

SAFARI UKDA: Shibboleth Authentication For Access to the Resource Infrastructures of the UKDA

Project

Project Acronym	SAFARI UKDA	Project ID	
Project Title	Shibboleth Authentication For Access to the Resource Infrastructures of the UKDA		
Start Date	21 March 2005	End Date	20 March 2006
Lead Institution	UK Data Archive, University of Essex		
Project Director	Kevin Schürer		
Project Manager & contact details	Karen Dennison, UK Data Archive, University of Essex, Wivenhoe Park, Colchester, CO4 3SQ. Tel: 01206 873574. Email: kdenn@essex.ac.uk		
Partner Institutions	None		
Project Web URL	http://safari.data-archive.ac.uk		
Programme Name (and number)	Core Middleware: Infrastructure		
Programme Manager	Ann Borda		

Document

Document Title	Shibboleth Dynamic Specification		
Author(s) & project role	Karen Dennison, Project Manager Kosigin Liver Pitchikan, Systems Developer		
Date	04 November 2005	Filename	Shib_spec_v2.doc
URL	N/A		
Access	<input checked="" type="checkbox"/> Project and JISC internal		<input type="checkbox"/> General dissemination

Document History

Version	Date	Comments
1.0	19 July 05	First draft, written by Lucy Bell and Kosigin Liver Pitchikan, reviewed by SAFARI team, submitted to MIMAS, EDINA and MATU for comments, 1 August 2005.
2.0	04 November 05	First draft updated by Karen Dennison and Kosigin Liver Pitchikan, reviewed by SAFARI team

Table of contents

1	Background.....	3
1.1	AIMS AND OBJECTIVES	3
2	Requirements	3
3	Technical solutions.....	4
3.1	VOSP.....	5
4	Issues	5
5	Implementation	6
6	Tracking summary of changes	6

1 Background

The UK Data Archive (UKDA) is the central registration hub for several JISC-funded MIMAS, EDINA and ESDS services. It manages eight Athens resources. Three are hosted at Essex, four at MIMAS and one at EDINA. These resources are all served by the UKDA's one-stop registration service, which encompasses the Census Registration Service (CRS) and ESDS registration.

Registration is a prerequisite of the majority of data depositors, and many have differing requirements. The one-stop system was developed in order to streamline these needs and to ensure that users' access to the data was as trouble-free as possible. The primary aim of this new work is to rationalise further the user's journey from desk to data.

SAFARI will apply a Shibboleth target to ESDS, the CHCC Collection of Historical Censuses and the Census Registration Service. Applying Shibboleth middleware to the system must not only provide the users with an alternative entrance to the one-stop registration service, it must also enhance the existing service. It should provide the UKDA with the opportunity to investigate the possibility of applying more fine-grained access control and make the system more flexible; it should also allow the services the UKDA manages to be used within the Athens-Shibboleth gateway.

1.1 Aims and objectives

The central **aim** of the project is:

- to apply Shibboleth middleware to the three UKDA-hosted ESDS and Census-related resources which make use of the one-stop registration system.

The key **objectives** are:

- the establishment of Shibboleth resource targets for ESDS, the Census Registration Service and the CHCC Collection of Historical Censuses;
- the embedding of these resource targets within the one-stop registration service;
- the investigation and establishment, within the target system, of a transfer mechanism to identify registered users and thus prevent users from having to register more than once;
- the investigation and establishment of a method of target-to-target communication of the details of special conditions to which users have agreed;
- the evaluation of the system via user and stakeholder consultation.

2 Requirements

The system developed will need to be embedded within the one-stop registration system. It will have to be compatible not only with the Essex-based services with which SAFARI is working, but also with the services for whom the live registration system registers users at MIMAS and EDINA. Specifically, these are:

MIMAS

- Census Dissemination Unit (Casweb)
- Census Interaction Data Service (CIDS)
- Samples of Anonymised Records
- ESDS International

EDINA

- UKBORDERS

The registration system currently uses Athens for both authentication and authorisation. This has brought with it some advantages (it is an 'off the peg' solution and is used nationally throughout academia) and some disadvantages (the resources for whom it authenticates users have less control over authorisation than would in some cases be desirable; additionally, the profiles used for recording users' registration status may not be over-written). The system developed by the SAFARI team will try to address some of the gaps within the current set-up, while retaining its robustness.

In order to slot easily into the existing registration system, the new development must:

1. provide communication from the registration database to the Service Providers (SPs) in order to identify each user's registration status prior to their being granted or denied access to the data;
2. provide a system in which more fine-grained access control may be applied;
3. be interoperable with systems already established at MIMAS and EDINA.

It is worth noting that, at present, the external services making use of the registration system need only to know the following, in terms of attributes:

1. user's registration status (registered user, expired user etc.);
2. user's entitlement to use data covered by special conditions;
3. a persistent identifier which will link the user to their registration record, in case of breach.

In terms of attributes, the registration system only needs the persistent identifier, which must be applied to the user's registration record, as all other details are gathered during the registration process. That said, it would be very helpful to be provided with details such as user's name, role, department, institution, email address etc. as this would reduce the burden on the user still further.

