Title	**Authentication Final Prototype (D12.3)**
Work Package	12
Authors	The UK Data Archive Shibboleth Development team with support from the FEIDE team
Source	UK Data Archive developed software
Date	December 2009
Dissemination Level	PU (Public)

D12.3 has been developed at the UK Data Archive and based on its Shibboleth system for the management of nationally distributed resource providers. This system was extended to include the Norwegian counterpart of UKAMF (UK Access Management Federation); Felles Elektronisk IDEntitet (Feide) (Eng: Common Electronic Identity) to demonstrate the feasibility of providing Single Sign On across two national Shibboleth-based federations.

The application can be accessed at:
https://shib-portal-cessda.data-archive.ac.uk/Cessda-Test/

Select access from FEIDE and use the following credentials:

Username: test
password: 098asd

This user name and password have been set up as a test credential for the FEIDE Federation. Any user, who has registered with the UK Data Archive, can test the system using their UK Data Archive login and password. In the latter case, their own email address will be displayed on the screen.

The technical overview of the application is appended below.

CESSDA-SHIBBOLETH

Technical overview

UKDA IDP section

Created by:	Vasuda Peddi
Maintained by:	Vasuda Peddi , IDP
Contributor(s):	John Payne, John Shepherdson, IDP
Version:	01.02
Controlled document:	N/A
Last amended:	20100722
Review due date:	N/A

UK Data Archive
University of Essex
Wivenhoe Park
Colchester
Essex, CO4 3SQ, UK

info@data-archive.ac.uk
+44 (0) 1206 872001

www.data-archive.ac.uk

Contents

Document Control

Version	Notes	Last Amended
01.02	Amended by (JWS) Updated for external release	2010-01-09
01.01	Created by (VP) First version, for internal use	2009-12-09

Replaces or supersedes

N/A

Review terms

Prior to release for external consumption.

Is related to

N/A

Scope

This document provides a technical overview detailing why, and how, Shibboleth has been implemented for the CESSDA SSO (Single Sign On) project.

1. Introduction

The CESSDA SSO Project has been created as a means of implementing and testing a potential technical solution for single-sign-on across multiple federations, for the CESSDA Portal. Unlike the Data Archive's ESDS and Census services provide access to datasets for UK institutions only, CESSDA operates across different European countries. Because of this, it is not enough to simply use the UK Access Management Federation (UKAMF) to service our requirements. If we did, any overseas users would not be able to log in to the CESSDA Portal, as they would never find their Home Organization within the Discovery Service.

To demonstrate the concept of a Single-Sign-On across multiple federations, we currently use UKAMF and the Norwegian Felles Elektronisk IDEntitet (FEIDE) and can accept users from any of the institutions within either Federation. Having proved the concept, there is no technical impediment to adding other federations as required.

Note: For testing we used FEIDE and UK federations. The metadata from these two providers are used within the Service Provider of the Virtual Organization Service Provider (VOSP) and the Discovery Service (DS).

Shibboleth is used within the Data Archive to protect the ESDS and Census datasets using the following process:

1. A User from establishment (A) wants to access a resource at location (B);
2. The user is redirected to the standard 'Where Are You From' (WAYF) service to ascertain their **Home Organization (HO)** from a drop down list of valid institutions. They are then redirected to establishment (A) and asked to log on with their normal account details.

Authentication from location (A) establishes that the user is who they say they are;

3. Back end interrogation from location (B) then queries core attributes about the individual from location (A), to determine if they have the necessary **Authorisation** to access the resource they have requested and responds accordingly, either granting or denying access;

   The user is effectively given a role (such as MEMBER, or STAFF, or STUDENT) which determines whether the user request can proceed or not, via the VOSP, to the Service Provider. The resource is set up to allow an Authenticated user with STAFF Authorisation to access the data.

The CESSDA SSO project works in the same basic way, however, it incorporates FEIDE as well as the UK Federation when selecting your Home Organization (HO) from the Discovery Service.

2. CESSDA SSO Components

The CESSDA SSO Authentication system contains the components described below.

2.1. Portal-SP (Service Provider for CESSDA Portal)

Any request for protected information within the CESSDA Postal is caught by the SSO process. It is the Portal-SP that is ultimately responsible for granting/denying access to these requested resources. In a conventional Shibboleth transaction, the Service Provider (SP) will communicate with the Home Organization IdP (Identity Provider) of the user – which is established by a Discovery Service (DS) WAYF, to ensure that they have the correct authority AND authorisation to access the resource. However, as CESSDA Portal has implemented a VOSP, the Portal-SP points directly to the Proxy IdP within the VOSP.

See Appendix A for pictorial examples of both a VOSP and a standard Shibboleth transaction.

2.2. VOSP (Virtual Organization Service Provider)

Due to the nature of the data we hold, Shibboleth authentication and authorisation against the user's HO are simply not sufficient to allow access to a protected service. The UKDA has an additional registration process which captures the user's information in detail. This process is only available AFTER a successful authentication.

To have a centralised registration system within ESDS, the VOSP model was designed by protecting the proxy-IdP with the proxy-SP. The same VOSP solution has been implemented for CESSDA. The proxy-SP of the VOSP redirects the user to their HO-IdP via Discovery Service-WAYF (part of VOSP model).

