we found that harmonisation of participating federations is beneficial for cross-federation interoperability. This chapter presents the issues we consider most imminent. We recognise that, so far, identity federations in higher education have grown in different environments to serve different needs. Some of the differences between federations have solid reasons, whereas some differences are merely results of a coincidence. Nevertheless, harmonising operational federations is a long and tedious process. In higher education, further discussion in this area is taking place in the REFEDs working group.

## 5.1 Attribute Harmonisation

Specifications for attributes have a long tradition due to the LDAP schemas, such as Person, orgPerson and inetOrgPerson. Most academic identity federations have re-used these schemas, supplemented by eduPerson and Schac. Still attribute incompatibility is a hard problem for cross-federation interoperability. This is due to the differing mandatory attributes, the different semantics of some attributes (especially those used for authorisation) and the definition of the attribute that is used as the persistent identifier of an end user.

| WAYF | Haka | FEIDE | Attribute name |
|---|---|---|---|
| MUST | MUST | MUST | eduPersonPrincipalName |
| MUST | MUST | MUST | cn |
| MUST | MUST | MUST | sn |
| MUST | | | gn |
| | MUST | | displayname |
| MUST | | MUST | mail |
| | | MUST | o |
| | | MUST | uid |
| | | MUST | userPassword (for LDAP BIND only) |
| | | MUST | eduPersonAffiliation |
| MUST | | | eduPersonPrimaryAffiliation |
| | | MUST | eduPersonOrgDN |
| | | MUST | norEduOrgSchemaVersion |
| | | MUST | norEduPersonNIN |
| MUST | | | eduPersonTargetedID |
| MUST | MUST | | schacHomeOrganization |
| | MUST | | schacHomeOrganizationType |
| | | MUST | norEduOrgNIN |
| | | MUST | eduOrgLegalName |

Table 1. Mandatory attributes in WAYF, Haka and FEIDE federations.

The concept of a mandatory attribute is not evident in an identity federation. As noted in section 4.5, the list of necessary attributes varies service-by-service and there may be even services which do not need any end user attributes at all. The federations' approach to the problem varies. Some federations (such as SurfFederatie in the Netherlands) do not have mandatory attributes, whereas some federations have a lot of attributes which must be populated and available for each end user in the federation. For instance, the FEIDE federation of Norway has 13 mandatory attributes.

Table 1 compares the mandatory attributes in three participating federations in Kalmar. As the table shows, only three attributes are mandatory in all the three federations. This may look like a secondary difference, but for Service Providers the difference is vital. A Service Provider typically wants to know the list of attributes available in all participating Identity Providers, i.e. the list of attributes whose existence they can rely on in their service. For instance, in Kalmar Union, the Moodle learning management system of University of Turku did not work with Danish and Norwegian end users because it expected the displayName attribute from each end user.

Difference in attribute semantics means, that the federations use the same attribute but in a different way. For instance, the order of the first name and the family name may vary in the cn (commonName) attribute, resulting diversity in the user interface.

A difference in the attribute semantics is more harmful in an attribute which is used for authorisation in the service. eduPersonAffiliation, which describes an end user's role in his home organisation, is an evident example. The eduPerson schema has clearly listed the values permitted for eduPersonAffiliation (faculty, student, staff, alum, member, affiliate, employee, library-walk-in), but their semantics are not defined well enough, and differing interpretations exist. For example, should `student` cover any kind of students or just degree students, whose relationship to a university is often considered stronger than that of an Open University student? Is a researcher in the laboratory `staff`, `faculty`, `employee` or any combination of them? Even completely contradictory interpretations exist in European federations (Table 2).

| **eduPersonAffiliation value** | **The Finnish Interpretation [37]** | **The British Interpretation [38]** |
|---|---|---|
| Student | Degree student, exchange student, visiting student | Undergraduate or postgraduate student |
| Faculty | Academic workers (research and education workers at laboratories) | Teaching staff |
| Staff | Non-academic workers<br>(administrational workers) | All staff |
| Employee | Person actually employed by the institution (e.g. not a contractor) | Other than staff or faculty<br>(e.g. a contractor) |
| Member | All above + students taking qualifying/further education courses | All above |
| Affiliate | Others, such as Open University students | Relationship short of full member |
| Alum | Graduate | Graduate |

Table 2. Interpretation of eduPersonAffiliation attribute in Haka Federation and UK Access Management Federation [36]. Mapping this kind of differences is difficult for a Service Provider or for a protocol gateway, if any.

