University of Oxford

Integration Requirements for Federated SSO

Project Name:	**ITS412 ADFS (IAM Project #2)**		
Document status:	**Approved**	Version no:	1.0
Intended audience:	**IT Services internal and 3rd party application providers**		
Date:	**31/01/2019**		
Author(s):	**Julian Williams**		
Owner/Job Title:	**IT Services, IAM Team**		

Document History

Revision History

Version Number	Revision date	Author	Summary of Changes
0.1	25/08/2016	JW	Initial draft
0.2	26/08/2016	JW	Corrections and amendments following feedback from IAM
0.3	06/09/2016	JW	Amendments following feedback from Ben Malin.
0.4	19/12/2016	JW	Additions & amendments before publishing on SharePoint. Incl: SSO arch diag; Implementation checklist; tabulated options for user provisioning.
0.5	17/01/2018	JW	Inclusion of sections covering integrating with SAML2 (Shibboleth) federation. Update of ADFS details to match current ADFSv4 environment.
0.6	31/01/2019	JW	Incorporated feedback from Kev Webber Removed comments about the ADFS staging env being private access.
1.0	18/02/2019		Approved

Approvals

This document requires the following approvals. Signed hard copies will be/are filed in the project files.

Name	Job Title	Date
Nigel Brown	IT Services, IAM team leader	18/02/2019

Table of Contents

1. Introduction

This document specifies the requirements that a supplier must meet in order to use the University of Oxford's federated Single Sign-On (SSO) together with integration and implementation detail.

It is anticipated that the requirements will be used in assessing an application's existing capability to integrate correctly with Oxford's federated SSO and also defining specification for any development work to add capability to do the same.

Services integrating with Oxford's federated SSO have a choice of either:

i. Using SAML2 Federation and Oxford's SAML2 Identity Provider service (Shibboleth)
ii. Using WS-Federation Claims and Oxford's Claims Provider service (ADFS).

This document covers both options. If both options are possible then integrations should choose option i) SAML2 Federation, because of the maturity, scalability and level of support for the Shibboleth Identity Provider service that is used at Oxford.

The systems that run Oxford's federated SSO are provided and supported by the Identity and Access Management (IAM) team, IT Services, and are designed for use by the whole of the collegiate University.

