



08-04-2010

Deliverable DJ3.2.1,1: Identity Federations



Deliverable DJ3.2.1,1

Contractual Date: 28-02-2010

Actual Date: 08-04-2010

Grant Agreement No.: 238875

Activity: JRA3

Task Item: T2

Nature of Deliverable: R (Report)

Dissemination Level: PU (Public)

Lead Partner: NORDUNET/UNINETT

Document Code: GN3-10-039

Authors: A. Solberg (NORDUNET/UNINETT), L. Florio (TERENA), D. Simonsen (WAYF), L. Haemmerle (SWITCH), T. Lenggenhager (SWITCH), T. Kersting (DFN), I. Thomson (DANTE), W. Singer (DANTE)

Abstract

This deliverable describes the work undertaken so far in GN3 JRA3 Task 2, "Identity Federations". It describes the sub-tasks within the Task, the approaches taken, the results so far, and work planned for the future.

Table of Contents

Executive Summary	1
1 Introduction	4
1.1 Collaboration with GÉANT SA3 eduGAIN	6
2 Sub-Task I: Virtual Organisations	7
2.1 Virtual Organisation Management	8
2.1.1 Preliminary Result 1: SWITCH Group Management Tool (GMT)	9
2.1.2 Preliminary Result 2: SimpleSAMLphp VO Management Module	10
2.2 SP-Centric Attribute Aggregation	11
2.2.1 General Aspects about Attribute Retrieval	12
2.2.2 Alternative Attribute Retrieval Protocols	12
2.2.3 Preliminary Result 3: Proof of Concept: Shibboleth, GMT and SAML 2.0 Attribute Queries	15
2.2.4 Preliminary Result 4: Draft specification: OAuth Attribute Query Protocol	17
2.2.5 Preliminary Result 5: Proof of concept: SimpleSAMLphp and OAuth Attribute Retrieval	17
2.2.6 Preliminary Result 6: Implementation of SpringFika	19
3 Sub-Task II: Metadata Distribution	22
3.1.1 Preliminary Result 7: Simple Metadata Aggregation Profile	22
3.1.2 Preliminary Result 8: Cross-Federation Technical Test Pilot	23
3.1.3 Preliminary Result 9: SimpleSAMLphp Metadata Aggregator	25
3.1.4 Preliminary Result 10: Metadata Aggregator Specification	25
4 Sub-Task III: Federation Harmonisation	27
4.1 Interoperable SAML 2.0 Web Browser SSO Deployment Profile	27
4.2 Deprovisioning	28
4.3 Logout in Federations	28
4.3.1 Different Logout Options	29
4.3.2 The Feide Solution to SLO	31
5 Sub-Task IV: User-Centric Identity	33
5.1 User-Centric Identity in European Identity Federations	33

5.2	OpenID Federations	36
6	Sub-Task V: Beyond Web-SSO	37
6.1	Preliminary Result 11: Beyond WebSSO using OAuth - Implementation in SimpleSAMLphp	37
6.2	Preliminary Result 12: SimpleSAMLphp Translation Portal – Use-Case of Command Line Authentication	39
6.3	Utilisation Outside the Task	39
7	Sub-Task VI: Federation Lab	41
8	Future Work and Conclusions	42
8.1	Real-Life adoption of VO Technology	43
8.1.1	Virtual Organisation Use-Case: TERENA Wiki	43
8.1.2	Virtual Organisation Use-Case: CLARIN	43
9	References	45
	Glossary	47

Table of Figures

Figure 1.1:	Identity Federation sub-tasks	5
Figure 2.2:	Virtual Organisation structure	8
Figure 2.3:	Management of group members in a VO using the GMT	10
Figure 2.4:	SimpleSAMLphp VO module	11
Figure 2.5:	Example management of a VO	18
Figure 2.6:	SpringFika workflow	21
Figure 3.7:	National federation metadata aggregation	23
Figure 3.8:	Entities on the central aggregator during testing	24
Figure 4.9:	Feide SLO interface	32
Figure 5.10:	Similarities and differences between the three approaches	35
Figure 6.11:	Popularity of OAuth during the last few years	38
Figure 6.12:	Demo-case components	38
Figure 6.13:	OAuth Client interface	39

Executive Summary

The ultimate goal of the Identity Federations task is to enable users of one domain to securely access data or systems of another domain seamlessly, without the need for redundant user administration.

Identity Federations (or Federations) are based upon the principle that a user's authentication is undertaken by their home organisation (their Identity Provider, or IdP), and that a resource (a Service Provider, or SP) trusts what the home organisation states about the user.

The GN3 JRA3 Task 2 “Identity Federations” aims to research different aspects of this field, to improve the inter-operability among federations in the Research and Education community and to support collaborative communities. It also aims to support new federation use-cases in order to expand the deployment of the federated framework.

The task is divided into six sub-tasks:

- Virtual Organisations
- Metadata distribution
- Federation Harmonisation
- User-centric Identity
- Beyond Web-SSO
- Federation Lab.

This deliverable describes the work undertaken in this task so far, providing details of the progress and conclusions made in each sub-task, and also reports on new use-cases that have been analysed in the community.

Three sub-tasks were given a higher priority during the first year of the project: “Virtual Organisations”, “Metadata Distribution” and “Federations Harmonisation”. This was a strategic decision, influenced by the need to better support the work carried out in SA3, particularly in eduGAIN.

A short summary of the work done in each of the sub-tasks is provided below.

- Virtual Organisations

Significant work has been carried out in the area of user attribute retrieval and aggregation, which is an important component of a Virtual Organisation Platform (VOP). A VOP is a technical infrastructure that allows

collaborative projects, spanning across multiple federations and institutions, to provide user data, which is then used for authorisation purposes and synchronised across multiple services.

Two different proof-of-concepts have been tested for providing a Virtual Organisation Platform that enables collaboration across multiple federations and services. These proof of concepts have shown that it is possible to implement a Virtual Organisation Platform using neutral and open standards. During the work it became clear that there are several alternative approaches to implementing a working Virtual Organisation Platform.

A new model of retrieving users' attributes, called Service Provider (SP)-centric, has been explored and is detailed in this document. This model is based on the assumption that the SP would be able to retrieve additional data from a third party without involving the user's IdP. The SP-centric approach offers more scalability, which is an important feature in inter-federation scenarios. Several protocols are proposed for implementing SP-centric attribute aggregation. A more in-depth analysis of the different approaches will take place during Year 2 of the project.

- Metadata distribution

Metadata contains information about entities participating in Identity Federations. The way in which metadata is aggregated and exchanged among various parties in an inter-federation scenario has been studied. In particular, the group has started to investigate how to move from a centralised metadata aggregation architecture (less scalable in the long term) to a more distributed architecture. Since the way in which metadata is gathered and exchanged has implication for the eduGAIN design, work in this area has been performed in close cooperation with SA3 eduGAIN.

A cross-federation test environment has been set up, configured and tested, using real services. This distribution approach is based on a central model with metadata aggregators. The test environment was successful. This approach is already being used in production in some cross-federations (such as the Kalmar Union). It is expected, however, that in the longer term more distributed and alternative models for distribution metadata will be used. Work with new and alternative models for metadata distribution will be carried out over the next few years, and the results will be provided to SA3 eduGAIN for evaluation.

- Federation Harmonisation

This task looks at creating guidelines to help identity federation operators make implementation choices that will not impact on interoperability. One of the main achievements in this area was the consolidation of the "Interoperable SAML 2.0 Web Browser SSO Deployment Profile" (see [\[saml2int1\]](#)), which defines a minimum set of bindings and rules to facilitate interoperability. This profile is gaining interest. It is important to promote the profile, to ensure that the higher education community adopts as few conflicting profiles as possible.

- User-centric Identity

A document on user-centric identity has been written. It provides a useful introduction to user-centric identity and how it can be used in identity federations. This work will be valuable to many federations that need more knowledge and experience of the new identity paradigm.

- Beyond Web-SSO

A proof of concept implementation of authentication beyond Web-SSO has been successfully implemented using OAuth (to reuse the web session). This approach has been adopted in real services, such as Confusa in 2010, and is likely to be adopted by others. Focus in the coming years will be on finding more and better ways

of providing federated authentication to applications that are not web-based, as well as improving communication between web services.

- Federation Lab

Work on federation lab was not started during the first year due to the priority assigned to other sub-tasks and because this work relies heavily on the output from the federation harmonisation sub-task.

1 Introduction

This deliverable describes the work carried out in Year 1 by JRA3 Task 2 “Identity Federations”. It describes the six sub-tasks that make up Task 2, their purpose and function, and what they have achieved.

Identity Federations (or Federations) are based upon the principle that a user's authentication is undertaken by their home organisation (their Identity Provider, or IdP), and that a resource (a Service Provider, or SP) trusts what the home organisation states about that user.

A user is typically characterised by identity information (attributes) that is exchanged between the user's home organisation and the service the user requests. The service uses the information received from the user's home organisation in combination with other information (for example user ID and password) known about the user to authorise access.

The most common use-case addressed by federations is the scenario where a user requests access to a resource website using a web browser. In this case the user is redirected to his/her identity federation page to authenticate. If the authentication succeeds, information about the user (attributes) and the result of the authentication are passed to the service for authorisation purposes. This process is transparent to users, who are only asked to enter their credentials (typically username and password).

However, there are an increasing number of use-cases where the client does not always use a web browser. These use-cases require a more complex authentication model, which is not fully available at the moment.

In the educational community, users belonging to different organisations often collaborate on research projects (e.g. GN3). These researchers create collaborative communities that span over different administrative domains. In these collaborative communities, the same users can have different roles. Currently there is no well-defined way of providing cross-organisation project-specific user and authorisation data.

There are different ways in which federations coexist and interact within the same country, or among different countries. The "classical" inter-federation scenario is one in which users trust their IdP, which establishes relationships with one or more SPs. However, new use-cases have emerged that require new models. For instance, in the case of eduroam (which provides seamless access to the network) different federations (the national eduroam federations) agreed to share common policies to address the use-case of international roaming. The eduroam model is called “confederations”. In other cases, where a central policy might not be needed, federations might decide to inter-operate in a less formal fashion, following an inter-federation model.

All these new models of interaction require the development of new features to support a combination of different authentication methods, authorisation mechanisms and levels of assurances. A key factor in such an environment is how federations can exchange the data that defines each of them (metadata) in a way that preserves security and trust.

New models for dealing with electronic identities (such as the user-centric model) and new ways of implementing protocols to preserve user privacy offer new opportunities to extend the initial federated framework built by the NRENs.

The JRA3 Task 2 “Identity Federations” aims to research the different aspects mentioned above to aid interoperability among federations in the Research and Education community, and to support collaborative communities.

The Identity Federation task also aims to support new federation use-cases that expand the deployment of the federated framework.

The Identity Federation task covers six largely independent sub-tasks described in this document within the field of Identity Management as depicted in Figure 1.1, namely:

- Virtual Organisations
- Metadata distribution
- Federation Harmonisation
- User-centric Identity
- Beyond Web-SSO
- Federation Lab.