In Kalmar Union, we used the approach to document the federations' attribute differences, and to some extent this may be inevitable in the long run, as well. However, if attributes are not harmonised, the Service Providers in the confederation shall process attributes differently depending on which federation the end user comes from. This imposes an additional burden for the Service Provider administrator, who is an expert on his or her service but not on understanding the differences in the national identity federations. As the result, the Service Providers' willingness to join a confederation decreases. To make setting up a confederated service easier, this kind of differences should be hammered out.

The unique identifier used for an end user is an important detail in the attribute specification, because most services need to uniquely identify him or her and store his or her profiles in the service. Traditionally, eduPersonPrincipalName has been used as a unique identifier in academic federations. ePPN uniquely identifies an end user, but only at a certain point of time. Over time, end users leave their home organisation and the ePPN value may be reassigned to a new person. If no preventive actions are taken, the new ePPN holder is able to access the previous holder's profiles, which is a notable security and privacy risk. In WAYF and FEIDE federations, ePPN values may be reassigned. SWAMID forbids ePPN reassignment completely and Haka federation allows it only after a 24 month fallow period. To make sure user profiles are not mixed, a Service Provider in Kalmar Union needs to follow the policy of the weakest federation.

A promising way out from the ePPN problem is to use eduPersonTargetedID or the SAML 2.0 persistent identifier, instead. They are privacy-preserving identifiers whose values are not reassigned, by definition. If they are seen as the future direction, the direction should, again, be implemented in all the participating federations in the confederation. The Service Providers are not happy with an identifier that is not available for end users in all participating federations.

## 5.2. Campus Identity Management Requirements

A fundamental characteristic of federated identity management is that the Service Provider needs to trust the Identity Provider which is responsible for authenticating an end user and maintaining his or her attributes. In a confederated setup, it is even more difficult to trust the Identity Provider which is from another country and culture. The assurance level of the end user's attributes and authentication depends a lot on the processes and practices the home organisations have deployed in the identity management system on which the Identity Provider relies.

There are existing initiatives on Levels of Assurance, such as NIST SP 800-63 [24] and IDABC eID Interoperability [25]. However, they focus on the initial proof of identity and reliability of authentication, while the quality of attributes has been left out of the scope. In higher education, a university can hardly claim to have a high-quality identity management system in place if the account of a departed student or staff member is not properly closed. The two specifications do not cover this issue.

The federations' requirements for federation members' campus identity management vary. There are federations who consider the quality of user identities as part of the institutional autonomy. The Nordic approach has been to require a high quality identity management when the home organisations join the federation. It covers also the quality of attributes; for instance, the eduPersonAffiliation value students must cease the same day when a student graduates in a FEIDE home organisation.

Like attributes, harmonising federations' levels of assurance is tedious work. For the same reasons as the attribute harmonisation, a definition of a certain minimum level for all federations is desirable from a Service Provider perspective. That way the confederation service is made simple enough for a common Service Provider.

## 5.3. Usability and User Experience

Usability from an end user point of view is important in a confederation deployment. After all, a confederation serves the needs of an end user who wants to use services in foreign federations. A usability flaw in a security service, such as a confederation, endangers the whole service.

More research is needed on how to implement the multi-federation Identity Provider discovery in an easy way for the end user. Furthermore, the end user must be aware that she or he is going to access a service in a foreign federation and security domain. This makes the requirements imposed by the data protection directive even more important; the user must be clearly informed that his or her personal data is to be released to a Service Provider in a foreign federation before he or she consents to the attribute release.

## 5.4. SAML 2.0 Profile

While SAML 2.0 is becoming the prevailing technology for academic identity federations, the complexity and the several optional features of the specification are hindering its use. In Kalmar Union, WAYF and FEIDE federations are based on SimpleSAMLphp and Haka and SWAMID are using Shibboleth software mainly. In the future, also commercial SAML 2.0 implementations are becoming more usual. All these implementations should be able to interoperate in a confederation.

