Title

Introducing transparency in hub-and-spoke federation architectures using SAML2 authentication request scoping elements

Authors

David Simonsen, Jacob-Steen Madsen, Mads Freek Petersen, Jacob Christiansen

Affiliation

The Danish federation WAYF - Where Are You From

Technical paper

Keywords

Usability, Security Assertion Markup Language ver. 2 (SAML2) authentication request scoping elements, federation, interconnecting architectures

Abstract

The architectural differences between peer-to-peer identity federations and hub-and-spoke identity federations are profound and have implications for the users' interaction with central federation components like the identity provider (IdP) discovery service (aka the 'wayf' or 'where-are-you-from' service). SAML2 authentication request scoping elements allows service providers in hub-and-spoke federations to build their own IdP discovery services. Furthermore, SAML2 scoping elements will in the future enable transparent interconnection of different federation architectures. In early 2010 the Danish WAYF federation was the first to introduce support for scoping elements. Scoping elements are, to the best of the authors' knowledge, still only supported by the software package 'simpleSAMLphp[1]' and in a single .NET implementation - but may come to be widely deployed if and when other SAML2-packages like i.e. the Shibboleth implementation introduce support for this feature.

Background

The basic concept of federated access management is simple: the user goes to the service (Fig. 1, arrow 1). When trying to login, the user is redirected to a web page with a list of trusted identity providers (IdP's) (arrow 2) - the so called where-are-you-from service or 'wayf'. Here the user chooses where to login and is redirected to the IdP's login page (arrow 3). Upon successful authentication, authorisation information about the user is send to the service which in turn decides wether to grant access or not.

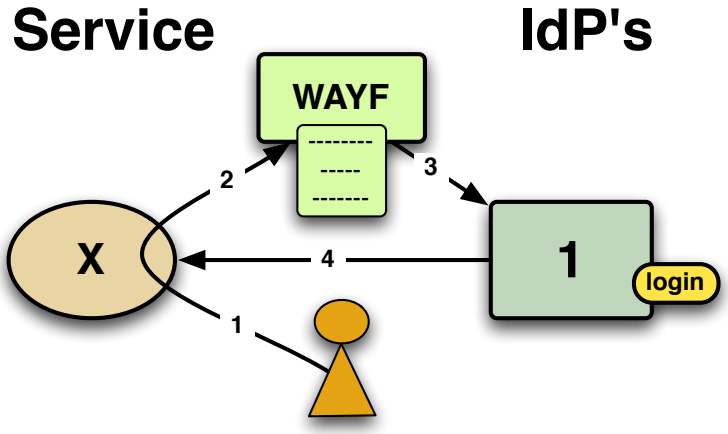

Fig. 1. Basic concept of federated access

Federation architectures generally fall into two categories: the loosely coupled federations, typically based on the Shibboleth-software[2] and accompanying SAML profile (Fig. 2), or hub-and-spoke federations (Fig. 3) like the Danish, Dutch and Spanish which feature a central 'proxy-identity provider' as federating component, providing the wayf-

function (where are you from), among other central services [3].

