Trusted third party based ID federation, lowering the bar for connecting and enhancing privacy

David Simonsen, Jacob-Steen Madsen
The WAYF secretariat, H.C. Andersens Boulevard 2, DK-1553 Copenhagen V, Denmark
david@wayf.dk, jsm@wayf.dk

Case study

1 Abstract

The rationale behind a new eID federation architecture is presented along with a host of new features and ways to operate established federation functions and procedures. The architecture of the Danish eID federation for education and research, WAYF - Where Are You From, is a combination of two well known ID-federation models: the loosely coupled Shibboleth model and the Norwegian 'central-login' model. The WAYF-model, the trusted third party, TTP, model, combines the decentral login from Shibboleth with the user and data flow from a hub-and-spoke-model. Added to this are centrally provided, complex services that institutions and service providers often see as obstacles. The new design leaves the opportunity to relief institutions and services in several ways: 1) multi-protocol support and real time translation lowers the bar for connecting to the federation, 2) informed user consent to data exchange is centrally provided and 3) a new privacy protecting model for user pseudonyms is implemented. When connecting to other ID-federations, the point of contact is transparent to services and institutions as only the central federating component needs to connect technically. This has been shown in the case of the Nordic 'Kalmar Union'. WAYF has now been in production for more than a year and is gaining strong momentum. As other federations are showing interest in the TTP model, both for complementing and further develop existing federations as for building new ones, it is our hope that this overview will provide basis for discussion, further development and adaptation of the new federation architecture.

2 Keywords

ID-federation, privacy, protocol translation, consent, SAML2, inter-federation

3 Background

When building large and heterogeneous systems, focus on decentralization and use of open standards and protocols seems the right way forward. Certainly in smaller countries or large organisations with relatively few sub-institutions or branches, the establishment of an trusted third party, TTP, like the one described here, might be a sustainable solution. In some cases the model may not be acceptable but this will be due to cultural factors and traditions as the technology used in WAYF[1] is capable of scaling to even very large installations.

Raising demand for web based (self)services in the sector for research and education has increased focus on the requirement for better identity management and federated access management for services. Several countries started implementing authentication and authorisation infrastructures (AAI) years before the Danish initiative was started. The lessons learned from these front runners, and their frequent advice has been and are still invaluable. WAYF has spent several years building the ID-federation for education and research. First a classic Shibboleth model was introduced with no luck. Then a hub-and-spoke model with centralized authentication was suggested - this also proved unsuccessful, see below.

The intended user group was originally 'higher education and research' but institutions from several levels of further education are now connecting along with university hospitals etc. Proof-of-concept to inter-federating with the national 'citizens login' is planned, perhaps paving the way for accessing more public services, which are normally seen as 'out of scope' for research and education.

3.1 Failing Shibboleth deployment

In 2005 it felt natural to build on the experience made available by the frontrunners (USA[2], Switzerland[3], Finland[4] etc.) and to the largest possible extend copy what was already working. Both policy wise and system wise. Shibboleth 1.3[5] was then seen as a the facto standard, and a Danish test federation was established.
Despite thorough preparation and strong signals of commitment from the institutions (signed letters etc.) only two actually installed the Shibboleth packages. The argument for not connecting was often that the software was complex and dependent on specific libraries and packages. Also fear of getting 'locked in to yet another protocol' played a role. Lastly it was considered too difficult to connect services - especially 'legacy services' based on i.e. LDAP, CAS etc.

Recognizing that only few people had knowledge in the field of federated identity and access management, the general conclusion after 16 months was that the knowledge- and technical barriers to the join the federation had to be lower. Thus Shibboleth as product was no longer considered useful in the Danish context. Shibboleth as protocol remains one of few de facto standards in federated identity and is therefore supported and used by WAYF.

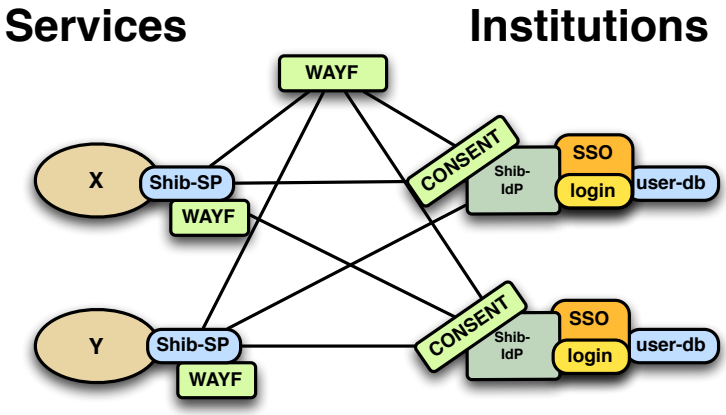

Fig. 1. The loosely coupled Shibboleth model which is based on a full mesh (many-to-many relation) between home institutions and service providers, decentral login-systems and decentral identity management. Implemented in UK, Switzerland, Finland etc.