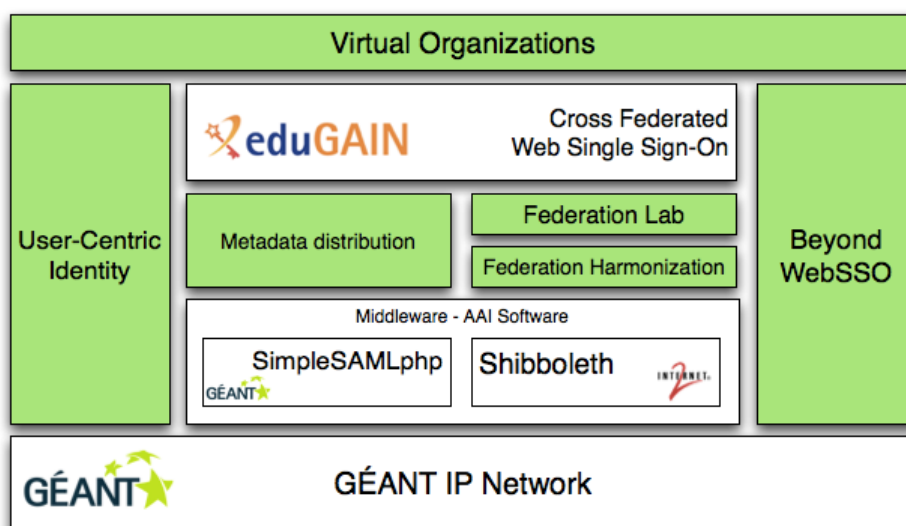


Figure 1.1: Identity Federation sub-tasks

The green elements in Figure 1.1 belong to the Identity Federation task. Figure 1.1 also depicts how the Identity Federation task builds on existing technologies such as SimpleSAMLphp [[SimpleSAMLphp](#)] and Shibboleth [[Shibboleth](#)] and how it relates to SA3-eduGAIN [[edugain](#)].

1.1 Collaboration with GÉANT SA3 eduGAIN

The JRA3 Task 2 collaborates closely with SA3-eduGAIN. eduGAIN aims to define and implement the framework for interconnecting the various Identity Federations in Europe, and to enable controlled access to GÉANT and NREN services and resources via identities asserted by those federations.

In particular, two sub-tasks are relevant to eduGAIN:

- Metadata distribution
- Federation Harmonisation.

These two sub-tasks form the core technical foundation for building a cross-federation environment. Task 2 also aims to ensure that the eduGAIN platform does not restrict the future addition of more sophisticated Identity services to the existing infrastructure.

Some of the sub-tasks in Task 2 rely on an existing cross-federated WebSSO layer, and hence depends on an infrastructure such as eduGAIN. In particular, this is the case for the Virtual Organisations sub-task.

Based on these shared goals and interests, a cross-activity technical working group has been established to discuss the current and future technical core foundation of the GN3 SA3 eduGAIN project. This working group consists of a subset of members of the two tasks, and involves regular meetings.

As a consequence of this collaboration, the two sub-tasks (Metadata Distribution and Federation Harmonisation) that directly relate to eduGAIN have been assigned high priority. Significant effort has been put into these sub-tasks in the first year of the project.

2 Sub-Task I: Virtual Organisations

Current identity federation architectures feature identity providers and service providers. Typically, each institution operates an identity provider. The identity provider takes care of authentication and provides authentication information as well as additional data about the user to the service provider.

Users from educational institutions often collaborate with partners from other institutions. This task aims at developing the identity architecture to better support such collaboration. There is not yet a well-defined way of providing cross-service project-specific user and authorisation data for a collaboration group that spans multiple institutions and national federations.

To aid this, we have introduced the concept of a Virtual Organisation Platform (VOP). This is a technical infrastructure that allows collaboration projects which span across multiple federations and institutions. The VOP provides authorisation and additional user data, and synchronises this information across multiple services. However, the data is maintained and stored in a single place.

Collaboration projects can use the Virtual Organisation Platform to establish a Virtual Organisation (VO). A VO is a group of individuals that have something in common and who collaborate using online tools. For example, this could be a group of international researchers working together on a large research project, such as GÉANT. Virtual Organisations can span across multiple organisations, federations and countries. The VOP contains lists of users and optionally additional user data associated with a specific user for a specific VO.

The ambition is that the VO Platform would simplify the collaboration process, as illustrated in the following scenario: a teacher in Norway invites a professor from Spain and a researcher from Croatia to join a VO. They set up a wiki (e.g. using Feide OpenWiki) where all participants in the VO have write access. The Croatian researcher has access to a local easy-to-use project file-sharing service, and, with a few operations, grants access to all VO members. The group decides to make use of two or three additional web-based collaboration tools. When a new member is added to the group, he or she automatically gains the access privileges assigned to members of that group.

When approaching realisation of a VO Platform we have identified two independent logical components:

- Virtual Organisation Management
- SP-Centric Attribute Aggregation.

Figure 2.2 illustrates this structure.

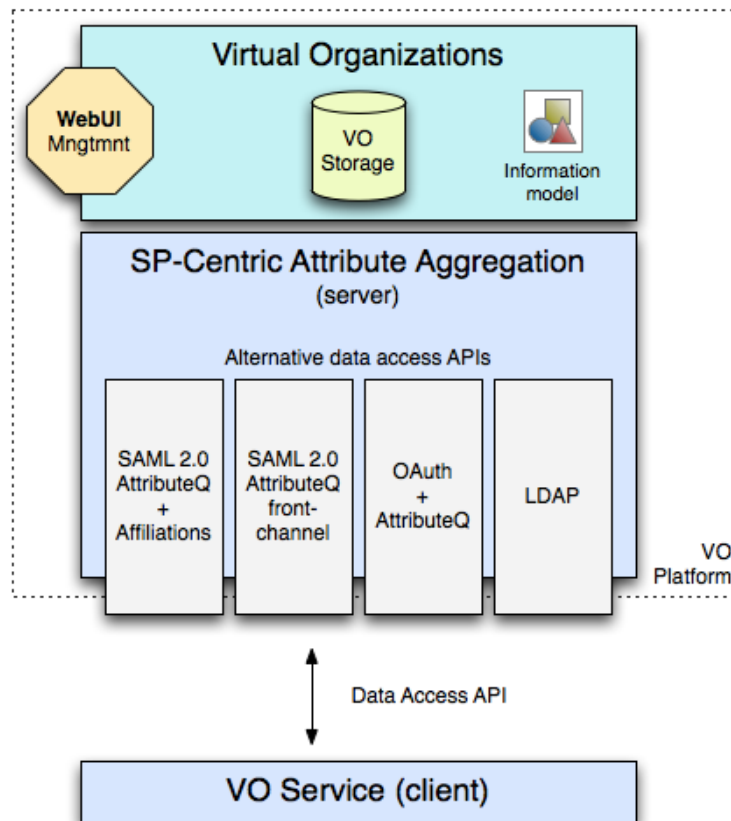


Figure 2.2: Virtual Organisation structure

Virtual Organisation Management includes a web-based user interface for creating and managing VOs as well as the user attributes associated with a VO. This information is collected in a VO storage facility, which preferably has a well-known access interface, such as SQL or LDAP.

SP-Centric Attribute Aggregation allows Service Providers to access information about users from sources other than the established identity provider. SP-Centric means that the retrieval of attributes (user data) is initiated by the service provider, and there is not necessarily any relationship between the identity provider and the attribute authority. For more information on these concepts, see [\[Virtual Organisations\]](#).

2.1 Virtual Organisation Management

Virtual Organisation Management Software already partly exists. Most of the available software has a limited scope, such as in-campus or one federation. Our goal is to ensure that generic software is available which can be used in a cross-federated environment and combined with any of the proposed SP-Centric Attribute Aggregation Data Access APIs, as described later in this document.

Two Virtual Organisation Management software solutions have already been considered for use with cross-federations. They will be used as important components in the future VO proof of concept. These are:

- SWITCH GMT
- SimpleSAMLphp VO Management Module. [[SimpleSAMLphp](#)].

2.1.1 Preliminary Result 1: SWITCH Group Management Tool (GMT)

The existing group management tool, GMT from SWITCH, is an obvious candidate for managing a VO for this project. This is due to its simplicity, and also because the main developer of the tool currently participates in the Identity Federation task. The SWITCH Group Management Tool is a web-based application for managing groups of users — performing access control and authorization on the same web server or on remote hosts using an API. GMT was designed to be easy to install and use.

Some improvements have been made to make this tool better suited as a VO component. The aim is to further explore various setup scenarios for a cross-federation VO platform.

The most significant update has been extending the flat-file storage back-end with a SQL storage back-end. The SQL storage handler scales much better, and is therefore better suited to manage large numbers of users. SQL is also a generic access API, which makes it possible to connect the user data storage to an Attribute Authority (as described in the Section 2.2); this is essential when implementing a VO Platform.

Figure 2.3 shows a screenshot of a GMT page used for the management of group members in a VO.

Virtual Organization Platform

This VO proof of concept (PoC) platform uses the SWITCH Group Management Tool (read GMT documentation) as VO administration interface. As VO admin you can change the group membership of users like the test user "William Tell". The membership is then reflected in the VO attribute, which in this PoC is the eduPersonEntitlement attribute. This attribute is available if the user accesses a VO service like VO Service Example choosing the "AAI Test Shibboleth (Shibboleth 1.3)" as his Home Organisation on the WAYF and authenticates with "w.tell" and "demo" as login name and password.

List of usernames and passwords you could use:

- voadmin/demo (AAI Test Home Organisation), "Hugo Boss"
- w.tell/demo (AAI Test Home Organisation), "William Tell"
- demouser/demo (AAI Demo Organisation), "Demouser SWITCHaai"
- demouser2/demo (AAI Demo Home Organisation), "Demouser2 SWITCHaai"

[Reset Database](#)

Members of Group: SwissResistance

- [Overview](#)
- [Add new group](#)
- [Invite users](#)
- [Add users](#)
- [Show roles](#)
- [Export all groups](#)
- [Need help?](#)

Name	Surname	Role	Change	Action
Tester	Kersting	Group Administrator	Change	Remove
Demouser	SWITCHaai	Group Administrator	Change	Remove
Hugo	Boss	Group Administrator	Change	Remove
Lukas	Hämmerle	Group Administrator	Change	Remove
William	Tell	Group Administrator	Change	Remove
Demouser2	SWITCHaai	Member	Change	Remove

[Invite users](#)
[Add users](#)
[Group settings](#)
[Export this group](#)

Figure 2.3: Management of group members in a VO using GMT

2.1.2 Preliminary Result 2: SimpleSAMLphp VO Management Module

UNINETT has implemented a VO Management module as an extension to SimpleSAMLphp [SimpleSAMLphp]. This VO Management module is simple to install and configure. It uses a SQLite backend for storage, which is automatically generated the first time the VO management UI is accessed. The implementation contains a limited set of functionality, sufficient for demonstrating a proof of concept. This implementation will be used in some of the proof of concepts based on SimpleSAMLphp.