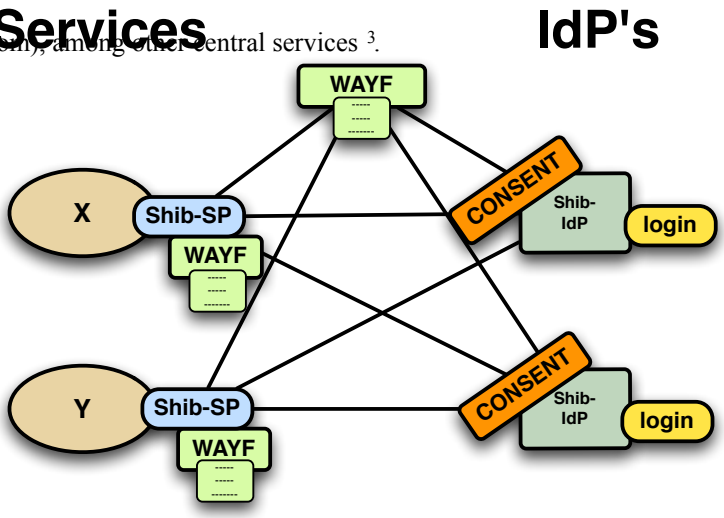

Fig. 2. Loosely coupled federation

One important difference between the loosely coupled federations and hub-and-spoke federations is that in the loosely coupled federations the 'wayf' may either appear as a central component in the federation, typically operated by the federation manager, or at the service providers (SP's). This way services may modify the layout to align with their own graphical layout and adjust the list of IdP's in the wayf to match their list of costumers.

Until now such decentral placement of the wayf function has not been possible in SAML2-based hub-and-spoke federations, even though long requested be the service providers. The SAML2 specification[4] supports a multitude of complex use cases, many of which require functions that are typically not supported by the most common SAML2 . In fact, no implementation is known to support all features of the SAML2 specification.

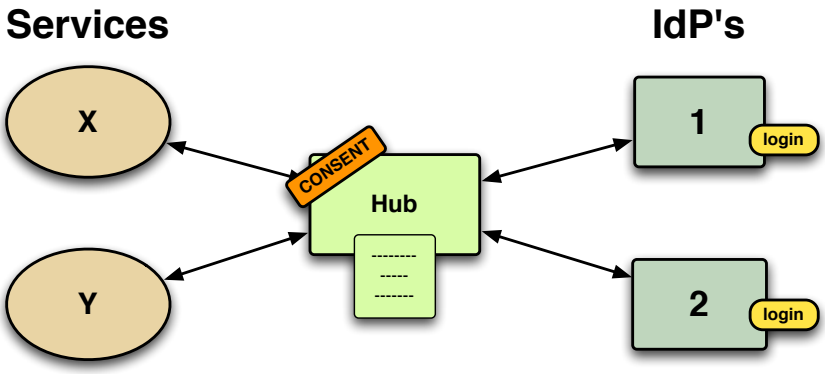

Fig. 3. Hub-and-spoke federation

The implementation of SAML2 authentication request scoping elements was initiated by feature requests from service providers. To complement the service providers' requests, usability experts were engaged to ensure compliance with usability design principles and best practice[5].

The simplest scenario in a hub-and-spoke federation, with a single proxy-IdP, like the Danish WAYF federation [6], is to make transparent redirects from SP's to IdP's. The user experience is a direct jump from the service to the IdP even though this is technically not the case, as the federations' hub plays a crucial, albeit to the user transparent, role in the data flow (Fig. 4).

The SAML2 authentication request scoping element

The SAML2 'authentication request scoping element' is intended for use in proxy-IdP-environments like hub-and-spoke federations.

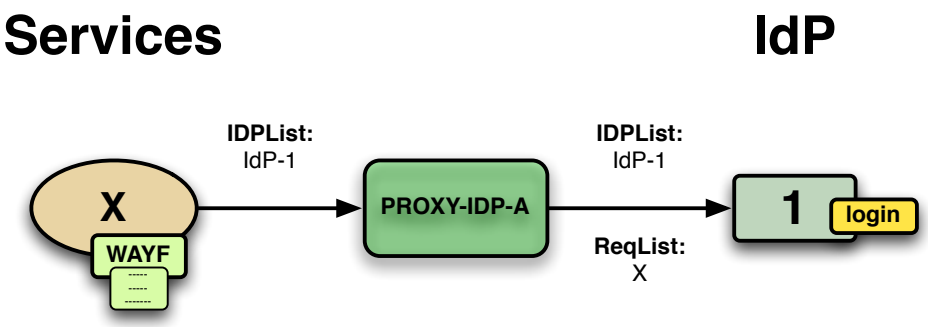

Fig. 4. Single proxy-IdP configuration, path definition by IDPList, path trail provided by RequesterList elements.

