UNINETT

Feide Integration Guide

Technical Requisites

Document History

Version	Date	Author	Comments
1.2	Mar 2016	Jaime Pérez	Stop requiring support for Single Logout.
1.1	Apr 2015	Jaime Pérez	Allow the use of the HTTP-POST binding.
1.0	Oct 2014	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

This document lists the technical requisites needed to connect as a Service Provider to Feide, the Identity Federation of the Norwegian National Research and Education Network (UNINETT).

Feide uses the *Security Assertion Markup Language version 2.0* [SAMLCore] and supports the *Interoperable SAML 2.0 Web Browser SSO Deployment Profile* [SAML2Int]. For more detailed information about integration with Feide as well as technical details for the integration, please refer to the *Feide Integration Guide* [FeideInt] and the *Feide Technical Guide* [FeideTech], respectively.

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 requisites

Here is the list of technical requisites that all Service Providers must meet in order to connect to Feide. You can use it as a checklist to verify that you comply with all the requirements and therefore you are ready to proceed with integration.

SAML 2.0 Web SSO Profile

Feide uses the *Web Browser SSO Profile* defined by SAML 2.0 [SAMLProf]. When implementing this profile, Service Providers MUST support the use of the following bindings:

- The *HTTP Redirect* or the *HTTP POST* bindings for sending *Authentication Requests* to Feide. Note that the *HTTP Redirect* binding is RECOMMENDED.
- The *HTTP POST* binding for receiving *Authentication Responses* from Feide.

Additionally, Service Providers MUST support the following authentication flows:

- The Service Provider MUST be able to send an *Authentication Request* to Feide when a user requests authentication, and consume the *Authentication Response* received upon successful authentication, commonly known as *SP-initiated authentication*.
- The Service Provider MUST be able to consume an unsolicited *Authentication Response* received from Feide, commonly known as *IdP-initiated authentication*.

SAML 2.0 Single Logout Profile

Full support of the *Single Logout profile* [SAMLProf] is RECOMMENDED in Feide. Service Providers SHOULD be able to:

- Send *Logout Requests* to Feide when a user initiates logout at the Service Provider.
- Receive *Logout Requests* and proceed accordingly, by terminating the session of the current user and replying with a *Logout Response* to Feide.
- Send and receive the aforementioned messages using the *HTTP Redirect* or *HTTP POST* bindings. Note that the *HTTP Redirect* binding is RECOMMENDED.

Identification of users

Service Providers MAY support the univocal and persistent identification of single users based on their attributes[1]. In particular, Service Providers MUST:

- Avoid the use of *name identifiers* as an identifier of a user. Feide uses *transient* name identifiers that change every session and therefore are not suitable for persistent identification.

Attribute format

Service Providers MUST support the following attribute name format [SAMLCore]:

- Basic, identified with the URI:
  `urn:oasis:names:tc:SAML:2.0:attrname-format:basic`

Identification of Norwegian organizations

Service Providers willing to perform authorization based on the home organization of the user, SHOULD identify the organization by means of one of the following:

- The *eduPersonOrgDN:norEduOrgNIN*[2] attribute, or
- The *realm* part of the *eduPersonPrincipalName*[3] attribute.

For those Service Providers that need a finer granularity to identify primary and secondary schools, the previous attributes can be used in addition to the following:

- The *feideSchoolList*[4] attribute, which holds the list of schools associated with the user.

Additionally, Service Providers identifying Norwegian organizations MUST:

- Avoid using Feide's *entity ID* to identify an organization, since Feide is a federation with one single SAML Identity Provider that provides service for all Norwegian institutions.

Secure web transport

[1] See Feide's attribute list for more information: https://www.feide.no/attributelist
[2] See the definition of the *eduPersonOrgDN:norEduOrgNIN* attribute for more information: https://www.feide.no/attribute/edupersonorgdn-noreduorgnin
[3] See the definition of the *eduPersonPrincipalName* attribute for more information: https://www.feide.no/attribute/edupersonprincipalname
[4] See the definition of the *feideSchoolList* attribute for more information: https://www.feide.no/attribute/feideschoollist

To ensure the security and privacy of Feide users, and avoid security warnings displayed by web browsers when logging in to Feide, Service Providers MUST:

- Support *HTTPS* on all the SAML URLs used to communicate with Feide.
- Support security protocols (TLS) and mechanisms (certificates signed by well-known certification authorities) compatible with most modern web browsers.

References

[RFC 2119] S. Bradner, *Key words for use in RFCs to Indicate Requirement Levels*, IETF RFC 2119, March 1997;
https://www.rfc-editor.org/rfc/rfc2119.txt

[SAMLCore] *Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V2.0*, OASIS standard, 15 Mar. 2005.

[SAMLBind] *Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0*, OASIS standard, 15 Mar. 2005.

[SAMLProf] *Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0*, OASIS standard, 15 Mar. 2005.

[SAML2Int] *Interoperable SAML 2.0 Web Browser SSO Deployment Profile*,
http://saml2int.org/profile/current

[FeideInt] *Feide Integration Guide*, Jan. 2014;
https://www.feide.no/sites/feide.no/files/documents/feide_system_architecture.pdf

[FeideTech] *Feide Technical Guide*, Sep. 2014;
https://www.feide.no/sites/feide.no/files/documents/Feide_technical_guide.pdf