2. Oxford SSO Architecture 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.

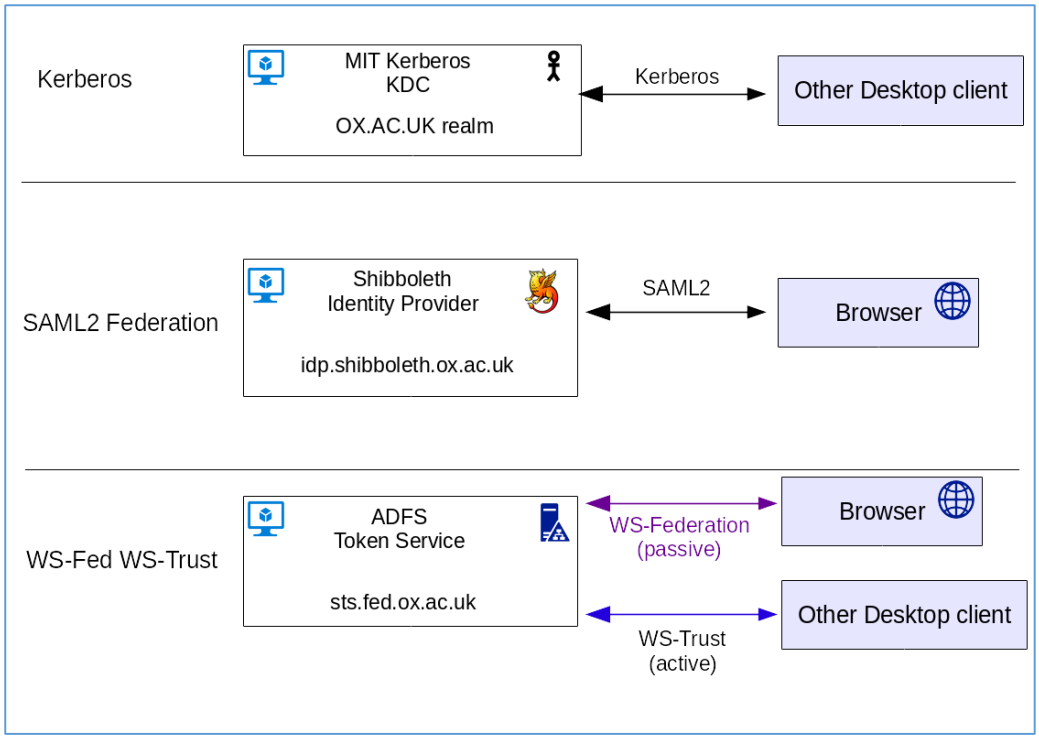

Figure 1: Oxford SSO architecture. Showing the 3 different layers of the authentication stack. WS-Federation; SAML2 and Kerberos

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 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.

3. Requirements

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].

3.1. Requirements for integrating with Oxford's federated SSO using SAML2 and the Shibboleth Identity Provider service

This is a list of requirements for a SAML Service Provider to integrate with Oxford Federated SSO. These requirements are in addition to what is normally required to integrate with SAML2 SSO.

Table 1: List of requirements for a SAML Service Provider.

REQ #	Description	Details
1	The 3rd party application provider MUST be a member of the UK Access Management Federation [4] or one of the international federations that participate in EduGAIN [5] (hence referred to as the Federation).	
2	The Service Provider metadata MUST be registered with the Federation and be present in the Federation's published metadata file.	
3	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.	
4	The Service Provider SHOULD except an eduPersonTargetedID or eduPersonPrincipalName [2] as the unique identifier.	Section 6.2
5	The Service Provider SHOULD NOT use the 'mail' attribute (email address) as a unique identifier.	Section 6.2
6	Only a minimum set of SAML2 Attributes are released by default. Additional personal Attributes that the Service Provider requires MUST have their release approved. This approval is subject to these Attributes being essential for the application to function and make authorisation decisions.	Section 6.4
7	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.	Section 6.1.1
8	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.	Section 6.1.1

	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.	
9	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.	

3.2. Requirements for integrating with Oxford's federated SSO using WS-Federation and the ADFS Claims Provider service

This is a list of requirements for an ADFS Relying Party to integrate with Oxford Federated SSO. These requirements are in addition to what is normally required to integrate with WS-Federation SSO.

Table 2: List of requirements for a WS-Federation Relying Party.

REQ #	Description	Details
1	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.	Section 5.5
2	The Relying Party MUST provide an X509 certificate to encrypt claims. This certificate SHOULD be self-signed & long-lived (say 10 years).	Section 5.4.1
3	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.	Section 5.4.1
4	The Relying Party SHOULD use the nameidentifier or UPN claim as the unique ID.	Section 6.2
5	The Relying Party SHOULD NOT use the 'emailaddress' attribute as a unique identifier.	Section 6.2
6	Only a minimum set of Claims are released by default. Additional personal Claims that the Relying Party requires MUST have their release approved. This approval is subject to these Claims being essential for the application to function and make authorisation decisions.	Section 6.4
7	The Relying Party SHOULD an automated mechanism to publish and make its metadata publicly accessible.	Section 5.3

4. Details for integration using SAML2 federation

4.1. Implementation checklist

Table 3: Example of the sequence of outline tasks required for a typical SAML2 integration

#	Summary	Required / Optional	Who?	Ref
1	Third Party organisation joins the UK Access Management Federation or one of the federations that participate in EduGAIN	Req	Third Party organisation	
2	Third Party registers the Service Provider (SP) metadata with the Federation	Req	SP admin	
3	Agree suitable ID to use	Req	Oxford & SP admin	6.2
4	Request additional attribute/claim release	Opt	SP	6.4
5	Approve and configure additional attribute/claim release	Opt	Oxford	
6	Provide SSO account for Third Party to test with	Opt	Oxford	7.3
7	Test service against the Staging or IAMTEST IdP	Opt	SP admin	
8	Decide account provision and authorisation solution	Req	Oxford & RP admin	7.2

4.2. SAML2 Federation entity details

4.2.1. Non-Production

For some cases it will be preferable to test against a non-production environment to aid debugging and fixing any problems. The choice of which non-production environment to use depends on what type of account is used for testing. Testing in the **Staging** environment will need a production Kerberos account, whereas testing in the **IAMTEST** environment uses test Kerberos accounts. See Section 7.3 for more details about the different test account options.