Once the user has authenticated against their HO-IdP, the proxy-SP of VOSP requests user attributes from the HO-IdP. If the attribute check is successful then the proxy-SP of the VOSP will pass the request to the proxy-IdP of VOSP. The proxy-IdP of the VOSP queries the centralised database using the unique id **edupersontargetedId** obtained from the HO-IdP, and passes the values to the Portal Service Provider in the form of attributes.

See Appendix A for pictorial examples of both a VOSP and a standard Shibboleth transaction.

2.3. UKAMF (UK Access Management Federation for Education and Research)

The UKAMF provides a single solution to access online resources and services for education and research. The Federation basically maintains a detailed list of members (institutions). These institutions may be either Identity Providers or Service Providers.

Feide ("Felles Elektronisk IDEntitet" - Norwegian)
Feide is the Norwegian equivalent to the UKAMF. It has been as widely adopted in Norway as the UK Federation in the UK.

2.4. Discovery Service

For a Shibboleth transaction to succeed, the user must be able to log in at their Home Organization

(HO). Because the CESSDA Portal model incorporates two Federations (UKAMF and FEIDE), this requires a custom WAYF called a Discovery Service WAYF. This is installed and configured as part of the VOSP model.

This Discovery Service WAYF User Interface presents the user with two list boxes:

- The left-hand list contains the federations (UKAAM or FEIDE);
- The right-hand list contains the IdPs of the federation selected in the left-hand list.

2.5. Registration

This is the final component is the actual registration page on the website itself. It captures the details that the CESSDA Portal requires to allow a user to actually acquire the data.

As part of the registration process, the user has to accept an End User Licence. Until this is done, no data can be obtained. Obviously this is a once only process for the user. The next time they log on to the site via Shibboleth, the proxy IdP is handed the Unique Id for the authenticated user and retrieves their details automatically.

Note: for the CESSDA SSO prototype, the registration page has been implemented with only three fields i.e. firstname, lastname and email address.

3. Current Issues

The **UKAMF** requirement for Shibboleth authorisation is based upon the existence of the following Core Attributes:

- **TargetedID** Unique Id of the user. This is an opaque string created from the users name and the addition of some ‘salt’;
- **ScopedAffiliation** Where the user originates from and their role. (e.g. role@institution. For example, staff@case.edu).

These attributes are recognised and required by virtually all institutions.

FEIDE does NOT currently provide us with any **ScopedAffiliation**. The current CESSDA–VOSP is only authorising requests based upon **TargetedID**. We do not know if this is a symptom of us using a test account.

4. Appendix: VOSP Example

The Virtual Organization Service Provider (VOSP) consists of both a Service Provider (SP) and an Identity Provider (IdP) as shown in Figure 1.