Figure 2.4 shows management of a VO using the SimpleSAMLphp VO module.

simpleSAMLphp

[English](#) | [Bokmål](#) | [Nynorsk](#) | [Sámi](#) | [Suomeksi](#) | [Dansk](#) | [Svenska](#) | [Deutsch](#) | [Español](#) | [Français](#) | [Nederlands](#) | [Luxembourgish](#) | [Hrvatski](#) | [Magyar](#) | [Język polski](#) | [Slovenščina](#) | [Português](#) | [Português brasileiro](#) | [Türkçe](#)

Virtual Organizations

Here you can create virtual organizations. You are successfully logged in as andreas@md.feide.no

Organizations where you are the owner

feidecore	Feide Core Developers	edit delete
geant	European Research Project	edit delete

Add new organization

Identifier Unique identifier [a-z] and [0-9]

Name Human readable name

Description


Copyright © 2007-2009 Feide RnD 

Figure 2.4: SimpleSAMLphp VO module

2.2 SP-Centric Attribute Aggregation

The Virtual Organisation Management enables management and storage of VO information. SP-Centric Attribute Aggregation is concerned with how SPs obtain information about VOs from the VO platform.

The intentionally layered approach to the VO problem — where SP-Centric Attribute Aggregation is completely separated as a generic and independent architecture — allows the solution to be applied on a number of use-cases within identity federations. The solution can be applied to all situations where additional user data (attributes) needs to be provided to an SP from a source that is independent of and different to the IdP.

Attribute Aggregation is concerned with retrieving user attributes from multiple sources, and not only from the user's home IdP. IdP-centric attribute aggregation is the process whereby the IdP collects additional data from external sources during user login.

In some scenarios, IdP-centric aggregation does not provide sufficient flexibility: it may not be scalable or possible to involve the IdP in all cases where an SP would like to retrieve additional data from a third party. In this case, an SP-Centric aggregation can be introduced. With SP-Centric Attribute Aggregation the attribute retrieval process is completely independent from the login/SSO.

Two roles are involved in attribute retrieval:

- *Attribute Authority*: The service that provides attributes.
- *Attribute Consumer*: The client that requests attributes from an Attribute Authority. The Attribute Consumer is usually an SP.

2.2.1 General Aspects of Attribute Retrieval

Some general aspects that need to be considered when designing a protocol for attribute retrieval are described below.

Reference to the Principal

When an attribute consumer requests attributes from an attribute authority, the attribute authority needs a way of identifying which user the consumer wants attributes for. There are some well-known solutions to this:

- *Front-channel communication*: When requests are sent with HTTP Redirects, the Attribute Authority can establish or get access to a WebSSO session with the user. The protocol can then implicitly refer to the current user.
- *Shared identifier*: When attributes are not retrieved via front-channel communication, the Attribute Authority has no implicit reference to the current user, because the WebSSO session cookie is not exposed. Reference to the user can instead be obtained by including a shared user identifier in the request.
- *Alternative solutions that do not require a shared identifier*: For example, ID-WSF [\[ID-WSF\]](#) is a protocol that enhances user privacy, by making use of an encrypted version of the user identifier. In the context of Virtual Organisations, ID-WSF would increase the complexity of the architecture, due to the introduction of a third party that is needed to provide the encrypted user identifier to the Attribute Authority.

Registration and Authentication of the Consumer Client

The service provider would usually maintain control over which Consumer is allowed to talk with what Attribute Authority and what information each consumer is allowed to retrieve.

One option is to include the user in this access control flow, asking the user for consent to release personal information.

2.2.2 Alternative Attribute Retrieval Protocols

The following protocols should be used for SP-Centric Attribute Aggregation:

- SAML 2.0 AttributeQuery and SAML 2.0 Affiliation Role Descriptors
- SAML 2.0 AttributeQuery + ID-WSF
- Front-channel SAML 2.0 AttributeQuery
- OAuth Attribute Retrieval
- LDAP.

A goal of the Identity Federation Task is to gain more experience with a number of alternative attribute retrieval protocols.

2.2.2.1 SAML 2.0 AttributeQuery and SAML 2.0 Affiliation Role Descriptors

This architecture is explained in a separate document by Chad La Joie (SWITCH). See [\[vo-chad\]](#).

Each VO has a Security Assertion Markup Language (SAML) 2.0 Attribute Authority, supporting the AttributeQuery protocol [\[saml2-core\]](#) in the Assertion Query/Request Profile as defined in [\[saml2-profiles\]](#).

Each VO Platform deployment may be a provider of a dynamic metadata document listing a set of SAML 2.0 Affiliations. A SAML 2.0 Affiliation is a list of Service Providers that will receive the same identifier (SAML 2.0 NameID) for a specific user.

This approach is already supported in the Shibboleth software, where an identifying attribute like `'eduPersonPrincipalName'` or `'mail'` is used as a shared identifier. If however, the value of a persistent identifier is used as the shared identifier (can be used to generate the `'eduPersonTargetedID'`), the Identity Provider must be extended to support the Affiliation Role Descriptor. The advantage of this approach is that the user's data privacy is better protected when the user is a member of multiple VOs, since he or she would have different shared identifiers for these VOs.

The VO Platform will be a part of the federation infrastructure and will be dynamically included in the distributed metadata. A VO Platform in this approach typically consists of an SP protecting a VO administration interface, a database and an attribute authority. The attribute authority could be a standard IdP, where the SSO components are disabled and only the attribute authority is enabled. One VO Platform can be used to manage multiple VOs.

Another advantage of this approach is that an attribute consumer can retrieve user information from the VO Platform without any user interaction. A requirement for this, however, is that the attribute consumer knows a user's shared identifier, which implies that the user has to access the attribute consumer at least once. This could, for example, be used for account deprovisioning.

2.2.2.2 Attribute Authority (back-channel) and ID-WSF

ID-WSF is a protocol from Liberty Alliance, which allows a service provider to obtain an encrypted user identifier before accessing an attribute authority, something that would be privacy-enhancing.

The ID-WSF protocol has not been tested in Year 1 of the Identity Federations task, but is still listed as a proposed protocol that is worth exploring for SP-Centric Attribute Aggregation.

Neither Shibboleth nor SimpleSAMLphp has built-in support for ID-WSF.

2.2.2.3 Attribute Authority (front-channel)

Front-channel protocols do not necessarily need to use an identifier to refer to the current user. Instead, the requester can implicitly refer to the user holding the browser session, and both the requester and the responder will have a common reference to the current user without sharing an identifier inline in the protocol.

If the AttributeQuery protocol is used with a front-channel binding, as HTTP-REDIRECT or HTTP-POST [[saml2-bindings](#)] the implicit reference of the current user could be exploited.

Unfortunately, there is no defined SAML 2.0 profile where the AttributeQuery protocol is allowed to be used with front-channel bindings. The option of drafting a new front-channel protocol in the Identity Federations task was discussed and it might be included in the plans for Year 2.

Another alternative proposed by Wayf.dk (participants from Denmark) is to use the SAML 2.0 authentication request to query attributes from the attribute authority. This proposal resulted in 2.2.6 "Preliminary Result 6: Implementation of SpringFika".

A third idea, as described below, is to introduce new protocols (not SAML) for querying attributes. UNINETT has proposed and implemented some proof of concepts using OAuth, Representational State Transfer (REST) and JavaScript Object Notation (JSON).

2.2.2.4 OAuth, REST and JSON

OAuth [[OAuth](#)] enables the service provider to establish a session with the attribute authority. The Service Provider becomes an OAuth Consumer and the VO Platform an OAuth Provider.

A simple REST interface is suggested to allow querying of group information. A list of access endpoints could be:

- `<base>/vo/<vo-ID>/info`` - to extract *Group information*.
- `<base>/vo/<vo-ID>/members`` - to extract *Group membership*.
- `<base>/user/memberOf`` - to extract a *list of groups* for the current user.
- `<base>/vo/<vo-ID>/attributes`` - to extract *VO attributes* for the current user.

The response from the attribute authority could be encoding using the simple JSON encoding, or alternatively use the SAML 2.0 Attribute statement (XML message).

The process would be like this:

1. The Service Provider requests a Request token from the VO Platform.
2. The Service Provider sends the user to the VO Platform to authorise the Request Token.
3. The user authenticates to the VO Platform, and may be asked for consent to release VO attributes to the specific Service Provider.
4. The user returns to the Service Provider, and the Service Provider request to exchange the Request Token for an Access Token.
5. The Service Provider uses the Access Token to extract data from the VO Platform, using one of the data access endpoints listed above.

This approach is explained in more detail in [[SP-Centric Attribute Aggregation](#)].

2.2.2.5 LDAP (Lightweight Directory Access Protocol)

It may be convenient to use the LDAP protocol as a data access interface to VO information, as it is already well-supported in many tools working with groups.

If VO information is stored in an LDAP storage facility, service providers that are granted access can gain access to LDAP account credentials. To extract VO information the client (service provider) would need to know the user identifier, in order to create a LDAP search operation and extract the VO information as an entry.

2.2.3 Preliminary Result 3: Proof of Concept: Shibboleth, GMT and SAML 2.0 Attribute Queries

The goal was to find out if and to what extent the proof of concept (PoC) would technically work in an interederation environment with different implementations of SPs and IdPs.

Another item that we wanted to check was whether the PoC could handle other attributes, such as the `eduPersonPrincipalName` instead of the `swissEduPersonUnique` attribute (only used in Switzerland) as shared identifier for the attribute query to the VO platform.

As described below, using `'eduPersonPrincipalName'/'swissEduPersonUnique'/'email'` as a shared identifier is only an intermediate step, since the end goal should be to use the `'eduPersonTargetedID'`, which cannot yet be used due to a missing feature.

Usability, organisational and legal issues were not covered in these tests.

For a short description, slides and demo instructions, see [[VO-CONCEPT](#)].

The basic test setup is described in the following table:

VO Platform	VO SP	IdP with test accounts
<ul style="list-style-type: none"> • Shibboleth 2.1.x IdP + MySQL database + GMT 1.3 [GMT]. • AAI Test federation. • [How to configure Shib IdP in a VO environment]. 	<ul style="list-style-type: none"> • Shibboleth SP 2.2.x • AAI Test federation • [How to configure Shib SP in a VO environment] 	<ul style="list-style-type: none"> • Shibboleth 1.3.x and Shibboleth 2.x, • AAI Test federation

All involved components recognised each other via metadata. This was done by either manually adding metadata files of the other components to an IdPs or SPs configuration or by making sure there were entries in the JRA3 T2 metadata aggregation test metadata files. For a description of the metadata files, see [\[Metadata-files\]](#).

The IdPs were configured to release at least given 'name', 'surname', 'email' and 'eduPersonPrincipalName' or 'swissEduPersonUniqueID' to the VO Platform administration and the VO SP(s).

The VO SPs were configured to accept the above attributes, plus the entitlement attribute. They were also configured to serve as VO SPs by making them query the VO platform upon access of an authenticated user. Generally, the tests covered what is demonstrated in the screenshot of the PoC demo. See [\[VO-Poc_demo\]](#).

The following parties and components were involved in the tests:

- Andreas Solberg (UNINETT):
 - Tests with SimpleSAML IdP OpenIDP.org
- Leif Johansson (NORDUNET):
 - Tests with Shibboleth SP as VO SP
- Lukas Hämmerle (SWITCH):
 - With the basic test setup listed above
- Roland Hedberg (UMEA University):
 - Tests with new Python implementation of SP serving as VO SP
- Torsten Kersting (DFN):
 - Tests with Shibboleth IdP + SP as VO SP

An attempt was made to connect the above-mentioned PoC components operated by SWITCH to the components operated by the parties listed above. IdPs were used to test whether it was possible to access the VO Platform administration and VO services with accounts from other federations. In particular, the goal was to use accounts that consisted of given name, surname, email and an identifier attribute (such as 'eduPersonPrincipalName'). SPs were configured to serve as VO SPs doing an attribute query to the VO Platform upon login.