3.2 Failing central-login-model deployment

As most institutions already ran LDAP-directories for user administration, the Norwegian federation model was considered. Characteristic of this model is the central login function which is used for accessing federated services. Each institution deploys a dedicated LDAP-server for connecting to the federation, in order to live up to the requirements regarding attribute schemas, formats etc. The Norwegian federation, FEIDE[6] [7], was conceived around year 2000, before single-sign-on-systems (SSO[8]) became daily life in institutional service portfolios. The barrier for connecting to such a system was confirmed significantly lower by the Danish institutions as good LDAP knowledge was abundant. One important difference from the Norwegian situation was not taken into account, though: the timing of the project which was now running well into 2006 - with SSO-systems already running at many institutions. Even though the institutions agreed that a central model looked compelling, the message was clear: they would not connect to a central login-system. The arguments ranged from potential branding issues towards the users, control of security domains, return of investment of prior investments in SSO etc.

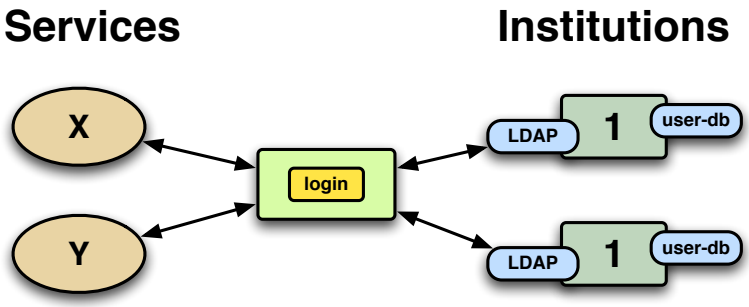

Fig. 2. The central login model providing a single-to-many relation between home institutions and service providers, with decentral identity management and dedicated federation LDAP-servers. Implemented in Norway.

3.3 Conceiving the trusted third party model

Conceiving the trusted third party model (TTP) was then relatively straight forward. The main requirements where: easy connection of institutions, support for multiple protocols, de-central identity management and reuse of existing single-sign-on systems. The result is shown in Fig. 3. A few complex services are provided centrally i.e. handling of users' consents to data release. When personal data is leaving the originating security domain, the user must consent to the data exchange. This requirement is written in EU directive 46/95 on data protection[9] and thus implemented in the various national legislations. The task is, however, not trivial - see below.

Going further, to harmonize the user experience across many institutions, seems not achievable, except if the task is performed 'outside' the institution by a common consent service. For the data not to leave the institutions' security domains, but still enter the central consent service, this service must be part of many multiple security domains a the same time. Legally this can be achieved by having the TTP acting as 'data processor' on behalf of the connected institutions, a role which should be contractually based.

