University of Oxford
Summary Integration Requirements for SSO

Table of Contents

1. Introduction

This document describes the Single Sign-On (SSO) and Access Management environment at the University of Oxford. It summarises requirements and options for application integrators & implementers to use for authenticating users and controlling access to applications. The systems that support this are provided by the Identity and Access Management (IAM) team, IT Services, and are designed for use by the whole of the collegiate University.

2. Requirements list

Below is a summary list of requirements for solutions/applications that need to integrate with the University of Oxford's central systems for authentication and authorisation (otherwise referred to as 'Single Sign-On (SSO) system').

#	Requirement	Requirement Level
Web based access using browser		
1	For web based access the solution MUST integrate with the University Single Sign-On system(s) using one of the following options, in order of preference: i. SAML2 Federation using the Oxford Shibboleth Identity Provider service (via the UK Access Management Federation for Education and Research [3] - or other equivalent regional federation that participates in EduGAIN) ii. WS-Federation using the Oxford ADFS service	MUST
Option 1.i SAML2 Federation		
2	For solutions using option 1.i (SAML2), the Service Provider metadata MUST be registered with the 'Federation' and be published in the 'Federation's' published metadata file.	MUST
3	For solutions using option 1.i (SAML2), Assertions sent to the Service Provider SHALL be encrypted with the Service Provider's public certificate. That public certificate SHALL be in the published metadata for that Service Provider. The Service Provider MUST be capable of decrypting this assertion.	MUST
4	For solutions using option 1.i (SAML2), the Service Provider SHOULD except an eduPersonTargetedID or eduPersonPrincipalName [2] as the unique identifier.	SHOULD
5	If it needs to, the solution MAY make use of the SSO assertion attributes eduPersonOrgUnitDN and eduPersonPrimaryOrgUnitDN [2] to confirm unit affiliation. Release of these must be requested and approved as part of the SSO integration.	OPTIONAL
6	If it needs to, the solution MAY make use of the SSO assertion attribute eduPersonScopedAffiliation [2] to confirm the person's type of affiliation to the organisation. E.g. member@ox.ac.uk/staff@ox.ac.uk/student@ox.ac.uk etc. Release of these must be requested and approved as part of the SSO integration.	OPTIONAL
7	The Service Provider SHOULD be capable of generating sign-in requests. In other words SP-initiated sign-on is preferred to IDP-initiated sign-on.	SHOULD
Option 1.ii WS-Federation using ADFS		

8	For solutions using option 1.ii (ADFS), the operators of the Relying Party MUST have a procedure (automatic or manual) for updating the ADFS metadata that the Relying Party consumes, and include such updates in their annual support provision.	MUST
9	For solutions using option 1.ii (ADFS), claims sent to the Relying Party will be encrypted with the Relying Party's public certificate. This certificate will have to be securely sent (& fingerprint confirmed out of band) by the third party to the IAM Team as part of the SSO integration. The Relying Party MUST be capable of decrypting these claims.	MUST
10	For solutions using option 1.ii (ADFS), the Relying Party MUST verify that the claims it receives are authentic by checking that the signature matches that of the Oxford ADFS service's published signing certificate.	MUST
11	For solutions using option 1.ii (ADFS), the Relying Party SHOULD except an nameidentifier or UPN as the unique identifier.	SHOULD
12	If it needs to, the solution MAY make use of the SSO claims for department, eduPersonOrgUnitDN and eduPersonPrimaryOrgUnitDN [2] to confirm unit affiliation. Release of these must be requested and approved as part of the SSO integration.	OPTIONAL
13	If it needs to, the solution MAY make use of the SSO claim for role to confirm the person's type of affiliation to the organisation. E.g. member@ox.ac.uk/staff@ox.ac.uk/student@ox.ac.uk etc. Release of these must be requested and approved as part of the SSO integration.	OPTIONAL
14	The Relying Party SHOULD have an automated mechanism to publish and make its metadata publicly accessible.	SHOULD
General		
15	Email address (normally defined as the 'mail' attribute) SHOULD NOT be used as a unique identifier.	SHOULD NOT
16	Release of Personal attributes to Service Providers or Relying Parties as part of the SSO login MUST go through a formal approval process. This approval is subject to these attributes being essential for the application to function and make authorisation decisions.	MUST
Authentication for non-browser based clients		
17	Authentication for an installed desktop application can integrate with the University Single Sign-On system(s) using one of the following options, in order of preference: i. Web based authentication using 1.i or 1.ii using an embedded browser. ii. WS-Trust authentication (active profile) using the Oxford ADFS service. iii. Direct Kerberos authentication using Oxford's Kerberos KDC (MIT Kerberos).	MUST

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [1].

3. Authentication stack overview

At the University of Oxford we have a 3 layer authentication stack comprised of the following services: MIT Kerberos; Shibboleth Identity Provider (IdP) providing SAML federation; and Active Directory Federation Services (ADFS) supporting authentication using the WS-Federation & WS-Trust profiles. Each of these provide authentication protocols specific to that layer of the stack and applications can integrate at potentially any of these layers.