We tested whether it was possible to access the VO platform administration with a test account. The next test verified whether it was possible to access a VO SP without being a member of a VO group. If this was possible, the account was then added to a VO group and one or more VO SPs were accessed again to check whether

there were any VO attributes available that corresponded to the VO group(s) this account was member of. If these attributes were available and the SP and VO IdP log showed no errors, the test was considered successful.

The tests demonstrated that the PoC was (technically) usable in an inter-federation environment. In order to configure the VO SP that protects the VO administration interface to use an additional attribute as shared ID, only a few lines needed to be added to the 'attribute-map.xml' of that Shibboleth SP.

In general, this approach was versatile and promising, at least for Shibboleth-based infrastructures. It is simple, uses standard components, is easy to configure and easy to understand. The tests can all be considered as successful and no showstoppers were found.

2.2.4 Preliminary Result 4: Draft specification: OAuth Attribute Query Protocol

OAuth is a simple protocol used for establishing a shared session between a requester and a responder. In the context of SP-Centric Attribute Aggregation it would be useful to exploit this, as it enables querying attributes from an attribute authority without the need for a shared identifier between the attribute consumer and the attribute authority.

OAuth does not define a specific protocol that can be used for attribute queries; instead it is a protocol framework that allows any REST-based request-response protocol to be able to use OAuth for session setup.

In Identity Federations a specification of a simple REST-based attribute query protocol was drafted that makes use of OAuth. The draft specification is implemented in [\[SimpleSAMLphp\]](#) and is used in the proof of concept described in Section 2.2.5 below.

2.2.5 Preliminary Result 5: Proof of concept: SimpleSAMLphp and OAuth Attribute Retrieval

UNINETT implemented these components as modules of SimpleSAMLphp:

- Simple Virtual Organisation Management UI with SQLite storage, as described in Section 2.1.2 "Intermediate Preliminary Result 2: SimpleSAMLphp VO Management Module".
- OAuth module. An implementation of OAuth.
- OAuth client registry module. A module with a user interface for management of OAuth clients.
- Implementation of the OAuth attribute query protocol on both client and server.

These modules provide a full VO Platform in SimpleSAMLphp.

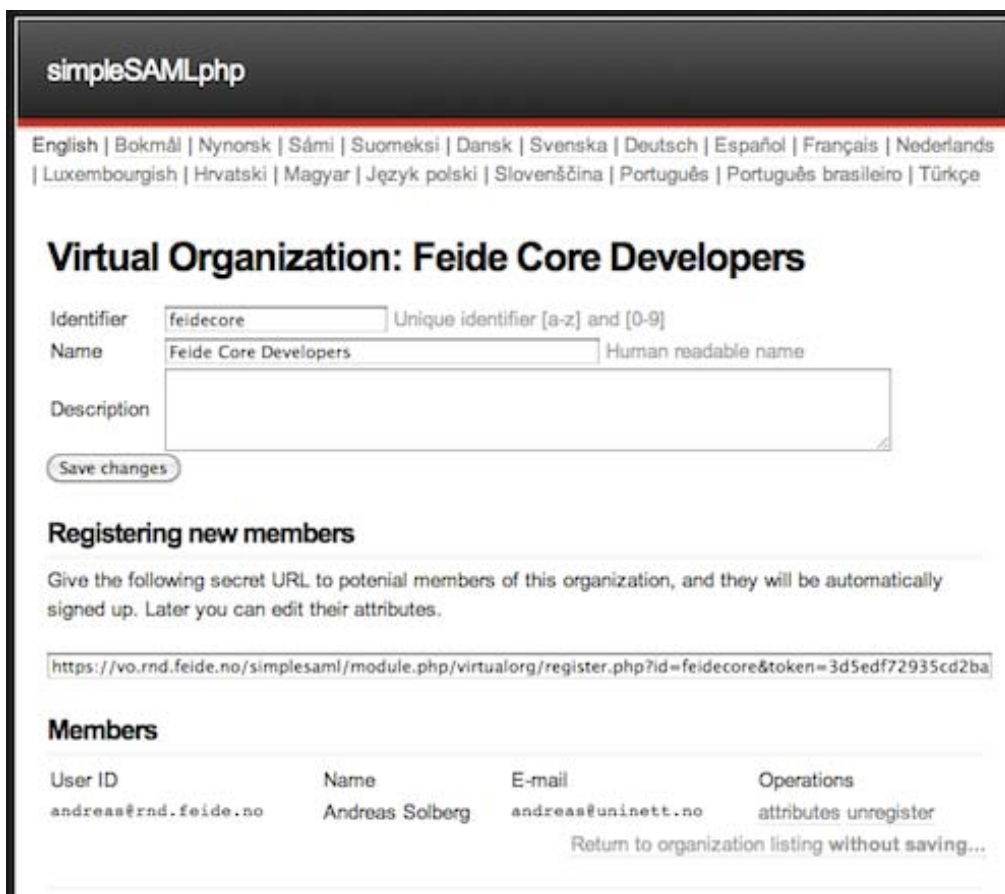
The OAuth trust model is based on the registration of OAuth Consumers (clients) at the Attribute Authority. Clients will then obtain a *key + secret* that ensures trusted communication between a client and the Attribute Authority. This would be independent of the Identity Federations' existing trust model, and would consequently not impose any changes to existing Identity Federations. As the existing SAML trust fabric may not easily be re-

used, the OAuth trust model would not benefit from the already established scalable trust management in Identity Federations. As an alternative approach, and in order to make the trust-model scalable, acceptance of new SPs could be left to end-users. This approach is often used in User-Centric Identity systems. The trust model in OAuth is an area that needs more research when used in the context of Identity Federations.

A user interface for registering new clients and obtaining “client key + secret” is implemented in the SimpleSAMLphp OAuth module.

This demonstration uses new technology, and currently only one implementation is available; see [[SimpleSAMLphp](#)]. On the other hand, the protocols involved are simple, making it less complicated to implement. OAuth libraries are also available for most major programming languages.

Figure 2.5 shows management of a VO as part of the demo. The screenshot illustrates how this can be used. The proof of concept is live and may be tested using the Feide OpenIdP, which allows any user to sign up.



simpleSAMLphp

English | Bokmål | Nynorsk | Sámi | Suomeksi | Dansk | Svenska | Deutsch | Español | Français | Nederlands
| Luxembourgish | Hrvatski | Magyar | Język polski | Slovenščina | Português | Português brasileiro | Türkçe

Virtual Organization: Feide Core Developers

Identifier: Unique identifier [a-z] and [0-9]

Name: Human readable name

Description:

Registering new members

Give the following secret URL to potential members of this organization, and they will be automatically signed up. Later you can edit their attributes.

Members

User ID	Name	E-mail	Operations
andreas@rnd.feide.no	Andreas Solberg	andreas@uninett.no	attributes unregister

[Return to organization listing without saving...](#)

Figure 2.5: Example management of a VO

The screenshot can be found online; see [[SC](#)].

2.2.6 Preliminary Result 6: Implementation of SpringFika

WAYF (Denmark) has implemented the SpringFika [\[SpringFika\]](#) attribute collector, which gathers attributes from across a number of identity providers and builds a superset of attributes about a given user.

Problem Description

It is not unusual for users to be affiliated with more than one institution (identity provider), and have different roles at these institutions (e.g. teacher, student, staff). Often, within a given institution, information about the users is kept in separate repositories; for example, entitlements to library services are kept by the library while more common information (such as username, email address and affiliations) is kept centrally.

The challenge of collecting information about a given user across multiple systems and organisations is known as attribute collection.

Multiple approaches were discussed in the initial requirement specification process for SpringFika. These approaches had only one constraint — the solution must be based on SAML2 assertions. Participants in these discussions included REDIris (Spain), FEIDE (Norway) and WAYF (Denmark).

One approach was chosen for the implementation of SpringFika: the front channel solution, which is user-browser centric and based on web re-directs. The obvious advantage of this solution is that the system is confined to the limited set of browser instructions and does not require interoperability with multiple backend systems, protocols or other components.

The question of how to approach non-web-based systems will be part of the ‘beyond-web-SSO’ work package in Task 2.

The implemented system is able to receive a SAML2 request from a service provider, collect information about a user from multiple identity providers, collate this information in an attribute superset, and then return this superset to the service provider.

Trust relations regarding authentication mechanism, intermediate attributes released to the attribute collector and other parameters are static and based on agreements among the involved identity providers and the attribute collector operator.

SpringFika Characteristics

SpringFika introduces the concept of “virtual identity providers”, where the result of choosing a given identity provider might transparently return attributes from multiple back-end identity providers as an extended set of attributes compared to what any single identity provider can provide. The list of back-end identity providers where attributes should be collected may be of any length.

A feature of special interest in this setup is the ability to issue “scoped” SAML2 authentication requests; see [\[scoped\]](#). Scoped authentication requests allow a single IdP to assert the identity for multiple organisations and enable an SP to discriminate between organisations rather than accepting or rejecting all users of an IdP. This feature can be particularly useful in those cases where one IdP is used for handling the users of different organisations. One of the benefits of this feature is that usernames can be generalised in the format

["username@home_institution.org"](#). A service can then decide to only grant access to a limited number of institutions, which could be easily implemented because of the scoped authentication.

One method is to query SpringFika to verify whether the user has a valid session and, if yes, trust that the user is the correct user. Alternatively, the identity provider may either use its own authentication mechanism or request the user to authenticate with a specified authentication system. The required SAML2 authentication request may then be scoped (and hence automatically redirected) to the correct authentication system. The use of scoped requests enables identity providers to rely entirely on external authentication systems, and act as pure attribute authorities.

The implementation of the attribute collector is a self-contained PHP-script and therefore easily deployed.

SpringFika's main data structure is the SAML2 assertions, requests and responses represented as php arrays. There is no abstraction layer between the script and the SAML2 entities, so all manipulation is done directly on the arrays/entities.

The "real" SAML xml is converted to arrays when coming into the script, and vice versa on their way out. The conversion has been simplified, so it does not cover all possible SAML2 messages. It is possible, at the cost of some added complexity, to configure the conversion to be more general. PHP arrays are really ordered maps, so element sequences can be preserved and constructed.

SAML2 system entities can be either identity providers or service providers, and in SpringFika they are always both (i.e. they are always bridges/proxies). This is because a service provider has an identity provider interface to present its assertions to the application proper, and an identity provider has a service provider side to authenticate the user. These interfaces can be considered as "internal" in that they do not need access to the same metadata and public key infrastructure as the federation-visible external interfaces.

To make these internal interfaces simpler to develop (in the application and authentication mechanism), but still allow access to the full SAML2 message, SpringFika can send and receive them in a JSON representation. They can be signed using a simple shared secret schema. SpringFika is thus always "remote" in the sense that applications are always seen as remote service providers and authentication mechanisms are always seen as remote identity providers. By default, SpringFika does not keep any session information (besides what is needed when acting as a proxy; i.e. remembering an incoming request while waiting for the response).

