Towards Interconnecting the Nordic Identity Federations

Walter M. Tveter
Center for Information Technology, University of Oslo, P.O. Box 1059 Blindern, NO-0316 Oslo, Norway, w.m.tveter@usit.uio.no

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

Mikael Linden
CSC the Finnish IT Center for Science, P.O.Box 405, FI-02101 ESPOO, Finland, mikael.linden@csc.fi

Abstract
In recent years, several identity federations have been established in higher education around the world. The federations have been national, but first attempts to interconnect national federations have taken place. In this paper we discuss policy issues related to a cross-federation. We look at the Nordic national federations and introduce Kalmar Union, our current initiative with regard to interconnecting the Nordic federations.

Keywords
Identity management, federated identity management, confederation, policy

1. Introduction
This paper outlines considerations for trust management between established national identity federations in education and research. Whereas Internet traffic has well defined protocols like BGP for managing traffic exchange, and PKI has work done on bridges and cross-certification of Certificate Authorities, there is not much work available on trust management for federations. However, federated identity cannot establish trust - it can only communicate it [13, p. 130]. Thus, in an identity federation, trust establishment is, in the first place, a policy issue, not a technical one.

Previous work in interconnecting identity federations have been done in the eduroam confederation for roaming network access [8] and in interconnecting the E-Authentication federation of the US government and the inCommon federation of the US higher education [9]. In private sector, project Fidelity has demonstrated interconnecting four teleoperator-centered CoTs (Circle of Trust)[10].

Users in national federations need access to services in other countries. The federation between national federations (cross-federation, or CoCoT - Circle of CoTs as dubbed by Liberty Alliance) enables an end user to have the same easy way of accessing services abroad as he or she has inside a national federation. For service providers this result in more efficient use of existing resources and for home organizations it can both reduce the institutions’ workload and increase what resources its users have access to.

A reason for looking at the Nordic area is that we are all covered by the same EU regulations, and we also have our common Nordic culture and history. Kalmar Union, a union of the Nordic countries in 1397-1520, provided inspiration and the name to our work. This chapter is a short introduction to the current nordic identity federations and the regulatory environment.

1.1. Nordic identity federations
Each of the four Nordic countries, Norway, Finland, Sweden and Denmark, have their identity federation services or projects. In Norway, Feide federation is a service provided by Uninett, covering currently 17 institutions and 73% of end users in Norwegian higher education. Technically, Feide is moving from the home-grown Moria login service to a SAML 2.0 compatible federation service based on Sun Access Manager product.

In Finland, since 2005, Haka federation has been a service provided to Finnish higher education by CSC, the Finnish IT Centre for Science. Currently, 23 institutions have subscribed the service that makes use of Shibboleth, a profile of SAML 1.1 protocol as specified and implemented by Internet2 of the US. In
March 2007, 168 400 logins were performed to Haka-enabled services including those related to e-learning, libraries and administration in universities and polytechnics.

SWAMI, a consortium of Swedish universities, is introducing the SWAMID identity federation for Swedish higher education. SWAMID is going to use Shibboleth as a technology for cross-organizational access to resources. The DK-AAI federation of Denmark is to follow Sweden and roll out a Shibboleth/SAML based federation before the end of 2007.

The first step towards a Nordic cross-federation was to make a technical demonstration of capabilities and that was carried out in Nordunet Conference in September 2006. For the demo, the Norwegian Feide federation and the Danish DK-AAI test federation was interconnected to the Haka federation of Finland, in order to let an end user from Norway and Denmark use Scientist interface, the web based interface to the high performance computing services provided by CSC, the Finnish IT Centre for Science [7]. The experiment involved a Service Provider with SAML/Shibboleth 1.3 federation software in Finland connecting to an Identity Provider with Sun Access Manager software in Norway and a Shibboleth 1.3 Identity Provider in Denmark. In the demo, Identity and Service Providers exchanged SAML assertions with each other directly; proxies, gateways or bridging elements were not used like in the eduGAIN architecture of Geant2 JRA5 project [12]. After the experiment it was decided to await SAML2.0 support in Shibboleth software before moving forward with more technical work, as SAML2.0 greatly facilitates cross-connects and has a clear definition of metadata.

The second step is adjustment of policies and establishment of the charter of Kalmar Union, whose key elements will be described in this document. The third step is going to be running the cross-federation in a production environment and promoting it to cross-national services.

1.2. Regulatory environment
In EU, the Data Protection Directive [11] sets the scene for federated identity. EU member states and Norway, although not in EU, have implemented the directive in their national legislation. The directive implies that, in an identity federation, any release of attributes that relate to an identified or identifiable natural person is considered as processing personal data, and the directive must be taken into account.

Typically, national identity federations have covered these issues in their policies, and in the policy of a cross-federation the compatibility of the policies have to be ensured. Thus, many of the issues in the following chapters are going to be about how the directive is taken into account in Kalmar Union.

