EDUGATE RULES

Table of Contents

1 Purpose and Scope

The purpose of this document is to define the procedures for the operation of the Edugate federation. It outlines the operation obligations on the Administrators and the members of the federation.

2 Membership

The Administrator will process applications for membership of the federation which fall within the categories of Identity and Provider Member outlined below.

Identity Members

- All organisations that are part of the HEAnet network (as listed on the HEAnet website) with the exception of primary and second level schools are eligible to become an Identity Member of the federation. Organisations of strategic importance to the federation and the higher education sector will be admitted to Edugate after consideration by the Edugate Governance Committee

Provider Members

- Organisations that are part of the HEAnet network (as listed on the HEAnet website) with the exception of primary and second level schools are eligible to become a Provider Member of the federation. Organisations that are considered by the Edugate Governance Committee to be of strategic importance to the federation and the higher education sector will be admitted after consideration by the Edugate Governance Committee. Organisations that are contracted to provide services to the participating institutions are eligible to join Edugate.

Membership of the Edugate Federation is provided on an annual basis and will be automatically renewed each year on the anniversary date of this Agreement unless the Member gives thirty (30) days

notice in writing to the Administrator of the Member's intention to cease its Membership of the Edugate Federation or in the event that the Agreement is terminated for any pursuant to the provisions of the Edugate Agreement.

Membership of the Edugate Federation does not always grant the Identity Member or its Users an automatic right of access to a Provider Member's Services.
Provider Members are entitled to require the Identity Member to enter into separate terms and conditions with the Provider Member for access to a Provider Member's Services.

Membership of the Edugate Federation does preclude Provider Members from supporting alternative means of access to Users.

3 Application Procedure

Applications for membership will be processed upon receipt of a signed copy of the Edugate Agreement.. The Administrator will confirm if the applicant's membership request has been successful after a maximum period of one (1) month. The applicant has a one (1) month period during which they must submit their relevant Member Metadata to the Administrator either by means of the Edugate Resource Registry or email, Provider Members must accompany this metadata with the user data from the Edugate Schema (as outlined in Appendix A) that will be required or desired when accessing the service.

4 Data Control and Data Sharing

4.1 Identity Members

The Identity Member must comply with the use of Personal Data as outlined in the Acts.
Identity Members have absolute control and responsibility over the authentication of Users and the data that an Identity Member provides to the Provider Member. For the avoidance of any doubt neither HEAnet Limited, the Edugate Federation nor the Administrator will have any responsibility for or control over the data provided to a Provider Member.
Identity Members may make access to its Users conditional on a Provider Member agreeing and entering into separate terms and conditions with the Identity Member.
Identity Members may prompt Users for their consent prior to the provision of the User's Personal Data to the Provider Member. In such cases, Users may consent to release all or part of the data required by the Provider Member.

4.2 Provider Members

Provider Members are required to protect and respect the privacy and confidentiality of User information which it receives from other Member organisations.
Provider Members have absolute control and responsibility the authorisation of Users. In the event a Provider Member requiring Personal Data, the Provider Member must declare to the Administrator the Personal Data that is required and outline why the data us required. Such requests must fall within the definitions of permitted uses of Personal Data as outlined in the Acts. The Provider Member must declare to the Administrator any changes to the Provider Member's requested data.
Consent must be obtained by the Provider Member before the Provider Member can use the User's Personal Data for purposes other than authorisation unless such use is otherwise permitted by the Acts.
The Provider Member should not permanently store or share or disclose or use for any purpose, other than for the purposes of authorisation and access control any Personal Data that the Provider Member receives from another Member unless otherwise permitted by the Acts.
Provider Members are permitted to use User data for the purposes of generating statistical information provided all data is anonymised to the extent that the data can no longer be linked with a Users data.

4.3 Edugate Resource Registry

The Edugate Resource Registry website serves as the Edugate system of record for the Identity Provider User attribute provision policies. Identity members must ensure that the policy recorded within the Edugate Resource Registry accurately reflects the provision of attributes for that Identity member within the configuration of the Identity Members system. All members who have access to the Edugate Resource Registry will have visibility of the policy.

4.4 Notification of the default policy

The Administrator will prescribe an initial User data provision policy ("default policy") for Identity Members upon joining Edugate. This policy will be limited to non-personal data and the Edugate Schema (the Edugate Schema is outlined in Appendix A).

Identity Members will be notified by electronic mail when the default policy has been defined. During a period of two (2) weeks commencing on the date of the notification, the default policy can be overridden by the Identity Member, after that period has passed the Identity Member will become an active member of the federation.

When a new Provider Member joins Edugate, Identity Members will be notified by electronic mail of the new Provider Members User attribute requirements. Where and Identity Member does not amend their policy for the new Provider Member, the default policy will apply.

Identity Members can change their policy (including their default policy) at any time.

