Pre-select organization

Bypassing Feide's Discovery Service

Document History

Version	Date	Author	Comments
1.1	Aug 2016	Jaime Pérez	Added "requirements notation" section. Added "security considerations" section. The entity ID of the service is now required to allow redirections.
1.0	Mar 2015	Jaime Pérez	First version of this document.

UNINETT AS

Abels gate 5 – Teknobyen
P.O. Box: NO-7465 Trondheim
Sør-Trøndelag, Norway

+47 73 55 79 00
support@feide.no

Introduction

When a user tries to login into a service for the first time with Feide, the Identity Federation of the Norwegian Research and Education Network (UNINETT), he or she will normally need to select a home organization, that is, the organization he or she belongs to. In large identity federations like Feide this could quickly become a usability issue, since users would need to choose from a potentially long list of different organizations.

For service providers who offer customized services to their customers, it is reasonable to assume they would be able to identify the organization a user would need to authenticate with in order to access a specific service. Some services already implement their own Discovery Service, and others are provided by the organizations themselves and targeted exclusively to their own users. Both scenarios are typical in an identity federation, and therefore Feide provides a mechanism to avoid the extra step of selecting the home organization by pre-selecting it before asking for authentication.

This document describes that mechanism, and suggests several ways to leverage it to enhance the usability of Feide.

Requirements notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC 2119].

The use of SHOULD, SHOULD NOT, and RECOMMENDED reflects broad consensus on deployment practices intended to foster both interoperability and guarantees of security and confidentiality needed to satisfy the requirements of many organizations that engage in the use of federated identity. Deviating may limit a deployment's ability to

technically interoperate without additional negotiation, and should be undertaken with caution.

Technical specification

Feide uses a *cookie* in the user's web browser to remember the organization he or she belongs to, in order to skip the Discovery Service and enhance the usability of the system. This cookie contains the *realm* of the organization or its main domain name, which will always be the same as the one present in the `eduPersonPrincipalName` or `schacHomeOrganization` attributes, as well as in any other scoped attribute. When a user reaches Feide's Discovery Service for the first time, there will be no such cookie, so a form to select his or her home organization will be displayed. Upon selection, this cookie will be set, allowing Feide to skip this step in future authentication requests for the same user.

However, cookies can only be set for the current domain. This means nobody can set this cookie for Feide, except Feide itself. In order to allow service providers to set this cookie on their own for their users, Feide provides a pre-selection interface where they can redirect them, and it is available here:

```
https://idp.feide.no/simplesaml/module.php/feide/preselectOrg.php
```

The pre-selection interface takes three parameters:

- `HomeOrg`: contains the realm or domain of the organization that we want to pre-select for the user.
- `ReturnTo`: a percent-encoded, fully-qualified URL [RFC 3986] where we want to redirect the user to after successfully setting the cookie.
- `entityID`: a percent-encoded URI [RFC 3986] identifying univocally the service requesting pre-selection. This entityID MUST match the one registered in the service's SAML metadata exchanged with Feide.

Depending on how the service provider knows on beforehand the organization a user belongs to, there's several ways to call this interface to pre-select the organization.

Own Discovery Service

If the service provider already implements its own Discovery Service, allowing the user to select among several organizations, it is possible to pre-select them in Feide by redirecting to this interface before triggering authentication at the service provider. Let's assume the Discovery Service is implemented by redirecting to distinct URLs depending on the option selected by the user. Pre-selection can then be achieved by redirecting to this interface instead of the specific URLs, which will then be passed inside the `ReturnTo` argument to initiate the login procedure after pre-selection.

For example, if our custom Discovery Service allows two different organizations, those being `uninett.no` and `feide.no`, and our service have URLs like the following to trigger authentication:

```
http://www.example.com/feide
```

We can then design our Discovery Service with two different options, which redirect to the following URLs when chosen by the user:

```
https://idp.feide.no/simplesaml/module.php/feide/preselectOrg.php?
HomeOrg=uninett.no&ReturnTo=http%3A%2F%2Fwww.example.org%2Ffeide

https://idp.feide.no/simplesaml/module.php/feide/preselectOrg.php?
HomeOrg=feide.no&ReturnTo=http%3A%2F%2Fwww.example.org%2Ffeide
```

Now, once the user selects one of the two options, he or she will be redirected to the pre-selection interface, effectively setting the home organization corresponding to the option chosen, and will be back to the service provider where authentication will be triggered immediately.

Organization-specific services

For those services that are targeted to a certain organization, there's no need for the user to select the organization in Feide's Discovery Service, since only the users of that organization will be using it. In this case, pre-selection can be done unconditionally without the user selecting the organization at all.

Let's assume a web page offering services targeted to the organization whose realm is `uninett.no`. In this case, we can unconditionally redirect to the pre-selection interface with the URL that triggers authentication and the fixed realm.

If we cannot change the links in the web page to point to the pre-selection interface, but we can change the page that triggers authentication, we can make it redirect to the interface for the first time it is accessed, and pass its own URL as a parameter to the pre-selection interface. Note that in this case, the page that triggers authentication MUST have a way to identify that pre-selection has already been done in order to avoid creating infinite redirection loops. This can be achieved by either setting a specific cookie, saving some information in the session of the user, or adding a parameter to the current URL. Then, every time we load the page that triggers authentication, the cookie, session or URL parameter can be checked, and pre-selection will only be initiated if missing.

Security considerations

Given that the pre-selection interface allows service providers to get the user redirected to a URL specified as a parameter, malicious links could be crafted to exploit an open redirection attack vector [CWE 601]. This facilitates phishing, and enables attackers to pass URLs that look legitimate to their victims, fooling them to give away personal data or even their credentials. This is specially critical for a login service such as Feide, so appropriate mitigations have been taken to allow redirections only to known URLs.

By default, Feide will trust no `ReturnTo` parameters. Only those fully-qualified URLs that have been previously registered will be allowed by the interface. The query parameters of the URL are the only part of it that may change without previous registration, allowing service providers to change the target of the redirection dynamically by changing those. If a large amount of different URLs may be used in the pre-selection interface, a suggested alternative would be a single, canonical URL keeping a table mapping a query parameter to the original target URL, and performing the final redirection.

A self-service interface will be implemented inside of the Feide Customer Portal in order to register new URLs. Meanwhile, until that interface is available, contact Feide to register any URL you may want to use with the pre-selection interface.

References

[RFC 3986] T. Berners-Lee et al, *Uniform Resource Identifier (URI): Generic Syntax*, Jan. 2005, section 2.4; https://tools.ietf.org/html/ 3986

[CWE 601] E. Dalci et al, *CWE-601: URL Redirection to Untrusted Site ('Open Redirect')*, Dec. 2015; https://cwe.mitre.org/data/definitions/601.html