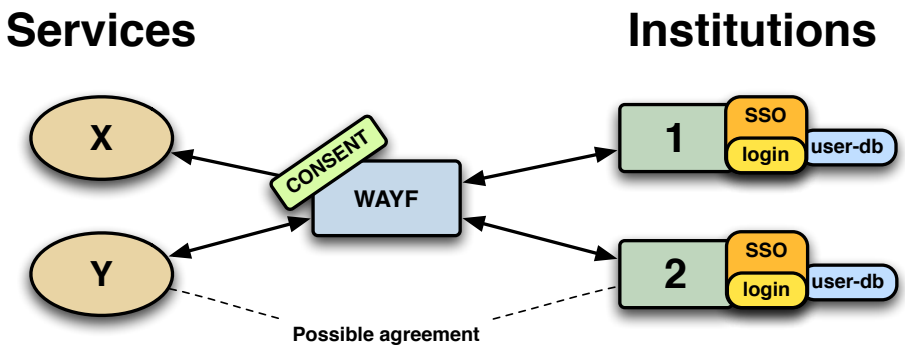

Fig. 3. Hub-and-spoke model, decentral login, decentral identity management

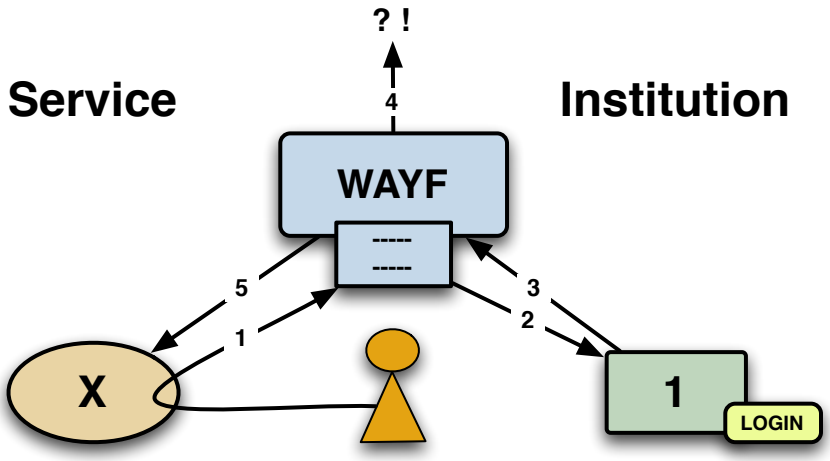

Fig. 4. User and data flow diagram

1. The web based service's login function sends the user to the WAYF web based source where the user chooses his/her institution.

2. If the user is not already logged in he/she is redirected to the institution's login page (he/she will automatically transferred back to the web based service).

3. After login at the institution information about the user is sent to WAYF.

4. The WAYF web page presents the information that will be forwarded to the web based service. The user gives his/her consent with a click on a button. The user can indicate with a 'tick' that the consent should be remembered when visiting the same web based service in the future.

5. WAYF sends the information to the web based service. If the web based service can approve the user based on the information then access is granted.

4 Functional, organisational and technical characteristics of the TTP model

4.1 Support for institutional branding efforts

Institutions are increasingly finding themselves competing for students, research funding etc. An important effort is branding towards the users. 'Login-portals' with single-sign-on to local services is seen as a way of staying in touch, and much money is spend developing coherent user experience and graphical expression to make users feel 'at home' when using the services provided by the institution. This effort was one of the strongest arguments against the suggested Norwegian central login model, which implied that users should log in using a common login-page with no local branding. The institutions argued that they would not support a scenario which both discarded the existing efforts and investments, and also would require the users to do something much different than today. Also the Shibboleth model points the user to the institutional login-page, but since Shibboleth had already been tried with no luck, this technology was not the answer.

4.2 Extending single-sing-on systems with federated services

Traditionally the institutional security domains have been well guarded, but raising demand for more and shared services (across several institutions) is pushing for adoption of services beyond the traditional boundary. When a user has first authenticated at the institution, the same session can now be reused to access in principle any service connected to the trusted third party. Access to services depends of course on the attributes delivered and their values. Accessing a service might require 'login', but if already authenticated at the institution, all the user has to do is to point to the institution. This establishes a session between the users' browser session (with the institution) and the TTP thereby enabling access to all other connected services. The user experience is that the 'local' authentication can now be used to access services 'out side'.

If the user did not authenticate before trying to access a federated service, login at the institution is required in order for attribute release from the institution to happen. WAYF caches the user attributes for 8 hours (a working day) before flushing (deleting) the user specific data. This way users can keep accessing WAYF-connected services for up to 8 hours without re-authenticating.

4.3 Single point of contact to multiple services and institutions

As can be seen in Fig. 3 both institutions and services only make a single connection to the TTP, indirectly connecting institutions to all connected services and connecting services to all connected institutions and their users. The one-to-many-relation model substantially lowers the administration work for both service providers and institutions. No further technical modifications are necessary for accessing new services or letting new user groups accessing the service, when first connected to the TTP which takes care of all the details and procedures for establishing new connections.

4.4 Opt-out

Normally when a institution is entering a formal relationship with a service, or vice versa, one contract per relationship is required. With the TTP-model this is no longer necessary since the TTP may have status of 'data processor' on behalf of the institutions. This leaves the opportunity to legally let the TTP engage contractually with the services on behalf of all institutions, initially enabling attribute transfer from all institutions (and from all users) to all services. Institutions can then opt-out of the agreement with any connected service at any time, blocking the attribute transfer to a given connected service. Paper work is this way kept at a minimum for all parties, taking full advantage of the indirect one-to-many relation provided by the TTP.

4.5 Central attribute release policy: one size fits all

The attribute release policy (ARP) for a given service is negotiated with the TTP when connecting to the federation. The ARP describes which user information is released to the service when a user tries to access the service. The ARP must support the principle of proportionality as defined by the EU directive on transfer of personal information (se above). This implies that the purpose of the service must first be described, and the amount of user data needed for granting/ denying access thereafter adjusted accordingly.