Table 4: Entity details for the two SAML2 Shibboleth non-production environments **Staging** and **IAMTEST** (public access)

Environment	Description	Endpoint
Staging	EntityID	https://idp-staging.shibboleth.ox.ac.uk/shibboleth-idp
	Specific Metadata URL (Federation published)	http://mdq.ukfederation.org.uk/entities/https:%2F%2Fidp-staging.shibboleth.ox.ac.uk%2Fshibboleth-idp
	Aggregated federation metadata URL	http://metadata.ukfederation.org.uk/ukfederation-metadata.xml
	Attribute scope	@ox.ac.uk
IAMTEST	EntityID	https://idp.iamtest.ox.ac.uk/shibboleth
	Specific Metadata URL (Federation published)	http://mdq.ukfederation.org.uk/entities/https:%2F%2Fidp.iamtest.ox.ac.uk%2Fshibboleth

	Aggregated federation metadata URL	http://metadata.ukfederation.org.uk/ukfederation-metadata.xml
	Attribute scope	@ox.ac.uk

4.2.2. Production

Table 5: Entity details for the SAML2 Shibboleth **Production** environment (public access)

Environment	Description	Endpoint
Production	EntityID	https://registry.shibboleth.ox.ac.uk/idp
	Specific Metadata URL (Federation published)	http://mdq.ukfederation.org.uk/entities/https:%2F%2Fregistry.shibboleth.ox.ac.uk%2Fidp
	Aggregated federation metadata URL	http://metadata.ukfederation.org.uk/ukfederation-metadata.xml
	Attribute scope	@ox.ac.uk

5. Details for integration using WS-Federation

5.1. Implementation checklist

Table 6: Example of the sequence of outline tasks required for a typical WS-Fed integration

#	Summary	Required / Optional	Who?	Ref
1	Pull ADFS metadata from Oxford's published endpoint	Req	RP admin	5.3
2	Cross-check thumbprint of ADFS signing cert for securing access to application	Req	Oxford & RP admin	5.4.2
3	Agree suitable ID to use	Req	Oxford & RP admin	6.2
4	Provide RP details, preferably in the form of metadata at a publicly accessible URL. This should include: long lived certificate for encrypting claims, RP entityID, RP endpoint.	Req	RP	5.3
5	Cross-check thumbprint of RP encryption cert	Req	Oxford & RP admin	5.4.2
6	Configure RP on the Oxford ADFS service	Req	Oxford	
7	Request additional attribute/claim release	Opt	RP	6.4
8	Approve and configure additional attribute/claim release	Opt	Oxford	
9	If using test ADFS service, provide IP addresses of test clients/RPs.	Opt	RP admin	
10	Configure firewall rules for testing	Opt	Oxford	
11	Decide account provision and authorisation solution	Req	Oxford & RP admin	7.2

5.2. ADFS endpoints

5.2.1. Non-Production

For most cases it will be preferable to test against a non-production environment to aid debugging and fixing any problems. Endpoints for the ADFS Staging environment are given in the table below. The choice of which **HomeRealm** value to use depends on what type of account is used for testing. Choosing the **Staging** Identity Provider (idp-staging.shibboleth.ox.ac.uk) will need a production Kerberos account, whereas choosing the **IAMTEST** Identity Provider (idp.iamtest.ox.ac.uk) will use a test Kerberos accounts. See Section 7.3 for more details about the different test account options.