SpringFika uses the concept of co-hosted system entities; communication between co-hosted entities is done by an internal binding mechanism (i.e. no browser involvement) for performance reasons.

SpringFika is geared towards a proxy environment as the Danish Wayf.dk federation, but it can be used to learn about and experiment with a peer-to-peer federation as well.

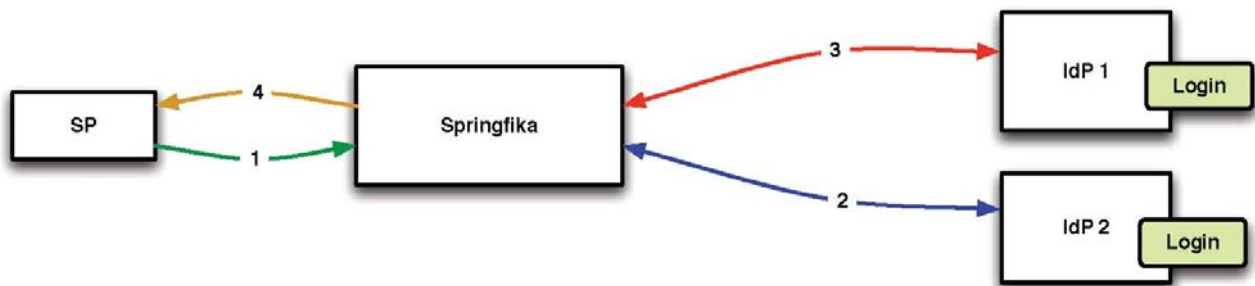


Figure 2.6: SpringFika workflow

1. SAML2 authentication request.
2. Request + attribute response from identity provider 2, received and cached by SpringFika.
3. Request + attribute response from identity provider 1, received and cached by SpringFika.
4. Attribute 'super set' response, containing attributes from both identity provider 1+2, send from SpringFika to service provider.

3 Sub-Task II: Metadata Distribution

Given that participating federations support the common federation protocol, SAML 2.0 [[SAML2](#)] and that they support the same version (see the Federation Harmonisation sub-task), the remaining part of the technical foundation for a cross-federation environment is how to distribute metadata.

Metadata in this context is information about a SAML entity participating in a federation. Information includes names and contact details as well as URL endpoints to direct SAML messages during Single Sign On (SSO). The OASIS SAML 2.0 Specification also includes an XML document schema for metadata for SAML entities. See [[SAML2](#)]. This specification introduces a document format for metadata. However, a distribution model that would be suitable for cross-federation is not covered in the specification.

As metadata needs to be exchanged in a secure way between all relying parties, metadata distribution is tightly integrated with the cross-federation trust-fabric.

This sub-task involves work on harmonising the metadata content as well as creating scalable methods for distributing metadata in a cross-federation context.

Most participants agree that a fully distributed metadata architecture is ideal. A fully distributed architecture is far more complex to design and is not likely to produce immediate results. Throughout the project, alternative architectures will be considered and designed. It is reasonable to start with a simple centralised design and gain experience before approaching more complex and distributed designs. This also meets the needs of the SA3 Task 3 eduGAIN.

3.1.1 Preliminary Result 7: Simple Metadata Aggregation Profile

A document has been produced, called “Simple Metadata Aggregation Profile”; see [[Simple Metadata Aggregation Profile](#)]. This profile is based on the work with the Kalmar Union cross-federation, in which UNINETT has been closely involved. This profile defines a simple centralised architecture based on:

- Key exchange (no PKI)
- HTTP GET for metadata transport
- Hierarchy of aggregators re-distributing metadata.

Figure 3.7 shows how national federation metadata is regularly pulled from the central aggregate:

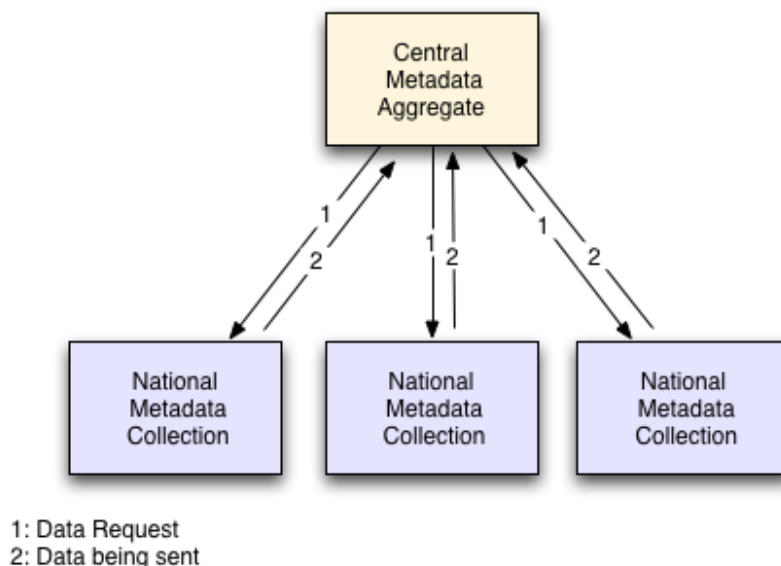


Figure 3.7: National federation metadata aggregation

3.1.2 Preliminary Result 8: Cross-Federation Technical Test Pilot

UNINETT set up a metadata aggregator following the “Simple Metadata Aggregation Profile”^{*} architecture, using the SimpleSAMLphp Metadata aggregator software. The intention was to gain more practical experience with metadata distribution using this architecture.

A number of federations participated in testing and published metadata for their federation with both Service Providers and Identity Providers. The participants were:

- UNINETT
- SWITCH
- PIONIER
- RENATER
- SUNet SWAMID
- DFN
- UK Access Federation
- CESNET















Some production services were connected to the metadata aggregate as well, such as the Feide OpenIdP [[FeidOp](#)] and the Feide Foodle [[FeidFoo](#)] service.

The tests were considered successful in the sense that operations worked smoothly and users were able to use the connected IdPs to gain access to the services.

The system has not been systematically tested on its handling of special cases that are more likely to cause problems.

Figure 3.8 shows the automatically generated list of entities on the central aggregator during the testing:

Identity Providers

-  CESNET [[more](#)]
-  NORDUnet [[more](#)]
-  DFN shibboleth Test IDP use test/tester as login [[more](#)]
-  IdP de test pour la fédération Éducation-Recherche [[more](#)]
-  DFN SimpleSAML Test IDP test/tester as login [[more](#)]
-  Linköping University [[more](#)]
-  PIONIER IdP [[more](#)]
-  Umeå university (New SAML2) [[more](#)]
-  Nicolaus Copernicus University in Torun [[more](#)]
-  CRU - comptes CRU [[more](#)]
-  DFN SimpleSAML Test IDP II use test/tester as login [[more](#)]
-  Test UMK SLO IdP [[more](#)]
-  Feide OpenIdP (guest users) [[more](#)]
-  JISC project: SDSS (Fountainhall) [[more](#)]

Service Providers

















-  Kalmar Attribute Viewer of Andreas [[more](#)]
-  <https://sp.swamid.se/shibboleth>
-  <https://foodle.feide.no/simplesaml/module.php/saml/sp/metadata.php/saml>
-  <https://sp-test.swamid.se/shibboleth>
-  OpenWiki [[more](#)]
-  OpenWiki Administration [[more](#)]
-  CESNET [[more](#)]
-  <https://services-federation.renater.fr/test/ressource>
-  Feide RnD Translation Portal [[more](#)]
-  Feide SecureMail [[more](#)]
-  Kalmar Attribute Viewer of Andreas (2) [[more](#)]
-  <https://connect.sunet.se/shibboleth>
-  Feide RnD Blog [[more](#)]
-  DFN shibboleth Test SP [[more](#)]
-  DFN SimpleSAML Test SP [[more](#)]
-  SDSS Fountainhall Shibboleth 2.X test SP [[more](#)]

Figure 3.8: Entities on the central aggregator during testing

More details concerning the test setup are documented in the test report; see [\[Metadata-test\]](#).

3.1.3 Preliminary Result 9: SimpleSAMLphp Metadata Aggregator

Section 3.1.2 describes the use of SimpleSAMLphp for metadata aggregation.

SimpleSAMLphp had (prior to the Identity Federation task) a module for metadata aggregation that was sufficient to initiate the cross-federation technical test pilot described in *Preliminary Result 8: Cross-Federation Technical Test Pilot* on page 23.

During the test pilot phase a number of improvements were requested and implemented to the SimpleSAMLphp Metadata Aggregator.

The improvements include, but are not limited to:

- Better handling of multiple endpoint descriptors with different bindings
- More human-readable output
- Better filtering capabilities
- New support for multiple certificates to support certificate roll-over
- Improved expiration handling
- New user interface for debugging metadata fetch
- New user interface for listing entities presented with flags for originating country.

These improvements and new functionality have made the metadata aggregation better suited for the variety of needs in European federations. Therefore, the list of features was extended beyond the simple set of features that were required for operating the aggregator in the Kalmar Union.

3.1.4 Preliminary Result 10: Metadata Aggregator Specification

During the development of the SimpleSAMLphp Metadata Aggregator's additional features, and in discussions related to the cross-federation technical test pilot, it became evident that a clearer definition of what a metadata aggregator is and how it is expected to behave is needed.

The metadata aggregator will be an extremely important component in first-generation connections between different federations. This approach will hopefully result in multiple competing implementations that are compatible. To make sure that these implementations behave in the same manner, a specification defining the aggregator role is required.

Work on an "Extensible Metadata Aggregator Specification" was started in Year 1. It will be continued in Year 2.

For more information on the current work in progress, see [\[FEIDE\]](#).

3.1.4.1 *Utilisation Outside the Task*

The Simple Metadata Aggregation Profile, as well as experiences from the test-pilot and the implemented improvements on the SimpleSAMLphp Metadata Aggregator, are adopted by the operational cross-federation Kalmar Union; see [\[Kalmar Union\]](#).

eduGAIN is also likely to benefit from this work and, if so, this will be a driving force towards better interoperability between federations and between multiple cross-federation initiatives.

4 Sub-Task III: Federation Harmonisation

Managing a federated identity infrastructure involves many choices. Best practice documents can help federations make the best choices, and hence increase the opportunities for cross-federation interoperability.

The initial plan was to cover the following topics:

- Interoperable SAML 2.0 Web Browser SSO Deployment Profile
- De-provisioning
- Logout in federations.

4.1 Interoperable SAML 2.0 Web Browser SSO Deployment Profile

SAML 2.0 provides the developer with numerous options. This includes how to pass attributes, which bindings to use, how to use PKI, what should be signed and what should be encrypted.

An unwanted side-effect of this flexibility is that two deployments of software supporting SAML 2.0 may not interoperate as smoothly as expected.

"The Interoperable SAML 2.0 Web Browser SSO Deployment Profile" defines a minimum set of bindings and rules that should facilitate interoperability.

This project began prior to the start of the Identity Federation task, but the specification work has been put into the Identity Federation task, and the profile is now in a more mature state.

