Technical recommendations

Notation

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 RFC2119 (http://www.ietf.org/rfc/rfc2119.txt).

Overview

This document provides technical recommendations for participants in the OpenAthens Federation. Please refer your IT department to this document if you require assistance with its contents.

Attributes

The OpenAthens Federation facilitates attribute exchange between member identity and service providers. Attributes provide the means by which authorisation decisions or personalisation can be based. While the particular attributes exchanged at the time of sign-on by a user are entirely up to the identity provider, these recommendations serve to provide a base-line. This aims minimise the likelihood of access to genuinely entitled services being denied, and seeks to achieve longevity in attribute usage.

More on attributes: Standard attributes in the OpenAthens federation

Targeted ID attributes

These attributes serve to provide a stable identifier for users in a manner that is targeted to different service providers. This means that different service providers will receive different values, but each provider will receive a value that is stable between sign-ins for the same user.

Name	eduPersonTargetedID
Long name	urn:oid:1.3.6.1.4.1.5923.1.1.1.10
SAML version(s)	2.0

Name	eduPersonTargetedID
Long name	urn:mace:dir:attribute-def:eduPersonTargetedID
SAML version(s)	1.1

Identity providers SHOULD provide both of these attributes (depending on the SAML version used in the exchange), if required by a service provider.

Organisational identifiers

Organisations within the OpenAthens Federation MUST be identified using DNS domain name notation (i.e comply with the hierarchical dot-delimited notation) E.g: `institution.ac.uk`. It is RECOMMENDED that these resolve to a real DNS domain registered to the organisation .

A single SAML entity MAY assert additional organisation identifiers - see Entities with multiple scopes such as NHS England and other consortia domains.

Identity providers SHOULD provide an organisation attribute, if required by a service provider.

In the case of scoped attributes (such as scopedAffiliation), the organisational identifier MUST be used as the scope. This MUST be the same value that is used for the organisation attribute.

E.g: `member@institution.ac.uk`

Supported SAML versions

Identity providers and service providers MUST support SAML 2.0 and / or SAML 1.1.

SAML 2.0 is RECOMMENDED.

SAML 2.0

- Entities supporting SAML 2.0 MUST comply with the Interoperable SAML 2.0 Web Browser SSO Deployment Profile.

SAML 1.1

- Identity providers generating SAML 1.1, MUST generate scoped attributes (where necessary, based on the attribute definition).
- Service provdiers accepting SAML 1.1 MUST validate scoped attributes against list of scopes appearing in the issuing identity providers metadata.

- Identity providers accepting SAML 1.1 MUST accept authentication requests with the `urn:mace:shibboleth:1.0:profiles:AuthnRequest` binding.
- Service providers accepting SAML 1.1 MUST generate authentication requests with the `urn:mace:shibboleth:1.0:profiles:AuthnRequest` binding.

Back-channel requirements

Back-channel is not supported by OpenAthens IdPs so MUST NOT be REQUIRED by SPs that only support SAML 1.1