Table 7: Endpoints for the ADFS non-production environment

Description	Endpoint
Federation Metadata URL	https://sts-stg.fed.ox.ac.uk/federationmetadata/2007-06/federationmetadata.xml
Issuer URL	https://sts-stg.fed.ox.ac.uk/adfs/ls/
Trust URL	https://sts-stg.fed.ox.ac.uk/adfs/services/trust
HomeRealm value (to preselect the	https://idp-staging.shibboleth.ox.ac.uk/shibboleth-idp

Identity Provider)	https://idp.iamtest.ox.ac.uk/shibboleth

5.2.2. Production

Table 8: Endpoints for the ADFS production environment (public access)

Description	Endpoint
Federation Metadata URL	https://sts.fed.ox.ac.uk/federationmetadata/2007-06/federationmetadata.xml
Issuer URL	https://sts.fed.ox.ac.uk/adfs/ls/
Trust URL	https://sts.fed.ox.ac.uk/adfs/services/trust
HomeRealm value (to preselect the Identity Provider)	https://registry.shibboleth.ox.ac.uk/idp

5.3. Configuration of trust using Metadata

The configuration of a trust relationship between the Oxford ADFS claims provider and a Relying Party SHOULD be done by exchanging metadata.

The **Claims Provider** metadata includes endpoint locations and the X509 certificate used in the signing of claims (see Section 5.4.1). Metadata for the Oxford ADFS claims provider should be obtained from the endpoint locations listed in Section 5.2.

The **Relying Party** metadata includes service endpoint locations and the X509 certificate used in the encryption of claims (see Section 5.4.1). Note that it is preferable that the Relying Party have an automated mechanism to publish and make this metadata publicly accessible. By having this mechanism in place, it should be possible to initially configure the RP trust in such a way that certificate rollover can be achieved at both the RP and IDP without a need for downtime, service at-risk notification, and technical liaison and co-ordination of change management procedures between the University and the service provider.
In cases where the Relying Party is not developed to support the provision of metadata, Oxford will configure the trust relationship manually using the details the customer has provided including the RP's X509 certificate file.

In all cases the solution must include procedures, automatic or otherwise, for the metadata to be refreshed. See Section 5.5 for more details.

5.4. Certificates

5.4.1. Use of X509 certificates for signing and encrypting claims

To correctly integrate with Oxford Federated SSO a Relying Party is REQUIRED to:

1. Provide an X509 certificate which the Oxford ADFS service will use to **encrypt** claims it sends to that Relying Party so that the claims/attributes are securely transferred between each

party. This certificate should be self-signed and long-lived (10 years). Note that the use of non-encrypted claims is not allowed (relying on HTTPS/TLS transport between the user's browser and each party is not sufficient).

This certificate SHOULD be provided in the metadata that is provided by the Relying Party. Alternatively the X509 certificate file can be provided directly to the Project Technical Lead.

2. Use the X509 **signing** certificate that the Oxford ADFS service provides, to validate the signature on the claims that it receives and reject claims that are not correctly signed. This signing certificate is included in the metadata published by our Oxford ADFS service (see Section 5.2). Typically a relying party will download this metadata as part of its configuration and trust the certificate included, identified by its fingerprint/thumbprint.

5.4.2. Checking the fingerprint/thumbprint of X509 certificates

When X509 certificates or metadata are swapped as part of the initial configuration of the trust relationship (typically via email or by download) it is good practice to check the certificate fingerprint/thumbprint out-of-band (e.g. telephonically) to give extra assurance that the certificate or metadata hasn't been tampered with. The same process should be followed when any of the certificates or metadata are refreshed.

5.5. Refreshing metadata & certificates

The metadata for Oxford's ADFS service (used for SSO) is expected to occasionally change due to normal operation of a Federation Claims Provider. In most cases this change is likely to be due to a renewal of the X509 certificates included in the metadata. Consequently, each Relying Party must renew/refresh their copy of the metadata, and importantly the signing certificate contained therein, which is used to check authenticity of the claim sent from ADFS to the Relying Party. The cost of doing this procedure (or handling it automatically) should be included in the normal support provided by the 3rd party operating the Relying Party.