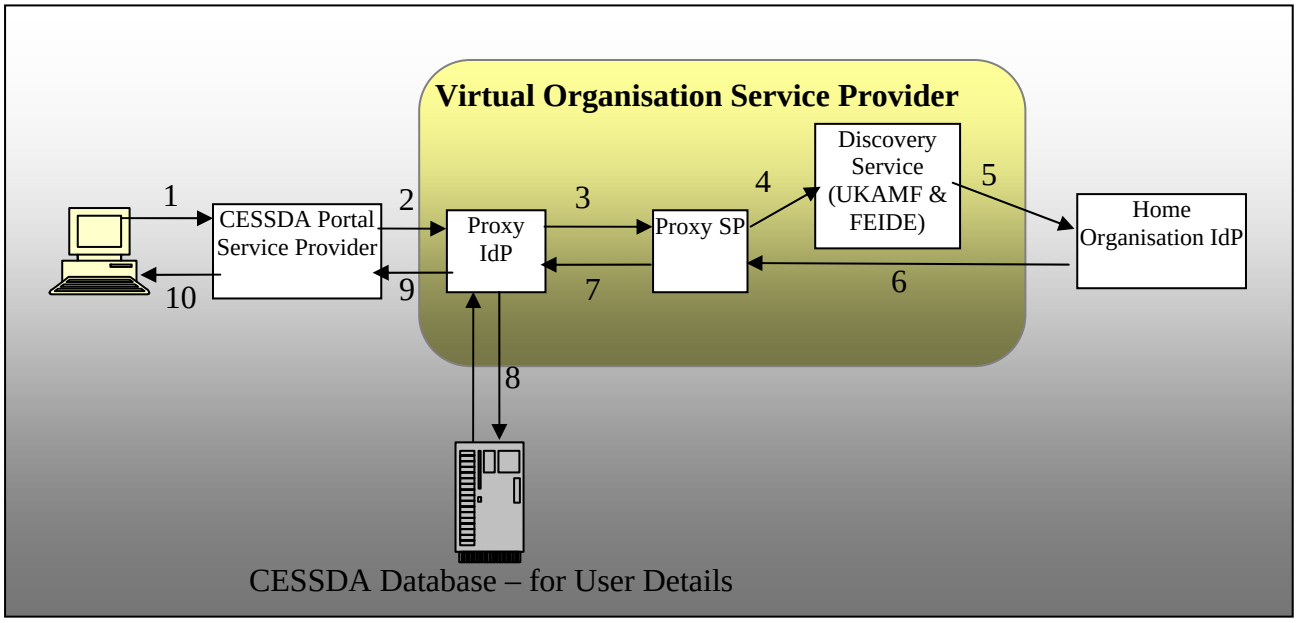

Figure 1: VOSP transaction flow

For the user, the overall process remains unaffected. The user is still authenticated against their Home IdP. However, there is now an extra phase sitting between the SP (which is making the request) and the IdP authorising the request. This does not interfere with the overall SP to IdP model. It does however provide the opportunity to capture the details necessary for registration within the process. The steps in the transaction flow shown in Figure 1 are explained in Table 1.

	Action
1	A user attempts to access the resources of the portal-SP for which access is governed by the one-stop registration system
2	This directs the user to the Virtual Organization Proxy IdP
3	The proxy IdP is protect by the Proxy SP
4	The Virtual Organization Proxy SP now needs to authenticate, so it directs the user to the WAYF service, which incorporates BOTH UK Federation and FEIDE Organizations
5	The user authenticates at their Home Organization (IdP)
6	The Home Organization replies to the Virtual Organization with SAML authentication assertion containing a handle. The Virtual Organization uses this handle and address of the Home Organization Attribute Authority to request attributes (**eduPersonTargtedID** and **eduPersonScopedAffiliation**). The Home Organization Attribute Authority releases **eduPersonTargtedID** and **eduPersonScopedAffiliation** to the SP in the Virtual Organization. **NB. Currently, FEIDE does NOT return a value for Scoped Affiliation.**
7	The Virtual Organization Attribute Authority now consults the Attribute Release Policy for a directory entry corresponding to the handle.
8/9	The Virtual Organization Attribute Authority releases the required attributes obtained from the user's entry from the CESSDA Users database to the initial SP.
10	Based on the attributes, the SP either returns the user to the one-stop registration system (separate SP) or allows access to the protected resource

Table 1: VOSP transaction details

Note: Compare this with the standard Shibboleth transaction flow, show in Figure 2. As you can see, the overall process is the same for the user journey. The request starts with an SP request, is routed to an IdP for Authorisation, and ends back at the initial SP.

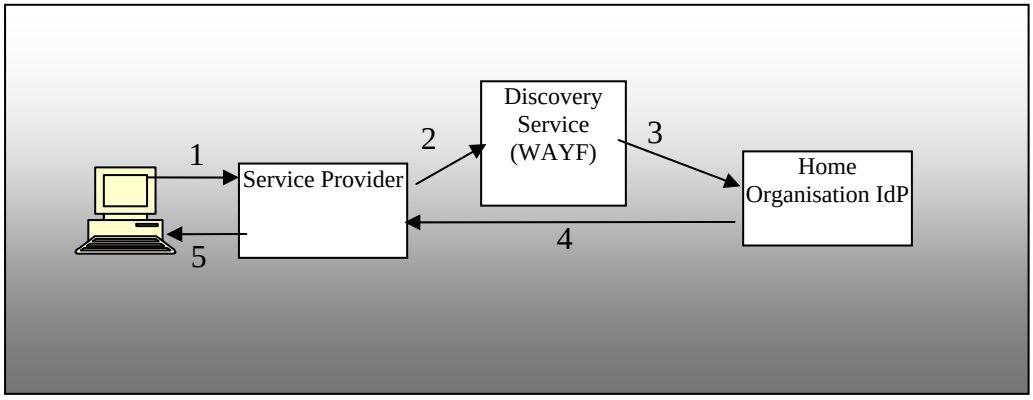

Figure 2: Standard Shibboleth transaction flow

The steps in the transaction flow shown in Figure 2 are explained in Table 2.

	Action
1	A user attempts to access the resources of the portal-SP for which access is governed by the one-stop registration system.
2	This directs the user to the Virtual Organization Proxy IdP
3	The proxy IdP is protect by the Proxy SP
4	The Virtual Organization Proxy SP now needs to authenticate, so it directs the user to the WAYF service, which incorporates BOTH UK Federation and FEIDE Organizations.
5	The user authenticates at their Home Organization (IdP)
6	The Home Organization replies to the Virtual Organization with SAML authentication assertion containing a handle. The Virtual Organization uses this handle and address of the Home Organization Attribute Authority to request attributes (**eduPersonTargtedID** and **eduPersonScopedAffiliation**). The Home Organization Attribute Authority releases **eduPersonTargtedID** and **eduPersonScopedAffiliation** to the SP in the Virtual Organization. **NB. Currently, FEIDE does NOT return a value for Scoped Affiliation**
7	The Virtual Organization Attribute Authority now consults the Attribute Release Policy for a directory entry corresponding to the handle
8/9	The Virtual Organization Attribute Authority releases the required attributes obtained from the user's entry from the CESSDA Users database to the initial SP
10	Based on the attributes, the SP either returns the user to the one-stop registration system (separate SP) or allows access to the protected resource

Table 2: Standard Shibboleth transaction details