2. Issues in the policy of a cross-federation
The different national federations in the Nordic area, and in Europe as such, have different polices and organizational and technical structures. Preliminary comparisons of these policies [2,3,4,5,6] make evident that the similarities far outnumber the differences. Furthermore, many of the differences appear to be caused by chance rather than by choice. We have compared the Finnish (Haka) and Norwegian (Feide) policies and in them, we find no obstacles that would hinder a cross federation. The Swedish and Danish federations that are being set up have draft policies that seem compatible to such a federation.

The remaining obstacles for achieving a cross-federation of different national federations therefore seem to lie mostly in the policy area. Many potential problems have arisen from legislation that has been passed in recent years concerning privacy and security, not only because the legislation in its provisions limits possible actions, but perhaps even more because the amount of issues that have to be sorted out and analyzed with regard to legislation and policy have sharply increased. The know-how necessary to accomplish this is not normally found in abundance in the environments that develop such systems as identity federations, in sharp contrast to technological know-how. This means that the obstacles to building systems no longer primarily exist as technological obstacles, but more to the policy implications the systems will have and the paperwork surrounding the systems as such.

As the technology used in the different national federations become more and more standardized, the technological challenges in making cross-federations become fewer. The same can be said for the actual policy-barriers, since more and more legislation in this area is passed within the EU. The remaining obstacles therefore seems to be legislative know-how, and because of this lack of know-how, sound information for decision makers to base their decisions on. The result of this lack of certainty is an
increase of risk. We believe that the known negative consequences of stalling progress outweigh these risks.

This chapter presents the issues we have found relevant for the policy of a cross-federation and how we plan to cover them in the charter of Kalmar Union.

2.1. Choice of organizational model
The Kalmar Union will not be based on any organization on top, but on bi/multi-lateral agreements between the participating federations, or consortium-model as described by Liberty Alliance [1]. One charter, made by the original partners will be at the heart of this. The charter has a simple mechanism of entering new members, by making every other member sign another copy of the charter with the new member listed. This model is easy to set up, but it does not scale very well.

Incompatibilities in federations’ policies are potential problems slowing down new federations to join the union. Every federation in the union will naturally have a veto against new members. This is a further hindrance in relation to scaling. Having good documentation that is easy to compare will reduce the negative effects of this. We do not, at present, have any accepted and well known way to compare levels of assurance and related attributes of each national federation or its members. This is a problem, but we hope such will come into existence in the future.

The advantages of the model is as stated the easy of setting it up. This is the case not only with the necessary paperwork and administrative tasks for making the cross federation in itself, but it lowers risks in joining, thus making the initial union something that can be accomplished rapidly.

2.2. Consent and terms of service
The use of services from another federation should be solely based on user-given consent. This necessitates that no relevant transfer, copying, caching or related processing of any personal data takes place outside the users own federation before consent is given, apart from that which is necessary for the consent-giving process in itself.

The charter states that the national federations need to have mechanisms for consent to be able to be informed. This includes information about what a user is consenting to, who the consent enables to act, what personal data is involved and preferable where this data comes from.

In their study, Friedman et al identify voluntariness as one component of informed consent [14]. A question can be raised as to whether consent is freely given if the consequences of declining to give consent are negative. If the receiving party when its request is denied creates a situation that directly affects the data subject in a negative manner, for example by terminating employment, consent cannot be said to be freely given. In the Kalmar model a situation may arise where refusal to consent to using a service will cause a negative effect in the relationship between the data subject and a third party. For instance where a scientist refuses consent to use a Norwegian service and therefore is unable to perform his duties as a researcher at his Finnish university. The fact that his employer can let this have consequences for him will not damage the quality of the given consent.

In relying solely on informed user given consent, we avoid most of the restrictions concerning cross border transfer of personal data.

2.3. Liability
We have attempted to avoid liability issues in as large degree as possible. Like the issues with regard to personal data we see the relevant problem with liability as one that presents itself across the different national federations, not within them. This is because the national policies concerning liability differ both in detail in the policies themselves and also because of differences in national legislation. By offering the services in a cross-federated setting on an as-is basis we hope to minimize such issues. This means that the quality of service in a liability perspective will be less when using the Kalmar Union. Because both users, home organizations and service providers can choose whether or not they wish to use services via the Kalmar Union this will perhaps cause some of them, especially service providers to asses the risk of opening their service as to great, but we have a realistic hope that most will not see this as a problem.
2.4. Subjects and roles in the federation
The organizational structure of the national federation differs from country to country. The different organizational structures of the national federations should, however, not have any consequence for the Kalmar Union as long as the body of the national federation that enters into the agreement has adequate powers delegated to it. The subjects of the agreements are therefore the national federations themselves. They each have a responsibility to have agreements in place with their respective members that makes this possible. This solution is essential to making the consortium-model possible, as a situation where every member of a national federation had to be a part of the union would be impossible to administer.

A further advantage is that a national federation that has members who trust it sufficiently to delegate authority to cross-federate with other federations has a high probability of being well founded and based on sound principles.