It is difficult to give a number for the number of metadata refreshes that will be required during the lifetime of the service. Best practice would be to check for metadata changes every day or on restart of the service, although in practice metadata won't change that often. Whilst we can predict the requirement for metadata refreshes for some scenarios such as certificate renewal (every 10 years now) and ADFS service upgrade/migration, other scenarios such as the compromise of a private key would force us to renew certificates & metadata unexpectedly.

Whilst Microsoft do provide a metadata auto-update feature in the ADFS product which is designed to allow for seamless certificate rollover, in our experience most other Relying Parties aren't able to handle auto-update. Part of the way metadata auto-update works is that both parties will periodically (e.g. daily) download the metadata for the other party and refresh their local copy. Metadata can include both current and new certificates so that both (thumbprints) are trusted in advance of any switchover on the ADFS claims provider. Then the old thumbprint can be removed at some point after the ADFS switchover. This is a common way of handling this in a SAML2 federation i.e. with the Shibboleth service provider software.

If Relying Parties can't handle certificate rollover automatically then administrators MUST adopt an operational procedure so that when necessary, given adequate notice, they can update the local copy and/or thumbprint of the metadata certificates provided by the Oxford ADFS service.

For costing purposes the administrators of the Relying Party SHOULD allow for an average of 2 refreshes per year i.e. a refresh roughly every 6 months. In practice there most likely won't be a need to do that many but 3rd parties should allow for that as an ongoing part of their normal support. Where possible University of Oxford will give the 3rd party operating the Relying Party 14 days' notice of any scheduled change to the ADFS metadata. Also, University of Oxford can provide copies of the certificates in advance of any change so that certificate thumbprints can be setup to be trusted in advance of any switchover.

6. Identifiers and attributes

6.1. Attributes available

6.1.1. Attributes available to SAML2 Service Providers as assertions

A full list of attributes potentially available to a Service Provider is documented at http://help.it.ox.ac.uk/iam/federation/attributes [3]. Only a small set of these are released to a Service Provider by default. See Section 6.4 for requesting the release of additional attributes.

Table 9: Examples of commonly used SAML2 attributes

SAML2 attribute Name	SAML2 Attribute OID	Release policy	Example	Notes
eduPersonTargetedID	urn:oid:1.3.6.1.4.1.5923.1.1.1.10	Default	ox1fHlLqpbf9JW68OucALm/ypPY=	
eduPersonPrincipalName	urn:oid:1.3.6.1.4.1.5923.1.1.1.6	Approval	oucs0175@ox.ac.uk	
givenName	urn:oid:2.5.4.42	Approval	Joe	
sn	urn:oid:2.5.4.4	Approval	Blogs	
mail	urn:oid:0.9.2342.19200300.100.1.3	Approval	joe.blogs@it.ox.ac.uk	
eduPersonScopedAffiliation	urn:oid:1.3.6.1.4.1.5923.1.1.1.9	Default*	member@ox.ac.uk*	
eduPersonScopedAffiliation	urn:oid:1.3.6.1.4.1.5923.1.1.1.9	Approval *	member@ox.ac.uk* student@ox.ac.uk	multiple valued
eduPersonPrimaryOrgUnitDN	urn:oid:1.3.6.1.4.1.5923.1.1.1.8	Approval	oakUnitCode=itserv,ou=units,dc=oak,dc=ox,dc=ac,dc=uk	
eduPersonOrgUnitDN	urn:oid:1.3.6.1.4.1.5923.1.1.1.	Approval	oakUnitCode=itserv,ou=units,dc=oak,dc=ox,dc=ac,dc=uk oakUnitCode=oerc,ou=units,dc=oak,dc=ox,dc=ac,dc=uk	multiple valued

* By default 'eduPersonScopedAffiliation' gets released with the value 'member@ox.ac.uk' for all types of person apart from those that have the looser 'affiliate' status. More detail about the nature of the affiliation (e.g. whether staff or student) can be released on approval if the release of 'eduPersonScopedAffiliation' is specifically requested. In this case the attribute takes a combination of multiple values. Possible values are: member@ox.ac.uk; staff@ox.ac.uk; student@ox.ac.uk; employee@ox.ac.uk; affiliate@ox.ac.uk.