The scoped authentication request is generated by the service provider, and tells which IdP to authenticate the user at. The part of the scoping element listing the name of the IdP is called the IDPList (see Fig. 4 and Fig. 6). For use in n-tier-proxy configurations it is possible to express lists of proxies to pass. The IDPList is ordered and may thus express paths in multi-proxy environments (see Fig. 5).

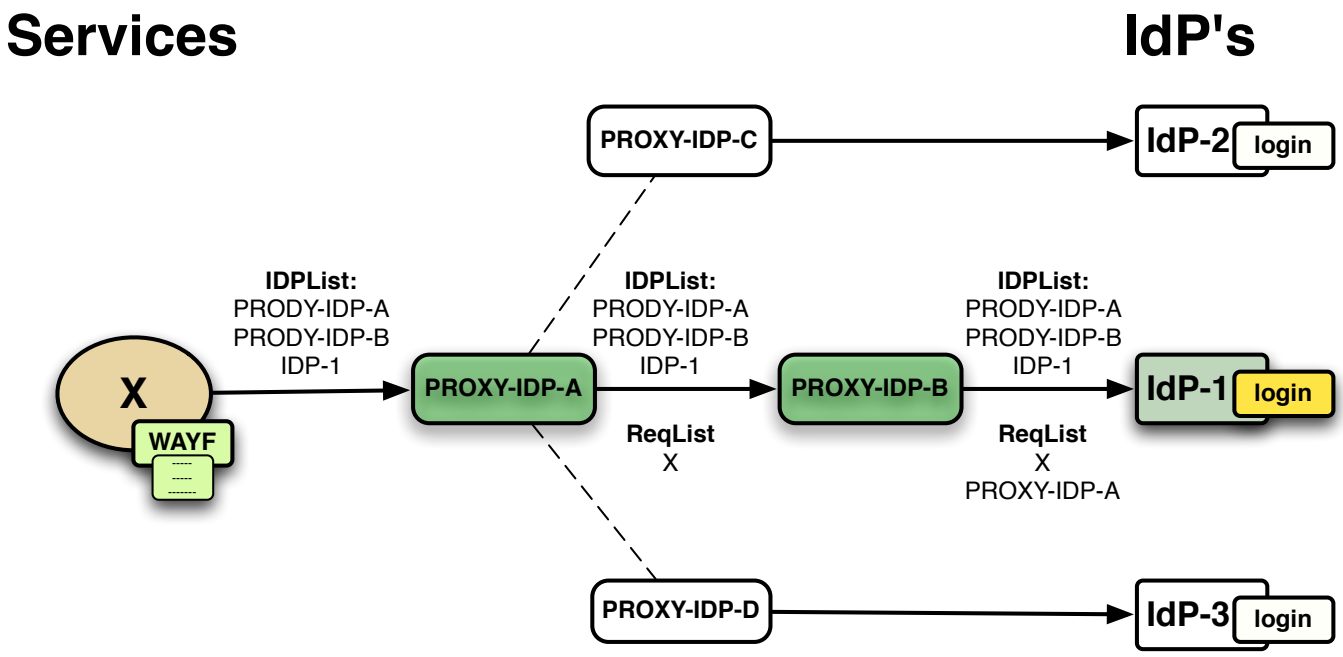

Fig. 5. N-tier-proxy-IdP configuration, path definition by IDPList, growing path trail provided by RequesterList elements.

```
<samlp:Scoping ProxyCount="2">
   <samlp:IDPList>
      <samlp:IDPEntry ProviderID="https://www.idp1.dk" Name="Identity Provider 1" Loc="https://www.idp1.dk/source">
      <samlp:GetComplete>https://wayf.sp2.dk/IDPList</samlp:GetComplete>
   </samlp:IDPList>
   <samlp:RequesterID>https://wayf.sp1.dk </samlp:RequesterID>
</samlp:Scoping>
```

Fig. 6. SAML2 authentication scoping element, XML format

The scoped SAML2 authentication request is issued by the service provider. The proxy-IdP in turn generates a new request for the IdP listed first in the IdP-list. To the new request is appended information about which entity the request was received from. This is listed in the field called 'RequesterID' which reflects the path traversed towards the endpoint (see Fig. 4). The RequesterID reveals who the originating service provider was, information which might be useful for accounting purposes etc.