To overcome the problem, additional SAML 2.0 profiles have been defined. The SAML 2.0 profile used in Kalmar Union aims at being a minimal SAML 2.0 profile, using just the strictly necessary features which most products are expected to implement. The profile tries to be specific enough to minimise the issues which are left as a deployment choice.

However, the community needs still more experience on profiling SAML use. Few national federations have yet defined their SAML 2.0 profile, not to mention the SAML 2.0 profiles for a confederation. This is also an opportunity; the time window for adopting a common SAML 2.0 profile is still open for academic federations.

### 5.5. Business Model

Some participating federations in Kalmar Union have an annual fee for Service Providers in the national federation, others do not invoice the Service Providers. This can potentially lead to Service Providers optimising their costs by joining in the cheapest federation, which leads to an unhealthy practice where the cheapest federation takes the burden of carrying out the contractual and technical work with new Service Providers. This holds true especially with international Service Providers, such as library content providers, who would otherwise join all the national federations, one by one. A confederation probably makes the participating federations to unify their pricing model for Service Providers.

There are currently no established business models or accounting frameworks in use in academic confederations. Traffic exchange for login is not common either, but is in theory similar to other forms of traffic exchange, such as IP traffic or multicast. Kalmar has chosen to not have any charging for transactions.

## 6. Conclusions

During 2008-2009, establishment of Kalmar Union, a confederation of five Nordic academic identity federations, has proved that a confederation of identity federations is possible both from policy and technical perspective. Real use cases have been identified for a confederation, making introduction of the confederation worth the effort.

Setting up a confederation should start with the policy work. What are the requirements the privacy laws impose on the confederation? What kind of minimal requirements are needed for joining federations? What kind of organisation the confederation will have, and how binding legal structure is necessary for its establishment?

Once the legal and policy side is fixed, a technical architecture implementing the policy can be designed. We showed that bridging elements or other protocol gateways are not necessary for a confederation. Instead, we used a profile of SAML 2.0 technology end to end in the confederation.

Our experiences also show that some harmonisation of the participating federations is necessary. In addition to a SAML 2.0 profile, the set of attributes and their semantics needs to be standardised. A certain minimum level for identity management in the participating Identity Providers must be agreed on. The business models of the participating federations may need some common principles. Finally, the user experience for the end user should follow common guidelines independent of the federation to which the Service Provider belongs.

### Acknowledgments

We express our gratitude to NordForsk for funding the establishment of Kalmar Union.

### References

[1] InCommon Federation: “InCommon glossary”, Referenced 19.4.2009. http://www.incommonfederation.org/glossary.cfm

[2] TERENA TF-EMC2: “REFEDs Federation Survey”, Referenced 19.4.2009. https://refeds.terena.org/index.php/Federations

[3] D. Lopez, R. Castro-Rojo: “Ubiquitous Internet Access Control: The PAPI System”, International Workshop on Trust and Privacy in Digital Business - TrustBus 2002. September 2002.

[4] M. Linden: “Organising federated identity in Finnish higher education”, Terena Networking Conference, 2005.

[5] M. Tysom: “The UK federation”, Terena Networking Conference, 2007.

[6] A. Reid: “The Australian Access Federation”, Terena Networking Conference, 2008.

[7] “eduroam”, Referenced 19.4.2009, http://www.eduroam.org/

[8] Geant2: “European eduroam confederation policy”, January, 2008.

[9] Geant2: “Deliverable DJ 5.1.4: Inter-NREN Roaming Architecture: Description and Development Items”, September, 2006.

[10] Geant2: “Deliverable DJ 5.2.2,2: GEANT2 Authorisation and authentication infrastructure Architecture – Second edition”, April, 2007.

[11] “The International Grid Trust Federation”, Referenced 19.4.2009 http://www.igtf.net/

[12] A. Whitten, J. Tygar: “Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0”, The 8th USENIX Security Symposium, pp. 169–184, 1999.

[13] D. Balfanz, G. Durfee, D. Smetters: “Making the Impossible Easy: Usable PKI” In Cranor L., Garfinkel, S. (eds): Security and Usability. Designing Secure Systems That People Can Use, pp. 319–333, O’Reilly Media Inc, 2005.

[14] P. Windley: “Digital Identity. Unmasking Identity Management Architecture (IMA)”, O’Reilly Media Inc, 2005.