6.1.2. Attributes available to ADFS Relying Parties as claims

Relying Parties using the Oxford ADFS service consume attributes provided as WS-Federation claims. The Oxford ADFS service generates its claims from SAML2 assertions/attributes provided by the Oxford Shibboleth Identity Provider (IdP). A full list of attributes potentially available to a Relying Party is documented at http://help.it.ox.ac.uk/iam/federation/attributes but note that these can't be consumed directly by an ADFS relying party because the formal naming schemes are incompatible.

A subset of these attributes have been mapped (transformed) to claims that can be consumed by an ADFS Relying Party and those are listed in the table below along with details about whether they are released by default or require specific approval on request (see Section 6.4 for approval process).

Table 10: Attributes (claims) available to a Relying Party

Friendly Name	Formal name/schema	Release policy	Example	Source SAML2 attribute
nameidentifier	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier	Default	ox1fHlLqpbf9JW68OucALm/ypPY=	eduPersonTargetedID (urn:oid:1.3.6.1.4.1.5923.1.1.1.10)
UPN	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn	Approval	oucs0175@ox.ac.uk	eduPersonPrincipalName (urn:oid:1.3.6.1.4.1.5923.1.1.1.6)
givenname	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	Approval	Joe	givenName (urn:oid:2.5.4.42)
surname	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	Approval	Blogs	sn (urn:oid:2.5.4.4)
emailaddress	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	Approval	joe.blogs@it.ox.ac.uk	mail (urn:oid:0.9.2342.19200300.100.1.3)
role*	http://schemas.microsoft.com/ws/2008/06/identity/claims/role	Approval	member@ox.ac.uk* student@ox.ac.uk	eduPersonScopedAffiliation (urn:oid:1.3.6.1.4.1.5923.1.1.1.9)
department	https://registry.shibboleth.ox.ac.uk/claim/department	Approval	itserv	eduPersonPrimaryOrgUnitDN (urn:oid:1.3.6.1.4.1.5923.1.1.1.8)
eduPersonPrimaryOrgUnitDN	https://registry.shibboleth.ox.ac.uk/attribute/eduPersonPrimaryOrgUnitDN	Approval	oakUnitCode=itserv,ou=units,dc=oak,dc=ox,dc=ac,dc=uk	eduPersonPrimaryOrgUnitDN (urn:oid:1.3.6.1.4.1.5923.1.1.1.8)
eduPersonOrgUnitDN	https://registry.shibboleth.ox.ac.uk/attribute/eduPersonOrgUnitDN	Approval	oakUnitCode=itserv,ou=units,dc=oak,dc=ox,dc=ac,dc=uk oakUnitCode=oerc,ou=units,dc=oak,dc=ox,dc=ac,dc=uk	eduPersonOrgUnitDN (urn:oid:1.3.6.1.4.1.5923.1.1.1.4)

Friendly Name	Formal name/schema	Release policy	Example	Source SAML2 attribute
			(multiple valued)	

* The 'Role' claim takes its value from the SAML2 attribute 'eduPersonScopedAffiliation' and needs to be approved for release to a Relying Party. The attribute takes a combination of multiple values. Possible values are: member@ox.ac.uk; staff@ox.ac.uk; student@ox.ac.uk; employee@ox.ac.uk; affiliate@ox.ac.uk.

6.1.3. Procedure for requesting the mapping of additional attributes to claims

If there is a need for attributes from http://help.it.ox.ac.uk/iam/federation/attributes [3] that don't already fall into the subset mapped as claims, then these will have to be formally requested as part of the work to integrate the application with SSO. If there is sufficient justification for requiring the attribute then work can be carried out to configure the mapping on the ADFS service. Release of any new attribute will still need to follow the usual approval process as described Section 6.4.