Handling SAML2 scoping element is optional, so any receiver of scoped authentication requests may ignore them. This provides on one hand side flexibility when designing user interaction but may also introduce uncertainty about consistency of user experience if systems get complex, i.e. when interconnecting federations.

The 'ProxyCount' of the scoping element and is decremented for each hop in any given proxy-chain. ProxyCount must never be negative which means that the service provider may decide how many hops in proxy chain are acceptable. The new authentication request must contain a ProxyCount attribute with a value of at most one less than the original value. A count of zero permits no proxying, while omitting this field expresses no restrictions.

The 'Name' field of the scoping element describes a human readable name for the IdP as opposed to the IDPEntry ProviderID which typically is a url. The Name field is optional.

'Loc' is a URI reference representing the location of a profile-specific endpoint supporting the authentication request protocol. The binding to be used must be understood from the profile of use. This enables any authentication mechanism, at any URI to be used, if trusted by the IdP.

Transparent federation session initiated by local single-sign-on system

Local single-sign-systems let users operate seamlessly within a local security domain. As soon as the user accesses an external service, (s)he is prompted to authenticate. Still more institutions buy or share external services which is why an extension of the single-sign-on domain, from a usability point of view, would be preferable. Federated access management of external services allows for more coherent and personalised service portfolios.

Using scoped SAML2 authentication requests, local web based single-sign-on systems, acting as federated service providers, may transparently initiate browser sessions between the federations' proxy-IdP and the users' browser as part of the login flow at the local single-sign-on system. This is done by letting the single-sign-on system send a scoped SAML2 authentication request through the central federation system, to the IdP of the same institution. This establishes a browser session with the central federation system. Later, when services in the 'external' domain send authentication requests, the users' browser will be polled for existing sessions with the federation's proxy-IdP. As a session with the federation is already available, authorisation information about the user, originating from the IdP where the local single-sign-on login was performed, will be made available to the service.

Local link collections, learning management systems etc. can now be made equally available to the user - weather placed inside or outside the local security domain.

Support for federations-in-federations

Scoped SAML2 authentication elements may be used to interconnect federations like loosely coupled federations (Fig. 2) and hub-and-spoke federations (Fig. 3) in configurations like the one shown in Fig. 7. Alternatively several hub-and-spoke federations may be combined as shown in Fig. 8.

Several federation operators are considering models for helping smaller institutions to connect to the federation. One solution would be a model where institutions have user data bases hosted as a service (the 'Hub' in Fig. 7) which in turn is connected to the federation. Each hosted solution will appear on the federations' list of connected institutions - but when chosen in the wayf, the relevant IdP-installation will be contacted using authentication scoping elements.