3 Technical solutions

Following consultation with colleagues from Guanxi, MIMAS and EDINA, and with Shibboleth developers and implementers overseas, four solutions to the registration system development were identified (those people who either suggested them or worked them out are shown in brackets):

1. The UKDA acts as a '**proxy**' **IdP** as well as a target, authenticating users a second time against its registration database (Scott Cantor, with reservations/Kosigin Liver Pitchikan, UKDA);
2. The **UKDA is pulled into the primary authentication flow**, with the WAYF located in Essex and registration-related attributes pulled from the registration database (Alistair Young, Guanxi);
3. The UKDA follows the model of the **Virtual Organisation Service Provider (VOSP)** with its centralised attribute repository (John-Paul Robinson, University of Alabama);
4. The UKDA sets up an **external call** from the SPs to its database, outside the Shibboleth protocol (Kosigin Liver Pitchikan, UKDA).

Preliminary details of each of these options appear in version 1 of the dynamic project specification document. After careful consideration of each option, it was decided to follow option 3, the VOSP model, the details of which are provided below. Should option 3 be deemed to not work satisfactorily, option 4 can be implemented as a failsafe solution.

3.1 VOSP

UKDA has modified the VOSP model as shown in the diagram below –

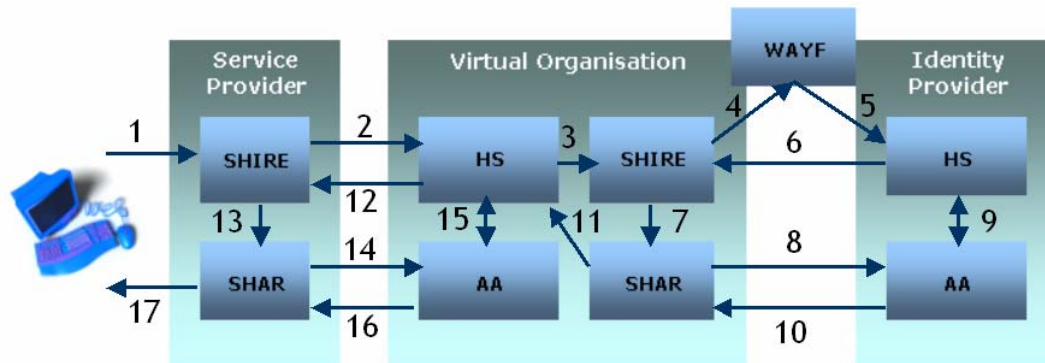


Figure 1: the Virtual Organization Service Provider

In the diagram above, one service provider is shown. This represents one of many service providers for which UKDA provides one-stop registration. SAFARI UKDA is represented by the Virtual Organisation box and consists of a proxy IdP and proxy SP.

The following steps attempt to capture the flow:

1. a user tries to access the resources of a service provider for which access is governed by the one-stop registration system.
2. this directs the user to the VO Handle Service (HS)
3. a request is sent to the VO SHIRE
4. the SHIRE directs the user to the WAYF
5. the user authenticates at their HO (IdP)
6. HO HS replies to VO SHIRE with SAML authentication assertion containing a handle
7. VO SHIRE hands the handle to the VO SHAR
8. VO SHAR uses handle and address of HO AA to request attribute (eduPersonPrincipalName)
9. HO AA consults ARP for directory entry corresponding to handle
10. HO AA releases eduPersonPrincipalName to the VO SHAR
11. VO SHAR directed to VO HS
12. VO HS directed to service provider (target) SHIRE
13. SP SHIRE passes handle to SP SHAR
14. SP SHAR arrives at VO AA to request attributes
15. VO AA consults ARP for directory entry corresponding to handle
16. VO AA releases attributes to SP SHAR
17. 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

4 Issues

It was decided not to pursue Options 1 and 2 due to the following issues / obstacles

1. Lack of unique identifier within the UKDA AA request
2. Requirement for all IdPs to change the data flow by adding a plugin for the UKDA attributes
3. Requirement for trust between each Identity Provider (IdP) and the UKDA, as well as trust between each Identity Provider and each Service Provider (SP)
4. Requirement to add additional attributes relating to the user's registration status to each resource

The VOSP model was chosen since

- the normal Shibboleth flow is not broken
- it is possible to employ the scoped eduPersonPrincialName attribute which is persistent across SPs
- there is no requirement for SPs or IdPs to install any additional plugins/make any additional modifications
- no trust issues arise between IdPs and UKDA or between IdPs and other SPs

5 Implementation

SAFARI UKDA has joined the SDSS federation and set up -

- IdP and SP to act as proxy origin and proxy target (VOSP)
- SP called CRS to provide a one-stop registration store where all users need to register. This uses MS sql server database to store user registration information and acts as AA for SAFARI UKDA proxy origin
- SP for CHCC at <https://chcc.essex.ac.uk/shibboleth/> registered with SDSS Federation

6 Tracking summary of changes

Version	Date	Changes made	Staff
1.0	19 July 05	None: first version of document.	LB, KLP
2.0	04 Nov 05	Updates to sections 3,4 and 5	KD, KLP

Appendix A

Glossary of acronyms

Acronym	Meaning
AA	Attribute Authority
ARP	Attribute Release Policy
CHCC	Collection of Historical and Contemporary Census material
CRS	Census Registration Service
ESDS	Economic and Social Data Service
HO	Home Organisation
HS	Handle Service
IdP	Identity Provider
SAFARI UKDA	Shibboleth Authentication For Access to the Research Infrastructures of the UKDA
SHAR	Shibboleth Attribute Requester
SHIRE	Shibboleth Indexing Reference Establisher
SP	Service Provider
UID	Unique Identifier
UKDA	UK Data Archive
VO	Virtual Organisation
VOSP	Virtual Organisation Service Provider
WAYF	Where Are You From service