The project has already gained attention from existing educational identity federations in Europe, and as of January 2010, these federations officially support and rely on version 0.1 [[saml2int1](#)] of the profile:

- Feide (Norway)
- Haka (Finland)
- HEAnet Edugate (Ireland)
- The RedIRIS Identity Service (Spain)

- SWAMID (Sweden).

In addition, the GÉANT SA3 eduGAIN project will most likely rely on the profile for its upcoming European cross-federation.

A neutral website is set up to hold the profile and some information about what it is used for, as well as supporting partners. See [[SAMLsite](#)].

4.2 Deprovisioning

NorduNet is currently leading work on writing a best-practice document on de-provisioning. Work is still in progress is addressing the following topics:

- The semantics of deprovisioning:
 - What it means to deprovision an identity.
 - The differences between deprovisioning and PKI revocation.
- Applicability:
 - Important uses of deprovisioning.
- Push vs. pull:
 - Deprovisioning in the enterprise.
- Deprovisioning as attribute aggregation:
 - Using SP-centric attribute aggregation.
- Privacy aspects:
 - Problems with the SP-centric approach.
- Other alternatives:
 - RSS, ATOM, OCSP, etc.

4.3 Logout in Federations

Cookies [[RFC2965](#)] are used to keep sessions on websites. Cookies are limited to a shared state/session between endpoints using the same domain name. Authenticated sessions require that users enter some credentials each time a session is established. Consequently, a user has to re-enter credentials for every new domain. Single Sign-On protocols such as SAML 2.0 [[SAML2](#)] enable the propagation of authenticated sessions between domains. This is considered convenient for the user, as the user does not need to re-enter credentials for every site.

All service providers that share authenticated sessions with an identity provider form a federation. A user is not likely to have a clear understanding of which services are part of a federation and which are not.

It is important to provide some way of terminating authenticated sessions for users. Two factors increase the need for logout in a federation compared to stand-alone services:

- The authenticated session grants access to a large number of services. At the same time the user is not aware of exactly which services can be accessed without re-logging in through the authenticated session at the IdP.
- One way of improving the end user experience is to increase the length of the session at the IdP. For example, in the Norwegian federation Feide, the session at the IdP lasts 8 hours. In comparison, sessions at Internet banks often last only a few minutes.

4.3.1 Different Logout Options

This section describes four different approaches to handling logout in a federation.

Solution A: Not Handling Logout at All

Due to the difficulties of implementing and providing logout functionality, most federations choose not to implement logout.

This solution is based upon the following:

- The default behaviour of most (if not all) web browsers is that when the browser is closed, all temporary cookies are deleted. This will terminate all authenticated sessions across all services that use temporary cookies for keeping the session.
- Most users are used to closing web pages in order to log out from their sessions.
- Even if a logout implementation is provided to the user, the option to close the browser will always be possible for users that prefer this option, which is also easy and secure if done properly.

There are a number of reasons for not using this solution:

- There is some inconsistency in how browsers behave when closing the browser. One example is Firefox, which will continue to run when there is still a download in progress. Therefore, temporary cookies are not deleted.
- Service Providers may use persistent cookies to keep the authenticated session. The federation may restrict this by rules. However, it may be difficult to control the behaviour of all service providers, and it is almost impossible to identify whether a user's session is held by a temporary or persistent cookie.
- When users close web pages to log out, they might only close the tab or the browser window. This is not sufficient to quit the web browser and thus delete session cookies. On the Macintosh platform in particular, users are more used to closing windows than applications. This tendency was found in single log-out (SLO) usability tests performed by Netlife Research in February 2009.

Solution B: Local Logout - at SP Only

This is not considered to be a practical solution, but is worth mentioning for the sake of completeness.

It is possible to do a local logout at the Service Provider (SP) by deleting all (session) cookies for the SP's domain. However, since the session at the user's IdP is still active, the user will immediately be logged in again on the SP without re-authentication as soon as the SP tries to enforce a session. Obviously, this is not what a user would expect to happen.

Doing a proper local logout is possible if the service provider uses 'ForceAuthN="true' in the 'AuthNRequest' that is sent to the IdP. 'ForceAuthN' disables SSO for that particular SP and thus forces the user to reauthenticate.

Solution C: Logout at one SP and the IdP

To fix the problem with local logout the obvious next step is to propagate logout from the SP to the IdP. This means that when the user logs out from SP1, the authenticated session at the SP and the IdP is terminated, but other sessions are still active (SP2, SP3, etc).

The main problem with this solution is that the user does not have good control over which services they are logged into. The borders between services may be diffuse and inconsistent. Since users have a single sign-on, they are given no indication when accessing a new SP and are automatically logged in. It is common practice to bundle multiple services into a common SP, for example to simplify the deployment. At the same time, the opposite example exists, e.g. the Feide OpenWiki acts as two Service Providers, the wiki part and the admin part. The wiki part is federated with a superset of the IdPs.

This solution is not recommended, mainly because users will not know what happens during logout.

Solution D: Fully Federated SLO - Propagated to all SPs

The most complex solution is where SLO is propagated from the initiator (SP) to the IdP and then to all other SPs with an active session.

This solution has several issues that have to be dealt with in order to provide a good experience to SPs and end users:

- The SPs should not be forced to implement IdP-initiated Simple Object Access Protocol (SOAP) SLO as it involves some extra challenges, not only at the SP but in the integration with the service itself. In this case, only front-channel SLO is left, and that raises a new issue:
- Front-channel SLO creates the scenario where the user initiates logout from SP1, gets a "500 Internal Error" at SP2 and is unable to complete logout. This is not acceptable, either for the end-user, the federation or SP1.
- The user is not expected to fully understand the consequences of SLO, and initiating SLO may lead to the fact that the user is logged out from a service that they did not intend to log out from. Examples of unwanted effects include large transactions that are interrupted or large wiki pages that are being edited but not saved upon log-out.
- If only a subset of SPs implement SLO properly, it provides an inconsistent experience for the user. A policy solution may be to require that all SPs in a federation support SLO.
- Even if all SPs are required to support SLO, it is unlikely to expect all SPs at all times to work flawlessly. When exceptions arise and SLO fails it is important that the user is notified of which services they were successfully logged out from and which they were not.

4.3.2 The Feide Solution to SLO

Feide, the Norwegian Identity Federation operated by UNINETT, has implemented a solution to SLO that works as follows:

The user initiates SLO by clicking “logout” at one of the SPs. Complex information (for example SLO or global logout) is not presented to the users, instead the user interface informs them about the state of logout, as described below.

When the user clicks 'logout', a HTTP-REDIRECT LogoutRequest is sent to the Identity Provider.

The Identity Provider presents a HTML page to the user with the following information:

- You have initiated logout from SP1.
- Button1: (Logout from SP1 and IdP only).
- You are also logged in to the following services that supports logout:
 - SP2
 - SP3
 - SP4
- Button2: (Logout from all services above including SP1).

If the user is logged into a service provider that does not support logout at all (which should be an exception if the federation requires that all SPs implement SLO; for example in the shibboleth federation, it may be that some SPs still use the Shib1.3 protocol and do not support SLO), the user will be recommended to close the browser to terminate all sessions.

If the user clicks “Button1”, a successful `LogoutResponse` is sent back to SP1, and SLO is not propagated to other SPs. This works as “Solution C”, but the UI messages solves the problem of notifying the user about what is going on and what other services the user still is logged into.

If the user clicks “Button2”, the IdP presents a HTML page to the user including hidden iFrames that point to the SLO endpoints of all services. The `href` field of the iFrames is a `HTTP-REDIRECT` `LogoutRequest` with `IsPassive="true"`, and the user is logged out from all SPs in parallel. The `LogoutResponse` is sent back to an endpoint at the IdP, and updates the status session of the SLO progress. The HTML page presented to the user displays a table listing all SPs, and shows a spinning wheel icon for each SP, indicating that the logout is in progress. When logout is completed successfully for an SP, a checkmark icon is displayed next to the SP name. If the SP is not responding, the wheel keeps spinning, and after 15 seconds an information box is displayed saying that some of the SPs are not able to be contacted and that the user should close the browser in order to be sure to end the session. If an SP responds with an error message, a red cross icon is displayed next to it and the user is notified about the actions that are needed to continue.

If all SPs respond successfully, the IdP waits for two seconds to enable the user to view the checkmark icons. The user is then automatically sent back to the initiating SP with a successful `LogoutResponse`.

The implementation has a fallback mechanism that works without JavaScript. However, since it is lacking the live update of the SLO progress it is not as appealing.

The solution described above is part of the SimpleSAMLphp code and is therefore available for anyone to use.

Figure 4.9 shows a screenshot from an early version of the SLO implementation:

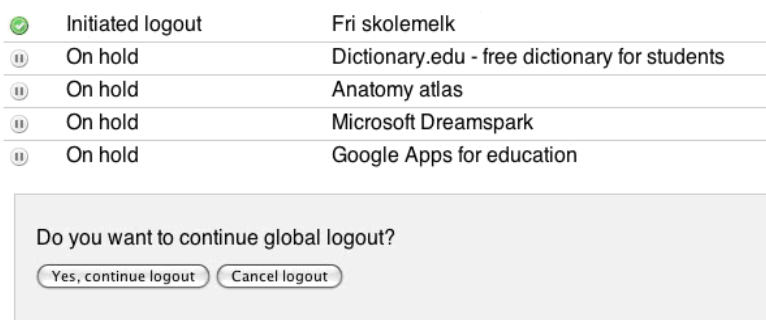


Figure 4.9: Feide SLO interface

A usability test was carried out with typical users. The test focused on how they managed to use the new login and logout implementation. The results of the test have been reflected in some UI simplifications and improvements.

In 2009 NIIF implemented a similar implementation of front-channel logout as a plug-in to the Shibboleth IdP.

During the work with the plug-in, NIIF and SWITCH became aware of an issue with web-browsers configured to reject third-party cookies in combination with iFrames. UNINETT is testing this special-case further, and is trying to map different browser behaviours with the logout approach. The work resulted in an updated version of the SimpleSAMLphp logout implementation, which is scheduled for release in April 2010 in SimpleSAMLphp version 1.6.

5 Sub-Task IV: User-Centric Identity

The work carried out in this sub-task produced two documents, the first one on User-Centric technologies [[User-Centric document](#)], which is summarised in Section 5.1. The second document describes how OpenID can be used to implement a federation that is equivalent to a SAML-based federation; this work is described in Section 5.2.

5.1 User-Centric Identity in European Identity Federations

One of the sub-tasks within the Identity Federation task focuses on user-centric technologies.

A document describing the main characteristics of the Federated Identity Management model and the User-Centric Identity Management model has been written by TERENA. The document focuses mostly on the user-centric approach and describes examples of technologies that implement this model. Due to the increasing interest around the user-centric model and related technologies, the document also explores possible use-cases for NRENs to support user-centric technologies within their Federated Identity Management Systems. The document summarises the work carried out in sub-task IV during the first year.

A short summary of the document is provided below.

In order to clearly establish the characteristics of the user-centric approach in the context of the academic identity federations, it is important to first recap some definitions. The process of mapping users to electronic identities is known as Identity Management.