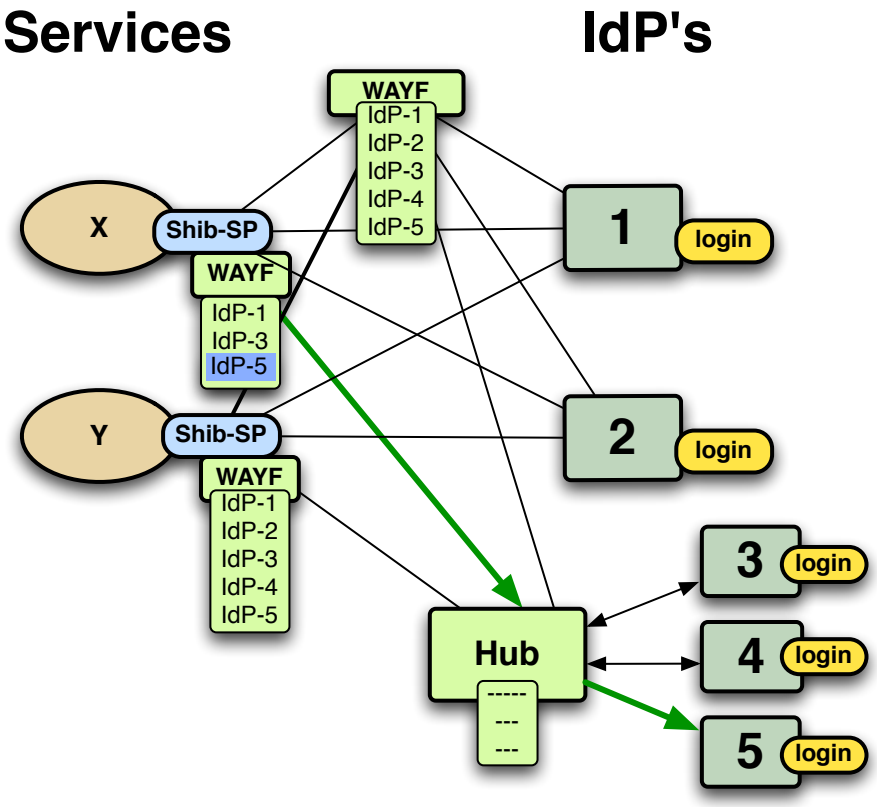

Fig. 7. SAML2 scoping used in federation setup of a loosely coupled federation combined with a hub-and-spoke federation

If two hub-and-spoke architectures are interconnected (Fig. 8), a service may send 2-tier scoped SAML2 authentication requests as mentioned above. Hub-1 (Fig. 8) will only be able to look up the endpoint of one of the two entities in the IDPList in its' metadata, namely Hub-2 which is directly connected to Hub-1. All other entries in the IDPList are ignored. Hence the request is passed on to this entity, which is also only able to look up one of the two scopes in its' metadata of connected IDP's (please note that the federation hub acts as service provider to the hosting IdP) and therefore pass on the request to the login system of the relevant IdP.