[15] P. Ahonen: “Funet - Finland's way to the Internet”, CSC - IT Center for Science Ltd, 2008.

[16] “Greater Nordic Middleware Symposium”, Referenced 19.4.2009 http://www.gnomis.org/

[17] M. Linden: “Nordic middleware identity federation”, Nordunet Conference 2006.

[18] W. Tveter, I. Melve, M. Linden: “Towards interconnecting the Nordic identity federations”, Campus-Wide Information Systems, pp. 252–259, Volume 24, Number 2, 2007.

[19] “Nordic Institute for Asian Studies”, Referenced 19.4.2009 http://nias.ku.dk/.

[20] C. Witzig: “Interoperability Shibboleth-gLite”, Terena Networking Conference 2007.

[21] “Nordic Master School in Innovative ICT”, Referenced 19.4.2009, http://www.nordicict.eu/

[22] “Ordbogen.com”, Referenced 19.4.2009, http://www.ordbogen.com/

[23] “Memorandum of Understanding and Charter for the Kalmar Union identity management collaborative effort”, available in http://www.kalmar2.org/kalmar2web/members.html

[24] W. Burr, D. Donson, W. Polk: “Electronic Authentication Guideline. NIST Special Publication 800-63, version 1.0.2.”, National Institute of Standards and Technology, 2006.

[25] IDABC Programme, eID Interoperability for PEGS: “Proposal for a multilevel authentication mechanism and a mapping of existing authentication mechanisms”, European Communities. December, 2007. 73 pages

[26] A. Cormack, E. Kassenaar, M. Linden, W. Tveter: “Federated Access Management. Version 10. Draft”, December, 2008

[27] F. de Quinto, M. Medina: “Best Practices in Federated identity scenarios”, In eChallenges 2006

[28] IDABC Programme, eID Interoperability for PEGS: “Common specifications for eID interoperability in the eGovernment context”, European Communities. December, 2007.

[29] S. Cantor, J. Moreh, R. Philpott, E. Maler: “Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0”, OASIS Standard, March, 2005

[30] S. Cantor: “SAML V2.0 Metadata Interoperability Profile. OASIS Working Draft 01”, August, 2008

[31] R. Widdowson, S. Cantor: “Identity Provider Discovery Service Protocol and Profile”, OASIS Committee Specification 01. March, 2008

[32] A. Solberg: “Extended Identity Provider Discovery Service Protocol”, August, 2008. http://rnd.feide.no/content/extended-identity-provider-discovery-service-protocol

[33] A. Solberg, E. Maler, S. Cantor, L. Johansson: “Interoperable SAML 2.0 Web Browser SSO Deployment Profile”, June, 2008. http://rnd.feide.no/documents/saml2simple.html

[34] C. La Joie: “The Difficulties of Single Logout”, May, 2008. https://spaces.internet2.edu/display/SHIB2/SLOIssues

[35] J. Hughes, S. Cantor, J. Hodges, F. Hirsch, P. Mishra, R. Philpott, E. Maler: “Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0”, OASIS Standard, March, 2005.

[36] M. Linden: “Schac implementation and related issues” in EuroCAMP, October, 2006. http://www.terena.org/activities/eurocamp/october06/day1/linden-schema.ppt

[37] Haka Federation: “funetEduPerson schema. Version 2.1”, August, 2008.

[38] I. Young: “Technical recommendation for participants”, UK Access Management Federation for Education and Research, November, 2008.

## Vitae

Dr. Mikael Linden has been involved in identity management of Finnish universities since 2000. He has been deploying and operating the Haka federation of the Finnish higher education since 2002. He is the leader for the TERENA TF-EMC2 work item on Federation Coordination.

David Simonsen has been involved in work with e-IDs and ID-federations for education and research since 2004, developing and deploying the WAYF federation since 2005. Before that he was co-charing the TERENA task force mobility which developed 'eduroam'.

Andreas Åkre Solberg is technical lead for Feide research and development, working on federation issues since 2005. He developed the open software simpleSAMLphp.

Ingrid Melve is the Uninett CTO and Feide manager, and has been involved in identity management since 2000.

Walter M. Tveter is senior legal adviser at The Centre for Information Technology at The University of Oslo. Tveter has worked with the legal issues of identity management since 2001.