In recent years, the notion of Identity Management has changed. User identities are no longer managed on a per-application basis, but rather as a part of the middleware infrastructure that interacts with services. This has several advantages, such as handling user data in a more centralised fashion, decoupling authentication and authorisation functionalities, and reducing the number of credentials to be remembered by users.

Federated Identity Management, also commonly referred to as Federations or Identity Federations, is the collection of all processes, standards and technology that allow a controlled exchange of users' identity data across organisational boundaries. This does not necessarily only mean between institutions, but can also mean between sections or departments within institutions.

The aim of Federated Identity Management is to provide authentication, authorisation and personalisation across a distributed services landscape in a scalable and trustworthy way.

The research and education community worldwide implements SAML-based federations; the models in which these federations can inter-operate are the subject of discussion and studies that involve both technologies and policies.

The **user-centric** model for managing identity has been the subject of increasing attention in recent years, as it has been identified with technologies linked to Web 2.0 (e.g. Wikis, blogs and collective services like Flickr). This generally refers to web-based communities and services that facilitate collaboration and sharing between users.

The user-centric approach emerged in response to the need to offer a portable electronic identity, not related to a specific domain, but controlled by the user. The user-centric model was also conceived to respond to the demand to protect users' privacy and to avoid unnecessary exchange of user data over the Internet.

Two main solutions have been proposed with respect to user-centric identity management:

- Information Card (InfoCard), proposed in 2008 and supported/coordinated by Information Card Foundation.
- OpenID managed by the Open ID Foundation.

Both organisations have announced a strategic collaboration to make both solutions compatible in future.

One of the main differences between Identify Federations and User-Centric Identity Management is that in the latter a user is not necessarily associated with a home institution that handles the user's data. On the contrary the user can gather the data requested by a resource, assemble it into a token or a URL and deliver this to the resource the user wishes to access. This would allow users to interact flexibly with multiple services. However the lack of binding between users and IdPs typically means that user-centric asserted identities are associated with lower levels of assurance.

The issue of trust is one of the key differentiations among the various technologies, ranking from OpenID (in which no trust links are required by the protocol) to SAML-based federations (in which trust is a key element). In the trust context it is important to note that OpenID protocol does not provide any real trust framework; on the contrary, OpenID builds on the assumption that trust should be completely open, meaning that each SP can decide to trust any OpenID Provider. In practice, however, SPs are rather reluctant to implement this model and normally will only accept a selected number of providers, especially in the case of SPs that offer commercial services. However the fact that the protocol does not require trusted relationships does not mean that OpenID Providers and SPs could not implement a policy to enhance the trust level.

Whether NRENs-operated federations should provide support for user-centric technologies depends very much on the use-case to address, and on the level of trust that is required by a given service.

The adoption of user-centric technologies in the European NRENs community is rather low, although most of the NRENs are well informed on the progress in this area. A few NRENs however have started some tests with

OpenID and InfoCard technologies. SURFnet and RedIRIS provide support for OpenID, whereas others like JISC and NORDUNETT have funded studies to investigate whether to support OpenID.

In summary it could be said that for the NRENs, SAML-based federations remain a fundamental service. User-centric protocols can be used in two additional ways:

- To build a federated access-control by requiring additional checks to be added (without violating the protocols).
- To enhance user experience in a federation, simplifying IdP selection, for low level of assurance services.

Figure 5.10 uses a Venn diagram to highlight similarities and differences between the three technologies mentioned in the user-centric document.

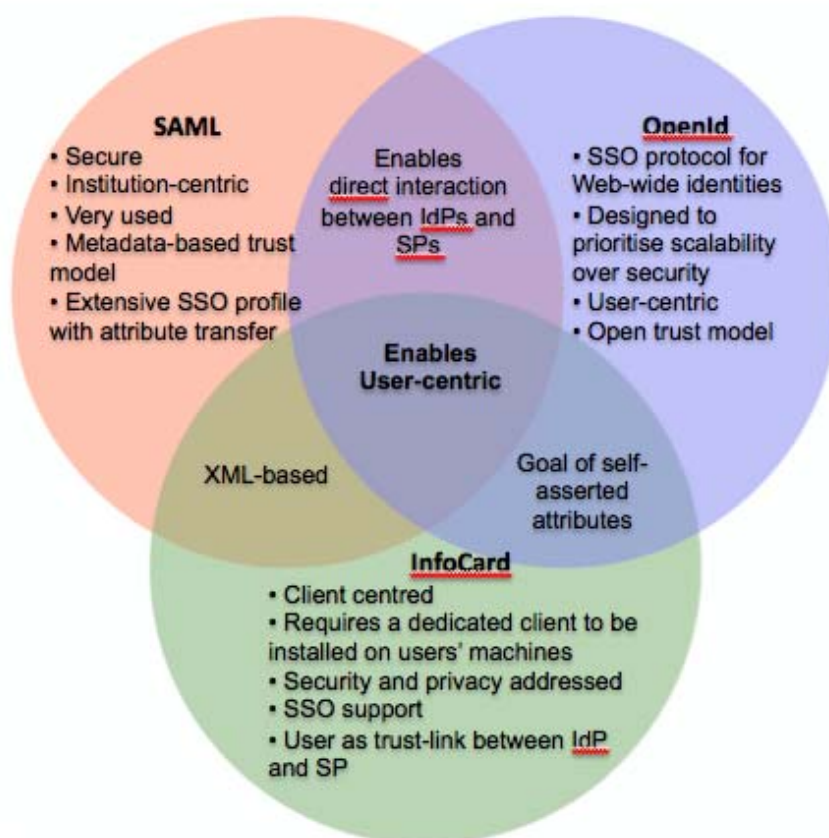


Figure 5.10: Similarities and differences between the three approaches

The Identity Federation group considered the user-centric document as an interesting insight into the issues related to user-centric technologies. Due to the interest in this area from some of the major players, such as Microsoft and Google, it was agreed to keep monitoring the user-centric space. The ultimate goal for Identity Federation operators is to be able to support multiple use-cases and to inter-operate with different federations, with the vision to liaise with other communities beyond HE (i.e. eGovernment, eScience, Health communities and so on).

During the second year this sub-task will test more ways for SAML-based Identity Federation to support user-centric technologies.

5.2 OpenID Federations

UNINETT wrote a short document [[OpenID Federations](#)] elaborating how OpenID could replace SAML to implement an Identity Federations and describing which features would be gained and which features would be missing compared to a SAML-based infrastructure [[OpenID Federations](#)].

This document is only an expression of an idea from UNINETT. The idea is controversial, and is less likely to be implemented, because of already deployed infrastructure. However these ideas are still valuable, as they help in building use-cases and consolidating existing architectures.

6 Sub-Task V: Beyond Web-SSO

Until now Identity Federations have been almost completely limited to Web Single Sign-On. There are an increasing number of requests and use-cases with more complex authentication scenarios, where the client is not always represented by a web browser. These use-cases can be mainly categorised into groups where:

- The client that authenticates to a service is not web-based but instead either an application like the personarUI or a command-line utility, such as remote shell access via telnet or ssh.
- The user authenticates to two different web-based services that want to communicate via a back-channel on behalf of the user. This use-case is often referred to as “delegation”.

The following are examples of some future projects:

- Proposal of an architecture presented by Josh Howlett at TNC 2009 in Malaga.
- Discussion on multi-domain Kerberos on the mailing list.

6.1 Preliminary Result 11: Beyond WebSSO using OAuth - Implementation in SimpleSAMLphp

OAuth is a recent protocol that has become increasingly popular. The protocol is simple to understand and implement. The orange line in the graph shown in Figure 6.11, from “Google trends”, illustrates the increasing popularity of OAuth during the past few years.

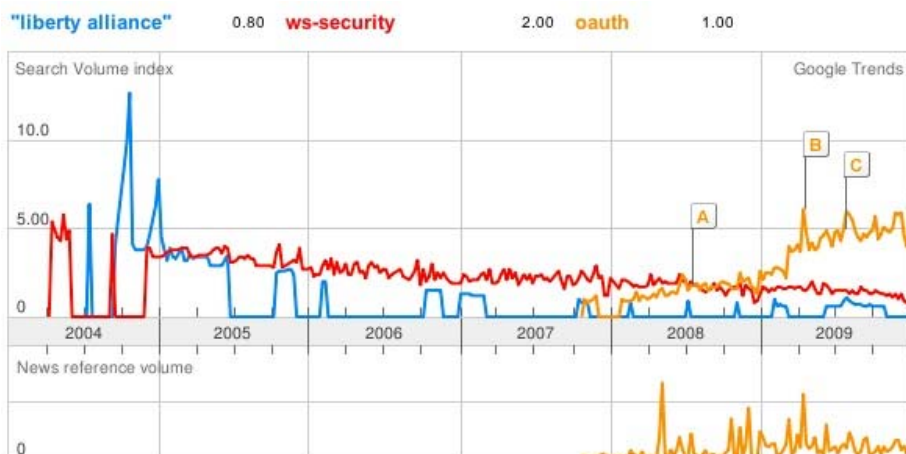


Figure 6.11: Popularity of OAuth during the last few years

An OAuth module has been implemented in SimpleSAMLphp in order to demonstrate how this protocol can solve a number of the use-cases that were seen.

In addition to implementing a generic OAuth module, a demo use-case has been implemented. A command line client uses SimpleSAMLphp to become an OAuth Consumer. In addition, an OAuth Provider, acting as a SAML 2.0 Service Provider, connects the command line client to an existing WebSSO Federation. Figure 6.12 provides an overview of the components in the architecture:

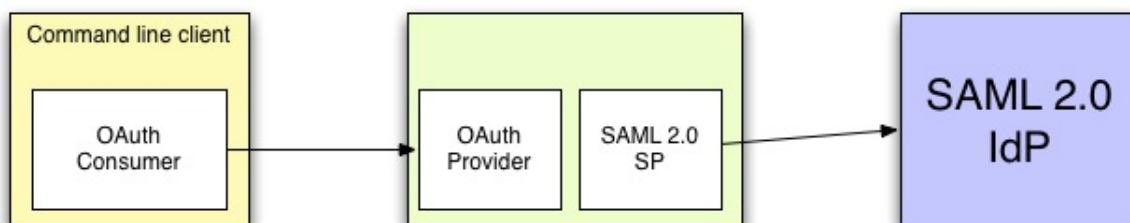


Figure 6.12: Demo-case components

Figure 6.13 shows the command line clients using OAuth in action.

```
[andreas@papaya:bin]$ ./demo.php
Welcome to the OAuth CLI client
Requesting a request token
Got a request token from the OAuth service provider [_45548a5b22451af19b6a93cd6e69a186296141]
Please go to this URL to authorize access: http://dev.andreas.feide.no/simplesaml/module.php/
Waiting 15 seconds for you to authenticate. Usually you should let the user enter return or o

Got an access token from the OAuth service provider [_ade3ebb6649341e40e832065ac763e9df75312b]
You are successfully authenticated to this Command Line CLI.
Got data [cn, sn, uid, eduPersonAffiliation, eduPersonEntitlement, eduPersonNickname, eduPers
Your user ID is : andreas@rnd.feide.no
[andreas@papaya:bin]$
```

Figure 6.13: OAuth Client interface

Documentation on this demo application is available online; see [\[Demo\]](#).