6.2. Unique Identifier

The following 2 attributes are suitable to use as persistent unique identifiers in the Oxford SSO environment:

1. **SAML2: eduPersonTargetedID**
   WS-Fed: Nameidentifier

   This is an opaque immutable identifier generated by the Oxford Shibboleth Identity Provider (IdP) and is unique to each SAML2 Service Provider. In the ADFS/WS-Fed environment the closest equivalent option is to use the nameidentifier claim which takes the value of eduPersonTargetedID released by the IdP to the ADFS service and so is unchanging between different Relying Parties. Being opaque it doesn't reveal any personal information to the Service Provider/Relying Party and so can be released to all Service Providers/Relying Parties without approval.

2. **SAML2: eduPersonPrincipalName**
   WS-Fed: UPN (User Principal Name)

   This is an immutable identifier based on the scoped form of the Oxford SSO username. In the ADFS/WS-Fed environment it is mapped to the more familiar UPN claim. It is scoped to the '@ox.ac.uk' domain so can be considered to be globally unique. Release of this to a Service Provider or Relying Party has to be approved.

Using email address as an identifier

A Service Provider/Relying Party SHOULD NOT use the 'mail/emailaddress' attribute as a unique identifier. It is unsuitable in the Oxford environment and strongly discouraged because:

- Email addresses are specific to a department/unit and change as people move between departments i.e. they are not immutable.

- Email addresses change when people change names e.g. after getting married. i.e. they are not immutable.
- People often own multiple email addresses (one for each department affiliation) and only one of these will be presented in the SSO claim. This can lead to confusion and means that the email domain presented to the Relying Party might not match with the department that is linked to entitlement to use the application.

6.3. Attribute scoping

Some attributes are 'scoped' which means they include the '@ox.ac.uk' suffix. This is Oxford's registered domain of jurisdiction within the UK Access Management Federation and is linked with the DNS domain that University of Oxford has ownership of. Within the context of the UK Access Management Federation this scope can be used to assert a globally unique identifier, and by entities to confirm that an identity provider is making assertions it is entitled to make. Its use in attributes for Relying Parties that aren't in the UK Federation has less of a formal meaning. Its use in the UPN attribute is in place of what would normally be the authentication Domain or Realm and for Oxford's SSO environment these match.

Checking that the scope of attributes matches '@ox.ac.uk', particularly for the edupersonPrincipalName or eduPersonScopedAffiliation attributes, is good policy for a general level of authorisation check on the Service Provider/Relying Party. There is usually an explicit relationship between scope and the trusted metadata for an Identity Provider/Claims Provider and checking the scope will provide additional assurance that the assertion/claim comes from the expected Identity Provider/Claims Provider.

6.4. Attribute Release Policy and Request process

Oxford's policy is not to release any personal attributes to Service Providers/Relying Parties by default and so any request to release these has to go through an approval process for each case. This approval process will take into account the following:

1. Whether the attributes are essential for the application to function. Any 'nice to have' or cosmetic attributes should be obtained from the users directly once they have gained access to the application (for example first name, last name, email address for correspondence).
2. The attribute release is sponsored by an authorised person of the University that is responsible for the service, or project to deliver it, and that they take responsibility for the use to which the released data is put, and that they have satisfied themselves that any 3rd party will adhere to the University policy for data protection and security.

7. Account provisioning & user authorisation

7.1. Authorisation

Table 11: Summary of the typical authorisation options.

Option	Summary	Authorisation decided by	Account provisioning

i	Access to the application allowed for the whole University of Oxford community including staff & students	All allowed.	Automatically on first access. See 7.2.2
ii	Access to the application allowed to users affiliated to one unit/department	Decide on the basis of the presence of a particular assertion/claim value	Automatically on first access. See 7.2.2
iii	Access to the application allowed to users with a certain role/status? E.g. staff	Decide on the basis of the presence of a particular assertion/claim value	Automatically on first access. See 7.2.2
iv	Access to the application allowed for only a subset of user accounts, pre-provisioned in a local user table or directory	Match of Unique ID provided in assertion/claim with record in the local user table or directory.	Pre-provisioned. See 7.2.1
v	Access given by a 2 stage process: first the user logs in and an application account is created; second an application admin manually gives the new account full access to the application.	Match of Unique ID provided in claim with record in the local user table or directory, which has been given privileges by an admin.	Automatically on first access. See 7.2.2