As previously seen, in the TTP model each service is connected to the TTP via a single connection. The concept of a 'single connection' also applies for the ARP which is the same for all users, at all institutions. The logic is as follows: a service can only have a single purpose, so the ARP should be the same for all. As only one contract is signed with the TTP (legally the 'data processor' acting on behalf of the institutions) only one set of attributes can be released to the service.

Negotiation of ARP's with the service providers is done by the TTP. Apart from placing a significant responsibility on the TTP it can be noted that representing multiple institutions provides the TTP with a certain negotiation power. This should carefully be used to comply with privacy legislation which is not common place in todays' trend of harvesting as much personal data as possible. The institutions are on one hand side relieved of the administrative burden of handling ARPs - on the other hand they must live with the ARPs provided by the TTP wether they like them or not. Note that if disagreement arises the institutions can always opt-out of the contract with a given service provider.

4.6 Protocol translation eases connecting efforts

It had previously been documented that institutions wanted an easy way of connecting to the federation as well as independence of specific protocols. It was therefore decided to support multiple protocols for connecting both institutions (at present: SAML2, CAS, CAS+LDAP) and services (at present: SAML2, Shibboleth 1.3) and let the TTP translate messages on the fly. This would lower the bar for connecting since many institutions would be able to reuse exiting systems and not have to install and understand new protocols. Upgrading to other protocols would also be unproblematic as it would be a single-institution task and not a federation wide effort. Introducing new protocols is done centrally at the TTP without anyone noticing as full translation between all supported protocols is done centrally.

In the Danish case only few institutions initially supported SAML2 so it was decided to develop code for supporting Central Authentication Service which allowed the existing and widespread deployments of CAS to be reused in the federated context (the implemented CAS v2 can return attributes). Also a hybrid connection variant, CAS+LDAP, was developed in which CAS v1 (which can not return attributes) at the institution is used for authentication, returning a user name to the TTP which can then be used to query the institutions LDAP-directory for user attributes. This way the TTP will never see any users' passwords - and thereby keep the secret part of the authentication process within the institutions security domain.

4.7 Central consent service and central consent administration

When information about a user is leaving the institutional domain the user must consent to the data exchange, as described in EU directive 95/46/EC on the protection of individuals with regard to the processing of personal data. Any consent must live up to three requirements: it must be voluntary (no disadvantage if not provided), specific (only one purpose) and informed (understandable). Additionally users must be able to withdraw any consent at any time. Putting in place and keeping such systems is seen by institutions as complex task - and many have been relieved when learning that the TTP in the case of WAYF takes care of this centrally. Doing so is a non-trivial task when no personal data is supposed to be stored, as is the case with WAYF. In the following the WAYF solution to the problem is described.

First time a user is trying to access a service, he/she is prompted for his/her consent to the attribute release. The purpose of the service is presented along with the actual values of the data to be transferred. The user can either decline (and hence not access the service) or accept the data transfer. Furthermore the user may choose to let the TTP store information about the consent, in order not to be asked every time the same service is accessed. The problem now is how to do this without storing personal data? The solution is use of destructive one-way encryption (hash-values). These are calculated, based on the name of the service name and the users' personal information, each time attributes are received following successful authentication at an institution. The resulting hash-value, acting as a digital fingerprint, is then looked up in the central database. If present, the user has not only previously consented but also asked to have the consent stored in order not to be asked for consent again - which is why the newly received attributes can be released to the service immediately. If the value is not found in the database, the user has either not previously consented or not asked for the consent to be stored. In this case the user is prompted for his/her consent to the data release - which is of course also true in the event of the database server being unreachable.

To withdraw a consent, the user must go the consent-administration service provided by the TTP. The service receives attributes about the user and calculates all hash-values for all connected services and look them up in the database. A graphical representation of existing consents and connected services is shown, and the user can then remove or add consents to individual services (removing or adding hash-values to the database). Please note that withdrawing a consent does not mean that the data earlier released is deleted. This requires separate contact with the service provider.