5 Cessation of membership

Where a member has provided notice in writing of their intention to cease their Edugate membership, the Administrator will notify all other members by electronic email of the impending cessation date within a period two (2) weeks.
The Administrator will remove the particulars of the Members Metadata from the Federation Metadata after a further (2) two week period. The cessation procedure may be accelerated at the members request provided no other member raises an objection to the accelerated cessation date.

Where a member wishes to cease membership as a result non-compliance due to changes to the federation membership agreement, the member will have a six (6) month grace period before the Administrator will remove the particulars of the Members Metadata from the Federation Metadata instead of the usual two (2) week period as outlined above.

6 Identity Assurance

Identity Members must adhere to the following when providing identity data from the Edugate Schema.

- Identity Members will provide identity data from the federation Edugate Schemas only when member Identity Members trust that data when providing access to that members own organisation services (whether those services are within the federation or otherwise). Member Identity Members may provide identity data in full or in part from trusted third party sources provided that the identity data is frequently trusted when accessing services within the Identity Members own organisation.
- Identity Members will not provide identity data from the Edugate Schemas that is insufficient to fulfil the requirements on user organisations as set out in the HEAnet Acceptable Use Policy.
- Identity Members will not provide identity data from the Edugate Schema that is fulfilled from a source where the source identity data is disabled, expired or known to by the member Identity Member to be compromised.
- Members will not permit generic or shared accounts from their identity sources to be used within the federation.

- Member Identity Members will not provide User affiliations where it is known by the member Identity Member that such affiliation has lapsed or is otherwise incorrect.

The provision of all other identity data (not included in the Edugate Schema) is the responsibility of individual members; such use is not covered by the terms of this agreement

7 Dispute Resolution Procedure

7.1 Compliance Dispute

In the event of any dispute concerning compliance by the Member with the Edugate Agreement and Rules (a "Compliance Dispute") and if such Compliance Dispute cannot be resolved then the Compliance Dispute will be referred by either Party to a person agreed by the Parties, and in the absence of such agreement within ten (10) Working Days of notice from either Party calling on the other so to agree, to a person chosen on the application of either Party to the President of Engineers Ireland or by the next senior officer of such body who is willing and able to make such a nomination. Such person ("the Expert") will be appointed to act as an expert and not as an arbitrator. The costs of the Expert will be borne equally by the Parties unless the Expert decides one Party has acted unreasonably in which case the Expert will have discretion as to awarding costs.

In all cases the terms of appointment of the Expert by whomsoever appointed will include :-

- a commitment by the Parties to supply to the Expert all such assistance, documents and information as the Expert may reasonably require for the purpose of his determination ;
- a requirement that the Expert will act fairly as between the Parties and according to the principles of natural justice ;
- a requirement that the Expert will hold professional indemnity insurance both then and for three years following the date of his / her determination and
- a requirement to give a decision as soon as is reasonably practicable and in any event within eighty-four (84) Working Days of the Expert's appointment.

The Expert's decision will be final and binding on the Parties. The Parties expressly acknowledge and agree that they do not intend the reference to the Expert to constitute an arbitration, that the Expert's decision is not a quasi judicial procedure and that the Parties will have no right of appeal against the Expert's decision, provided always that this will not be construed as waiving any rights the Parties might have against the Expert for breaching his / her terms of appointment or otherwise being negligent.

7.2 Policy Dispute

With respect to any dispute other than one concerning compliance by the Member with this Agreement including, but without limitation, a dispute involving the policies of the Edugate Federation (a "Policy Dispute"), then if such Policy Dispute cannot be resolved the Policy Dispute may be referred by either party to the Federation Governance Committee. The decision of the Federation Governance Committee will be final and binding upon the Parties.

7.3 Dispute Classification

Where it is not clear whether a dispute is a Compliance Dispute or a Policy Dispute, the Administrator will decide, following consultation with the Member. The Administrator's decision will be final.

7.4 Representation

If a dispute arises between the Parties relating to the provisions of the Agreement, the Administrator or the Member must refer the dispute to their respective representatives, whereupon the Administrator's

representative and the Member's representative will promptly discuss the dispute with a view to its resolution.
If a dispute cannot be resolved within fourteen (28) Working Days, the Member or the Administrator may require that the matter be referred for consultation between the Chief Executive or equivalent of the Member or his / her authorised representatives and the Chief Executive of the Administrator or his / her authorised representatives ("Chief Executive Level Consultations"). In this event, both the Member's Manager and the Administrator will be represented in person or by their representatives.

8 Support

8.1 Availability

Members are responsible for the availability of their federation services. Member Provider Members and Identity Members must ensure that their federation services are available for a minimum of eight (8) months out of a twelve (12) month period. Member Provider Members and Identity Members may provide a greater degree of availability at their discretion. Member Identity Members have a six (6) month period to commission their federation services during which they are not required to meet the minimum period of availability.