7.2. Account provisioning

7.2.1. Pre-provisioning of accounts/ bulk load

For authorisation case iv the application's internal accounts need to be pre-provisioned in whatever 'user store' it is using. Consideration needs to be given to how these are maintained over the lifetime of the service as users arrive and leave the University. In most cases it will be advantageous if the application can import a dataset with the accounts to be provisioned and have this import scheduled regularly. The dataset with necessary fields (including Unique ID) can be provided by University of Oxford from one of their IAM systems. In other cases the internal accounts may be setup using some manual process.

7.2.2. Automatic account creation on first login

For authorisation cases i, ii, iii, & v it is likely that the application's user accounts will be created automatically when the user first logs in. For example in the event that the Oxford SSO login is successful, but no matching user account is found in the internal application 'user store', then a new user will be automatically created by the application with the matching Unique ID provided in the assertion/claim. If the application receives other assertion/claim values, e.g. Givenname & Surname, then these will also be used to populated fields in the user record.

7.2.3. Allowing claims to update existing user fields

Where identity attributes in the form of assertions/claims are released about the user following a successful SSO Oxford login, these attributes SHOULD be used by the application to overwrite the corresponding (non-keying) fields held in the internal 'user store'. This means that the Oxford Federated SSO service (and the IAM systems that underpin it) is always authoritative for these identity attributes. It is acceptable if this happens even if the particular assertion/claim is empty.

7.2.4. User attribute retrieval post login

Some applications may be designed to make a secondary (LDAP) query against a user directory to retrieve user attributes following an initial login. This capability isn't provided in the Oxford Federated authentication stack to Third Party external applications, so instead all attributes will need to be received as attributes or claims provided by the Shibboleth or ADFS service. This is consistent with good practice in federated authentication where release of attributes/claims is controlled at the Identity Provider/Claims Provider.

7.3. Accounts for testing

SSO accounts can be created for a third party supplier to use in the development & testing of an application integration. There are 2 options for test accounts type:

A. Accounts in the production IAM system (production Kerberos realm).
Ownership & use of these accounts is tied to particular nominated persons carrying out development and testing. To request one of these accounts the nominated person must apply to have a 'Virtual Access Card' using the form that University of Oxford, IT Services will provide. The request will need to be sponsored by an authorised person of the University that is responsible for the service integration, and the lifetime of the account will be limited to the duration of the integration project.

B. Accounts in the IAMTEST system (IAMTEST Kerberos realm).
These accounts are managed by the IAM Team or other IT Services project or service team responsible for the testing of a particular application. Testing using these accounts will use a separate IAMTEST stack of services (Shibboleth/Kerberos). There is currently no attribute store for these accounts which means that it is hard to do testing that relies on particular attributes or claims being available to the Service Provider/Relying Party. Credentials for specific accounts can be shared/booked out to Third Parties and will have a lifetime limited to an agreed testing period.

Depending on which option is chosen, administrators need to configure their systems appropriately using the corresponding non-production configuration details listed in Section 4.2.1 (SAML2 Service Providers) or Section 5.2.1 (WS-Fed relying parties).

7.4. Accounts for ongoing support

SSO accounts can be created for a third party supplier to use for ongoing support of the production system. To request one of these accounts a nominated person must apply to have a 'Virtual Access Card' using the form that IT Services will provide. The request will need to be sponsored by an authorised person of the University that is responsible for the service.

8. Security testing

IT Services reserve the right to test that access to a third party application is correctly restricted by using a combination of different techniques including the spoofing of assertions/claims. Typically these tests would be carried out in the implementation/UAT phase of a new application and results would normally be shared with the third party responsible for the application.

9. 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] Attributes available to Federation Service Providers
http://help.it.ox.ac.uk/iam/federation/attributes

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

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