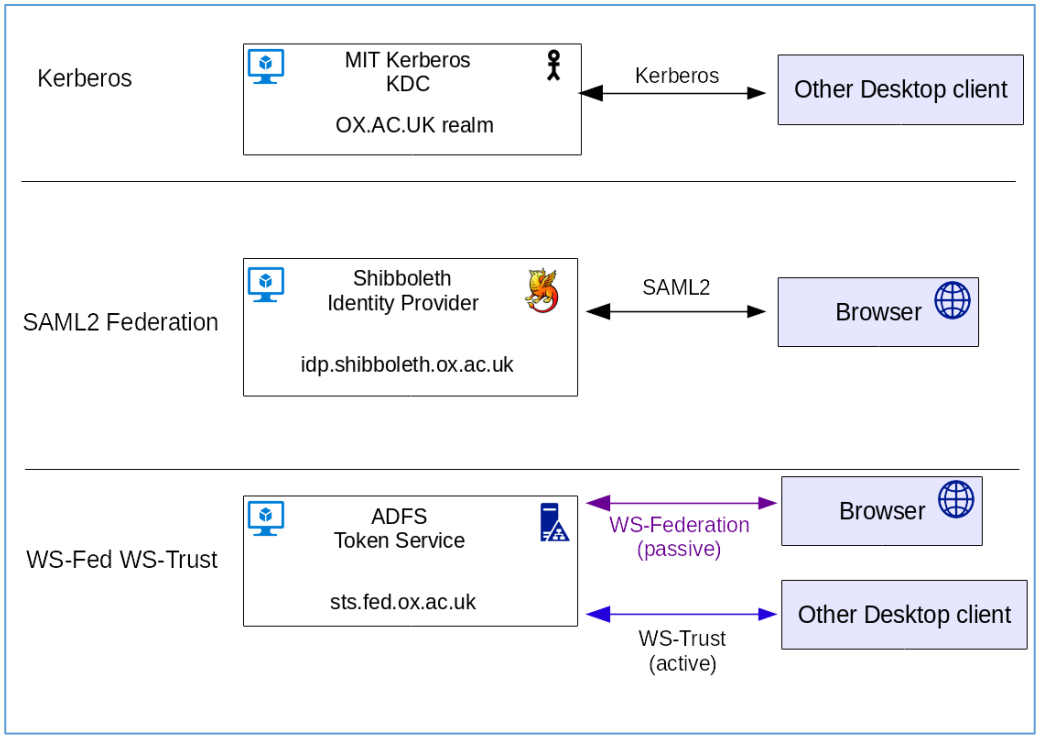

Figure 1: Oxford SSO stack

These technologies are reasonably common and will be familiar to most application integrators. However, it should be noted that there are some constraints on these services due to the large and diverse environment that they serve and our policy of adhering to the best security practice and open standards. These constraints mean in practice that some of the options that integrators might expect to be available, given the technologies that we use, aren't actually supported by us. For example, we only operate ADFS as a means of providing WS-Federation & WS-Trust authentication to applications that can't use SAML federation (and it hands over to the Shibboleth IdP to provide the Claims Provider role). Our ADFS service isn't backed by a full Active Directory that holds credentials and user attributes and so other authentication options that are dependent on a typical Active Directory being available aren't supported. For example, AD group membership cannot be used in an authorisation decision.

It's also worth pointing out that there is no common desktop throughout the whole University. Depending on the organisational unit, some workstations are joined to a 'local' Active Directory Domain which provides authentication for their desktop session, but that Domain (and credentials) won't be equivalent to the central MIT Kerberos realm, OX.AC.UK, that is used by SSO. Therefore,

any desktop client using direct Kerberos (SSO) authentication (Requirement 13, option iii) will typically have to manage its own Kerberos tickets.

We expect the majority of modern applications to use browser based access and SSO for those will normally be provided by integration with the SAML2 Federation layer of our SSO stack. This is a mature reliable service based on open standards, scalable and well supported. We require that the solution supplier is registered with the UK Access Management Federation [3] or one of the equivalent regional federations that participate in EduGAIN [4] (Requirement 1.i), and that metadata for the solution/application is published by the federation as part of that registration (Requirement 2). The SAML assertion provided to the solution will be encrypted (Requirement 3) and a suitable unique identifier should be used (Requirement 4). Other personal attributes can be made available to the solution as part of the assertion but release of these has to be formally requested by the solution's procurement representative for the University of Oxford and authorisation approved (Requirement 16).

4. References

[1] Key words for use in RFCs to Indicate Requirement Levels, https://www.ietf.org/rfc/rfc2119.txt

[2] eduPerson Schema, https://www.internet2.edu/media/medialibrary/2013/09/04/internet2-mace-dir-eduperson-200806.html

[3] UK Access Management Federation, http://www.ukfederation.org.uk/

[4] EduGAIN https://technical.edugain.org/status