2.5. Support
The different entities in the Kalmar Union naturally need access to support. The chosen model is to let the national federations provide support for all their end users, members and service providers. The national federations themselves will have to obtain assistance from each other on a top-level where this is necessary. The Kalmar Union in itself, i.e. the mechanisms that enable the cross-federation, will be supported by the parties that run them, that is the founding members Feide/Haka. At this point of time no plans exist for reimbursement of such costs from potential new members. If the cost of this operation in the future should become substantial, a cost sharing can be implemented between the national federations.

2.6. Making services available
The different national federations at a policy level as well as the technology being used will determine at what level of detail an entity can decide who gets access to a service, both in regard to a service provider and a home organization. A goal of the Kalmar Union is that all service providers shall be able to choose who they are willing to open their services to in as fine grained way as possible, based on the systems for accomplishing this, on a technical and national federation policy level.

Institutions and users should also be given this choice, in other words, only if a service wants to be available to a user and both this user and its home organization wants it to be able to access the service, can this take place. Limitations in technology or policy will perhaps not enable a fine grained approach to this in an initial phase. An institution will, for example, be given the choice of giving its users access to another national federations or not. Eventually this choice can be made to differentiate between different services and different users or groups of users.

2.7. Intellectual property issues
Each national federation is responsible for the Intellectual Property Rights (IPR) of the software components used to deliver the federation services. The responsibility for any proprietary Kalmar components should be taken by Haka or Feide as the founding members, and software should be made available with an open source license.

Given the many controversies with regard to Intellectual Property Rights (IPR) related issues one cannot exclude the possibility of a third party, or any party as such, trying to seek damages or otherwise hold responsible any entity or individual in an IPR-dispute. However, this is not a risk that is much amended by cross-federating in itself. As for the member institutions of the national federations, they are for the most part publicly funded education and/or research facilities that should be able to shoulder any such cost if it indeed were to appear.

2.8. Data processing contracts
It is necessary for any controller to have a written agreement with its data processors. The national federations may be (and, in the case of Feide federation, is) such processors with regard to the home organisations of the end users.

If each national federation has adequate contracts with its members and can guarantee that none of its services spread personal data to third countries, one could probably avoid using several layers of data-processing contracts, just by expanding the one between the home organizations and the national federations to cover other Kalmar Union national federations as subcontractors for the respective national federation.
2.9. Attributes
According to the Data protection directive, all the attributes released must be relevant for the service. A list of what attributes a service legally can request must be available for both the home organization and the end user from the foreign federation. Ideally, the user should be able to see this every time consent for attribute transfer is given. It may be sufficient to show the user what attributes will be released, although it is far better if the content of the attribute is also revealed.

2.10. Cost and payment
The Kalmar Union is established as a non-payment service where participating federations cover their own cost. The interconnection is done by metadata exchange, and does not require central components. Data should not be released to be used to charge costs to services. The main reason for this is that, in the beginning, Kalmar Union has no mechanisms to support either initial usage statistics sufficient to use for demanding payment or auditing purposes. Any service that require payment has to establish its own payment mechanisms out-of-band.

2.11. Jurisdictional issues
Information about jurisdictional issues and other related consequences of offering or using cross-border services must be made available to home organizations, services and end users. This shall be amongst the extra information that is presented when a Kalmar Union service is offered.

2.12. Conflict resolution
Given the model of the Kalmar Union and the as-is nature of the services provided, most conflicts can either be avoided or governed and solved inside the national federations. A conflict between two (or more) Kalmar Union participating national federations however will be governed by the Kalmar Union charter. This attempts to reduce the possibility of such conflicts arising. If they arise there will be a mechanism for arbitration where either Terena, some underlying body of the Nordic council of ministers, or both can solve the conflict.

This being said, there is of course no way to hinder a participating national federation or any other entity from taking legal action against another. The model as it is will hopefully limit the ability of any entity to gain much from such action and therefore discourage it.

3. Further work
As noted earlier, we have no accepted and well known procedures for assessing levels of assurance across federations. There is work to be done on the semantic interoperability of attributes, as definitions and regulations for the same attribute may differ from federation to federation.

It is important to follow the EU work on eID and identity management requirements, both legislation as it is enacted in each country and guidelines and best practices. The work done with the Kalmar charter is valid only within the European context, and for non-European federations to join those federations would need to do assessment of their legal context as it relates to the European Union and European Economic Zone. The role of data processor varies with the different legal interpretation of EU legislation. Each participating federation must provide a clearing house, with the minimum being a list of contact points, and a statement on their policy with regards to data processing.

With regards to user consent, we need to collect operational experience and do more user testing to find the best way to inform users.

The Liberty Alliance work on crossing circles of trust has provided valuable input, and is something to follow as more environments gain operational experience with cross-federations.

4. Conclusion
As the technology used in federated identity management become more and more standardized, the technological challenges in making cross-federations become fewer. Therefore, the remaining obstacles
seem to be legislative know-how, causing lack of sound information for decision makers to base their decisions on.

For this paper, we compared policies of existing academic identity federations and found more similarities than differences. In this paper, we presented the key issues for a policy of a cross-federation. Based on this work, we continue establishing Kalmar Union, a cross-federation of the Nordic academic identity federations.

References