4.8 Centrally provided or calculated attributes enhances privacy and prevents spoofing

'SchacHomeOrganization' is an attribute telling the name of the institution where the user has authenticated. This is often used as authorisation information as agreements regularly are negotiated on behalf of all users in an institution. To prevent the hypothetical case where an institution would pretend to be an other institution by providing a false SchacHomeOrganization value, and hence gain its' users access to otherwise restricted services, this particular attribute is provided by the TTP which always has authoritative information about from where the user data was provided. The attribute eduPersonTargetedID (EPTID) is centrally calculated (a hash value) based on three set of parameters: the service name (service specific), user data (user specific) and the institution name. As the user data is not stored at the TTP, the result cannot be recalculated by the TTP without the data about the user kept at the institution. The institution cannot do the calculation since it does not have the exact formula (kept secret by the TTP). The service only receives the user pseudonym (EPTID) and has no chance of reveling the true identity of the user, since it has neither the original attributes nor the formula for calculating.

To identify a user, all three parties, the service with the EPTID value, the TTP with the EPTID formula and the institution with the user database have to corporate. Thus the users' privacy is better protected than in loosely coupled federation models, as the users' pseudonym stays non-decipherable to both service providers, institutions and the trusted third party until an important matter brings the three parties together to identify the user.

4.9 WAYF's wayf - the 'sticky' list of institutions

The use case depicted in Figure 4 shows the use/data flow where the user choses which institution to authenticate at. This is called the 'where are you from' function - the origin of the name of the Danish federation, WAYF. As navigating or scrolling is mostly perceived as tedious a 'sticky' list of institutions has been implemented. The TTP stores a cookie on the users' machine enabling preselection on the list of the institution the user chose last time. The presumption is that users with high probability authenticate at the same institution most of the time. It is recognized that services in some cases want to provide the list of institutions (business partners) at their web site. Investigations into how to support this scenario with dynamic listing, preselection etc. is work in progress.

4.10 Legal status of the TTP: data processor

The trusted third party's legal status is in the case of WAYF 'data processor' on behalf of the connected institutions. This places the responsibility for the users' personal information with the institutions and consequently lowers the audit requirements for the TTP - which is not an insignificant detail when running a federation. A step to further consolidate the status of 'data processor', in the case of WAYF, is the decision not keep any decipherable data about the users for longer than 8 hours. It is generally well received that WAYF in principle is a simple messenger for authentication requests and responses: a true data processor.

4.11 Inter-federating made easy: single point of contact

When ID-federations based on the TTP model connect neither the institutions nor the services have to adjust their technical setup since the new connections are provided centrally by the TTP. This has been proven to be true when establishing the Nordic Kalmar Union where both loosely coupled federations as well as TTP-based federations are inter-connected. Such new structures nourish new partnerships which can easily be established across previously established borders.

5 Future work

The third-party-model, as implemented by WAYF is still in its' infancy, being only one year old at production level. A small albeit growing number of users are using the infrastructure on a daily basis which brings forward several usability questions:

- When the central wayf-function is used, what reactions should be expected if a service does never authorize users from institutions that can be chosen in the list of connected institutions?
- If the central wayf-function is used, what reactions should be expected if an institution does not let their users access a given service?
- How does the trusted third party earn to be trusted by the individual user? Is it up to the connected institutions to educate the users?
- How (in)visible should the trusted third party be to the end users?
- How can users provide attributes from more than a single institution to a service?
- How can services dynamically integrate the list of connected institutions in their web sites?

Solutions for the above mentioned questions, and certainly many more must be provided in a foreseeable future.

A use case concerning age verification has recently gathered support for a new international attribute: SchacYearOfBirth which now enables users to anonymously prove their approximate age. A new and unexpected role for ID-federations - but surely not the last.

6 Conclusions

A federation architecture has been conceived as a combination of two existing models. The resulting 'trusted third party' model is a hub-and-spoke setup with decentral login, decentral user management, central wayf- and consent services as well as privacy protecting generation of service specific user pseudonyms. The system has been in production for more than a year and is gaining strong momentum as one of the primary goals seems to have been met: to lower the bar for connecting both institutions and services.

7 Vitae

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'[10].
Jacob-Steen Madsen was head of IT-development at the University of Southern Denmark for a number for years while also being involved in WAYF - before recently joining the WAYF secretariat full time.

8 References

[1] WAYF - Where Are You From (http://www.wayf.dk)

[2] InCommon, USA (http://www.incommonfederation.org)

[3] SWITCH AAI, Switzerland(http://www.switch.ch/aai)

[4] HAKA, Finland (http://www.csc.fi/english/institutions/haka)

[5] Shibboleth (http://shibboleth.internet2.edu)

[6] FEIDE, Norway (http://feide.no)

[7] FEIDE arhictecture (https://ow.feide.no/feide:architecture)

[8] Single-sign-on: http://en.wikipedia.org/wiki/Single_sign-on

[9] EU, data protection (http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm)

[10]eduroam (http://www.eduroam.org)