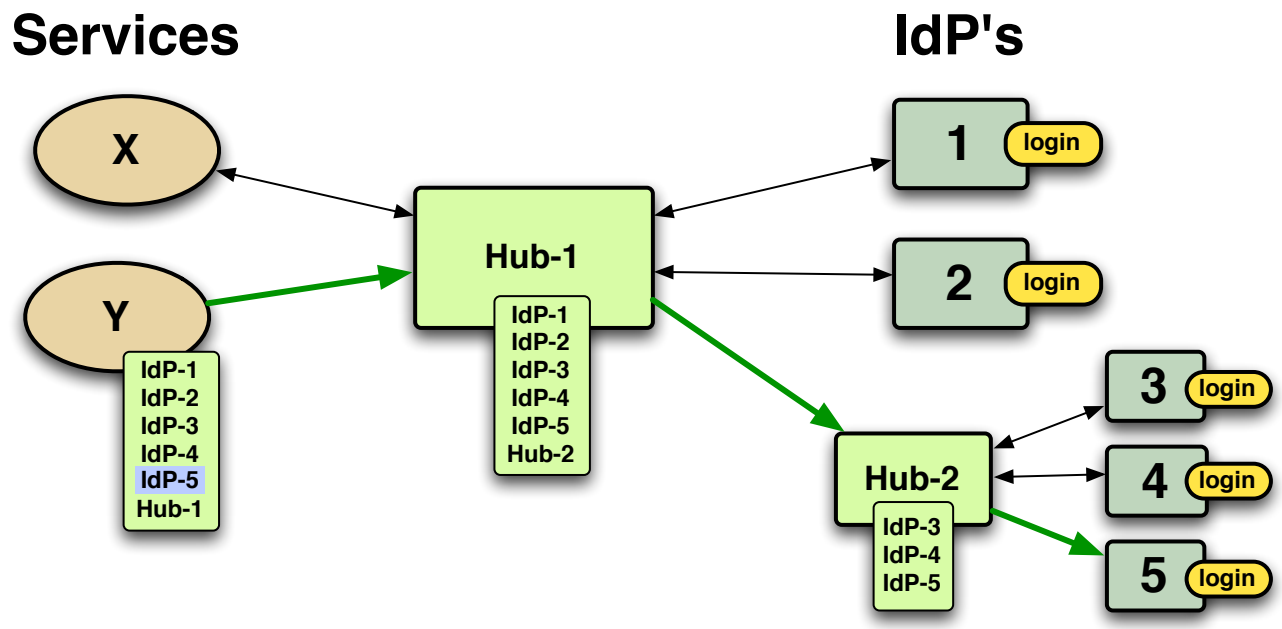

Fig. 8. SAML2 scoping used in federation setup of two interconnected hub-and-spoke federations.

Conclusion

The Danish federation (WAYF - Where Are You From) has implemented support for SAML2 authentication scoping elements in the software package simpleSAMLphp. This enables services to build decentral IdP-discovery services, which until now has not been technically possible in hub-and-spoke federations based solely on SAML2. Scoping elements may be of use for accounting in hub-and-spoke federations where the name of the originating service provider can now be known by the IdP (in stead of only knowing that the authentication request came from the federations' proxy-IdP).

SAML2 scoping elements allow for the interconnection of various federation architectures - loosely coupled (i.e. Shibboleth) and hub-and-spoke. This opens the door for new IdP-hosting models in loosely coupled federations where hosted IdP's may be listed as independant entities even when being part of a IdP-cluster or 'IdP-orphanage'.

As SAML2 authentication scoping elements are not yet supported by other software packages than simpleSAMLphp, the interconnection of different federations have still not been tested. Still it seems obvious to do in scenarios where service providers in loosely coupled federations have relations with only a subset of the IdP's in a hub-and-spoke federation.

Future applications of SAML2 authentication scoping elements may be front channel attrubute collection of attributes from multiple IdP's based on authentication requests - a prototype named Corto[7] is made available. Also transparent extention of local single-sign-on systems with intire federation domains can be achieved by using scoped authentication request as part of the login procedure of the local single-sign-on system.

Vitae

David Simonsen: M.Sc. Working at the WAYF secretariat since 2005, former co-chair of TF-mobility, former member of the Governments' IT council, and the advisory board of the Danish Virtual University. Email: david@wayf.dk. Address: The WAYF secretariat, H.C. Andersens Boulevard 2, DK-1553, Denmark

Jacob-Steen Madsen: M.Sc. Working at the WAYF secretariat since 2007, former head of development of University of Southern Denmark and former member of the national XML standardisation body.

Mads Freek Petersen: Developer at WAYF, developer at University of Roskilde.

Jacob Christiansen: M.Sc. Developer at WAYF.

References

[1] simpleSAMLphp, http://simplesamlphp.org/

[2] Shibboleth, http://shibboleth.internet2.edu

[3] Simonsen et al., 2009: Trusted third party based ID federation, lowering the bar for connecting and enhancing privacy

[4] SAML2 specifications, http://saml.xml.org/saml-specifications

[5] Simonsen et al, 2010: Enhancement of the graphical user interface of WAYF - Where Are You From, http://wayf.dk/wayfweb/artikler_og_notater_attchmt/2010_04_26_WAYF-usability_Fraunhofer.pdf

[6] The Danish federation WAYF - Where Are You From (http://www.wayf.dk)

[7] Corto, attribute collector prototype, http://code.google.com/p/corto/