6.2 Preliminary Result 12: SimpleSAMLphp Translation Portal – Use-Case of Command Line Authentication

The SimpleSAMLphp project contains a popular web-based translation portal, which allows volunteers to translate the software into different languages. There have been many requests to reuse the translation portal for other software projects.

In January 2010, the SimpleSAMLphp translation portal went through a major update, making it more generic so that it can be used in any software project. The translation portal consists of two main components:

- A command-line client to download translated dictionary files and to upload definition files to the translation portal.
- The web-based translation portal for end-users to contribute with translation.

Authentication of the command line utility was enabled using the OAuth module in SimpleSAMLphp. This allows each software project to configure a set of users who are allowed to upload new definition files for the project. Thus, authentication makes use of the Identity Federation WebSSO solution using SAML 2.0.

6.3 Utilisation Outside the Task

An example of the utilisation described in Section 5.2 is illustrated by the Confusa project [\[Confusa\]](#). Confusa is a software project that provides an easy way for an end-user to request and get a X.509 certificate based on attributes released from the users' identity provided (IdP).

The Confusa project has already started using the SimpleSAMLphp translation portal for translating their web-based tool used for issuing personal certificates. Developers from the Confusa project are authorised to upload definition files for translating the software using the solution implemented in "Preliminary Result 12:

SimpleSAMLphp Translation Portal – Use-Case of Command Line Authentication”, using a command line utility and OAuth.

Using an established Identity Federation makes sense for several reasons:

- The users already have one well-maintained identity
- JRA 3 Task 2 do not have to maintain their own user database
- It scales to a large number of users.

The Confusa software has been used since February 2010 to implement a web portal for the TERENA Certificate Service (TCS) [[TERENA TCS](#)]. Confusa is SimpleSAMLphp-based and allows for federated authentication of end-users using Identity Providers of the participating Identity Federations.

The TERENA Certificate Service allows a variety of digital certificates to be offered to research and education institutions served by participating National Research and Education Networks (NRENs).

Confusa also supports a command line client for extracting certificates from the web-based service. As existing Identity Federations are mainly available for web-browsers only, Confusa is planning on making use of the work from the Identity Federation task on “Preliminary Result 11: Beyond WebSSO using OAuth - Implementation in SimpleSAMLphp” to allow the command line client to establish a session with the server part of Confusa and authenticate the user using existing Identity Federations before issuing the certificate.

7 Sub-Task VI: Federation Lab

The vision behind the Federation Lab is to provide a cross-federation test environment to validate whether a SAML entity conforms to the specifications agreed by the participating federations. This could be particularly useful once services like eduGAIN are operational and specific SAML 2.0 Profiles (like saml2int) are used.

This sub-task was not started in Year 1, due to the need to prioritise other sub-tasks.

A first version of the Federation Lab would probably be part of the plan for Year 2 of this project.

8 Future Work and Conclusions

During Year 1 use-cases mostly related to “VOP” and to “Beyond Web SSO”. New use-cases from the GN3 and other communities have emerged (some of which were not foreseen before the start of the project). Unfortunately not all the use-cases identified can be addressed by the Identity Federation Task and therefore a selection was deemed necessary.

Based on the preliminary results detailed in this document and on the use-cases identified, the Identity Federation future work will focus primarily on the following:

- Metadata Distribution

The most important focus of metadata distribution will be to complete the Metadata Aggregator specification, and begin designing more distributed models for metadata distribution. This is particularly important to enable eduGAIN to deal with a larger number of federations and with the related metadata.

- Federation Harmonisation

More effort will be required to complete the work on de-provisioning.

- Federation Lab

During the next year the Identity Federation Task expects to have results on the Federation lab sub-task; the goal is to provide an automated SAML conformance test suite that will be used as a Federation Lab for testing the interoperability of new components in SAML-based environments. Such a suite will enable federations, in particular small ones, to test new components without having a disruptive effect on the operational federations.

- Beyond Web SSO

The proof of concept based on OAuth, to implement authentication beyond Web-SSO by re-using the web session, has been proven to work. This approach, already adopted by production services such as Confusa, is likely to be adopted by others as well. It is envisaged that this sub-task will gain higher priority over the next few years. The aim is to investigate further alternatives that will enable the federated framework to support a wider range of applications. This would be particularly relevant to some of the services included in the GEANT Service Area.

- Virtual Organisations

Although a significant amount of work has been done in the area of Virtual Organisation (see Chapter 1 “Virtual Organisations”) more experience is needed with alternative data access APIs. Furthermore, various proof-of-

concepts, presented in Chapter 1, need more testing in real-life scenarios. Some of the identified scenarios are described in Section 8.1.

8.1 Real-Life adoption of VO Technology

As the proof-of-concepts from this sub-task become more stable, and the solutions become better documented, the objective is to see more real-life use-cases solved with VO technology.

8.1.1 Virtual Organisation Use-Case: TERENA Wiki

TERENA provide a wiki for collaboration between European NRENs in various areas. Users requesting access to this wiki span multiple identity federations, which makes the wiki an ideal use-case for authorisation and access control, as well as for testing VOP.

Until now, the wiki has required participating institutions to set a special "entitlement" flag in their LDAP user repository for those users that need to access the wiki. This is not an optimal solution as it imposes new requirements on participating institutions and presents some scalability issues. Some users may not be able to access the wiki with current practice because their institution does not have any procedures for setting "entitlement" values.

As the TERENA wiki uses SimpleSAMLphp for access control, it is ideally suited to the new Virtual Organisation modules implemented for SimpleSAMLphp as described in 2.1 "Virtual Organisation Management".

The plan is to implement this use-case for real-life use during 2010.

8.1.2 Virtual Organisation Use-Case: CLARIN

The CLARIN [\[CLARIN\]](#) project is a large-scale pan-European collaborative effort to create, coordinate and make language resources and technology available and readily usable. CLARIN offers scholars the tools to allow computer-aided language processing, addressing one or more of the multiple roles language plays (i.e. carrier of cultural content and knowledge, instrument of communication, component of identity and object of study) in the Humanities and Social Sciences.

Many of the resources available in the CLARIN language resource domain will not be accessible without adhering to some legal and/or ethical rules that are typically expressed in Codes of Conduct (CoCs) and license statements. While license statements are well known, CoCs need some explanation. CoCs define rules for proper usage and proper ethical behaviour, which are required before a user is allowed to access a resource (i.e. a user commits to adhering to these rules and the community implements controls to monitor and enforce behavior). We refer to all these as EULAs (End User License Agreements).

Representatives of the Identity Federation task met with the CLARIN project, to discuss how technology from this task can be applied to the CLARIN use-case. After evaluating various technologies, Identity Federations, in agreement with the CLARIN project participants, concluded that a solution based upon SAML 2.0 attribute queries and Shibboleth software may effectively solve their use-case.

In the proposed solution, a central EULA server will implement a user interface for collecting EULA agreements from users; this server will also act as an Attribute Authority running Shibboleth 2.0 IdP. All CLARIN Service Providers may be configured to collect EULA information about the current user during the login process.

The CLARIN project is planning to implement a proof of concept of this design with guidance from Identity Federations during 2010.

9 References

[CLARIN]	http://clarin.eu
[Confusa]	http://www.assembla.com/wiki/show/confusa
[Demo]	http://rnd.feide.no/content/federated-command-line-client-authentication-simplesamlphp-and-oauth
[edugain]	http://www.edugain.org
[esfri]	http://ec.europa.eu/research/infrastructures/index_en.cfm?pg=esfri
[FEIDE]	https://rnd.feide.no/content/metadata-aggregation-requirements-specification
[FeidOp]	http://rnd.feide.no/category/topics/feide-openidp
[FeidFoo]	https://foodle.feide.no/
[GMT]	http://www.switch.ch/aai/support/tools/gmt.html
[How to configure ShibIdP in a VO environment]	http://wiki.geant.net/bin/view/JRA3/ShibVOIdP
[ID-WSF]	http://www.projectliberty.org/liberty/resource_center/specifications/specifications_archives/liberty_alliance_id_ff_1_2_id_wsf_1_0_and_id_sis_1_0_specifications/
[Kalmar Union]	http://www.kalmar2.org
[Metadata-files]	https://hbe.edugain.bridge.feide.no/simplesaml/module.php/agggregator/?id=edugain&set=saml2
[Metadata-test]	https://rnd.feide.no/content/metadata-aggregation-testing-GÉANT3-jra3
[OAuth Attribute Query Protocol]	http://rnd.feide.no/content/oauth-attribute-query-protocol
[OAuth Core 1.0 Protocol Specification] (IETF Draft: draft-hammer-oauth-08)	http://tools.ietf.org/html/draft-hammer-oauth-08
[OAuth]	http://oauth.net/
[OpenID Federations]	https://rnd.feide.no/content/openid-federations
[RFC2119]	http://www.ietf.org/rfc/rfc2119.txt
[RFC2965]	http://www.ietf.org/rfc/rfc2965.txt
[saml2-bindings]	http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf
[saml2-core]	http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf
[saml2-frontchannel-slo]	https://rnd.feide.no/content/front-channel-single-logout-deployment-profile
[saml2-interoperable-profile]	http://saml2int.org/profile/current
[saml2-metadata-profile]	http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf
[saml2-profiles]	http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf
[SAMLsite]	http://saml2int.org/
[scoped]	https://spaces.internet2.edu/display/SHIB2/ResolverScopedAttributeDefinition
[SC]	https://rnd.feide.no/content/video-virtual-organization-proof-concept
[Shibboleth]	http://shibboleth.internet2.edu/

[Simple Metadata Aggregation Profile]	https://rnd.feide.no/content/simple-metadata-aggregation
[SimpleSAMLphp]	http://rnd.feide.no/simplesamlphp
[SP-Centric Attribute Aggregation]	http://rnd.feide.no/content/sp-centric-attribute-aggregation
[SpringFika]	http://code.google.com/p/springfika/
[TERENA TCS]	https://www.TERENA.org/activities/tcs/
[TERENA]	http://TERENA.org
[User-Centric document]	https://intranet.geant.net/sites/Research/JRA3/T2/Documents/user-centric-v_1_1.doc
[Virtual Organisations]	https://rnd.feide.no/content/virtual-organizations
[vo-chad]	https://spaces.internet2.edu/display/~lajoie@idp.protectnetwork.org/VOPlatform
[VO-CONCEPT]	http://www.switch.ch/aai/about/vo-concept/
[VO-Poc_demo]	http://www.switch.ch/aai/downloads/VO-PoC-Demo.mov
[saml2int1]	http://saml2int.org/

Glossary

AAI	Authentication and Authorisation Infrastructure
API	Application Programming Interface
CoC	Code of Conduct
EULA	End User License Agreement
GMT	Group Management Tool
IdP	Identity Provider
ID-WSF	Identity Web Services Framework
JSON	JavaScript Object Notation
LDAP	Lightweight Directory Access Protocol
NREN	National Research and Engineering Network
PoC	Proof of Concept
REST	Representational State Transfer
SAML	Security Assertion Markup Language
SLO	Single Log Lout
SOAP	Simple Object Access Protocol
SP	Service Provider
SSO	Single Sign On
TCS	TERENA Certificate Service
VO	Virtual Organisation
VOP	Virtual Organisation Platform