8.2 End user support

End user support may be agreed between member Provider Members and Identity Members. Where such an agreement does not exist, member Identity Members and member Provider Members must agree to support users in accordance with the following procedures;

Identity Members must act as the first point of support for their users. In the case where the user has been denied access by a Provider Member, the Identity Member must ensure that they have provided the user data that the service expects before referring the problem to the Provider Member or the Administrator. Where the problem has been referred to the Provider Member, the Identity Member can request the Provider Member to handle further communication with the user (and further users with identical issues). Provider Members must support users who have been referred to them by Identity Members provided the Identity Member can produce evidence that shows that the correct identity data has been provided. Provider Members may act as the first point of contact for users with access issues at the Provider Members discretion.

9 Interfederation and confederation

The Administrator will notify members by electronic mail when the Administrator has established a new Metadata exchange agreement with a peer federation and will include the Metadata exchange agreements within the notification. All metadata exchange agreements will be published on the Edugate web site [www.edugate.ie]. If the Member wishes to participate in such Metadata exchange agreements the member must notify the administrator by electronic mail of the intention to participate. Members will continue to adhere to the Edugate Agreement when their Service or Users are being used by the participating members of a peer federation. Participating members of the peer federations are not required to adhere to the Edugate Agreement and Rules.

10 Technical Specification

Identity Members must adhere to the requirements set out in Appendix A.

11 Changes to the Edugate Rules

The Edugate Rules will be amended from time to time by the Edugate Governance Committee, each Manager will be notified by electronic mail of the effective date of such changes.

APPENDIX A: TECHNICAL SPECIFICATION

1 Technical Specification

Membership of the federation is subject to members adhering to the technical specifications set out below.

2 Attributes

2.1 Edugate Schema

Member Provider Members can expect member Identity Members to support (but not necessarily release) a minimum set of data as set out in **Error! Reference source not found.**. This data will be formatted according to the Interoperable SAML 2 Web Browser SSO Deployment Profile[i] .Members may choose to support additional data from the eduPerson data schema[ii] and the OASIS X500/LDAP Schema (OASIS Security Services Technical Committee) or agree their own additional data schemas. Provider Members must accept that the federation operator may extend the Edugate Schema in the future or adopt changes made by the eduPerson data schema standards body (Internet2 MACE-Directories Working Group). Members have a two year period to support the revised minimum attribute set.

Attribute	Personal Data	Example
eduPersonTargetedID	No	ffedacb4ag215f3ed
eduPersonScopedAffiliation	No	student@ucd.ie
eduPersonEntitlement	potentially	urn:mace:heanet.ie:edugate:media:user
eduPersonPrincipalName	potentially	jbloggs@ucd.ie 9944ab@ucd.ie
givenName	Yes	Joseph
Sn	Yes	Blogs
Mail	potentially	Joe.blogs@staff.ucb.ie 9944ab.stu@ucb.ie
organizationName	No	Dublin City University

eduPersonScopedAffiliation.

The eduPersonScopedAffiliation consist of two parts separated by the '@' symbol, the latter part is discussed in the section of this document titled 'Scoped Attribute' below. The former part is limited to a vocabulary as defined by the eduPerson specification, for convenience the permissible values are limited to the following vocabulary as follows;

faculty, student, staff, alum, member, affiliate, employee, library-walk-in

The value '*employee'* is not recommended as the value of '*staff*" has greater meaning in the context of Irish HEI's. Where a postgraduate research student is issued with a campus account equivalent to fulltime paid employees such as faculty and administrative staff, the value of 'staff' should be used. A user may have multiple affiliations to an institution, therefore multiple values are permitted.

2.2 Scoped Attributes

eduPersonPrincipalName and eduPersonScopedAffiliation are two examples of scoped attributes. Identity Members must ensure that the value of the scope that is asserted matches the organisations primary registered domain name as used on the organisations primary website. Sublevel scopes below the primary registered domain name are permitted.

3 Name Identifiers

All members of Edugate must adhere to the NameID requirements as set out in the SAML2 Web-SSO Interoperable Profile at a minimum.

4 Federation Protocol

The federation supports the protocols SAML2 Web-SSO Interoperable Profile. Members must support this all the bindings and message contents of this profile as a minimum.
Members must accept that the federation operator may add support for additional protocols or profiles in the future, where the federation operator declares to members that support for additional protocols or profiles is mandatory, members will have a two year period to support these additional protocols or profiles.
Members must also accept that the federation operator may or adopt changes made to the SAML2 Web-SSO Interoperable Profile, where the federation operator declares to members that support for the amended protocol is mandatory; members will have a two year period to add support for the amended protocol.

5 Federation Metadata

The SAM2 Web-SSO Interoperable Profile mandates the use of the SAML V2.0 Metadata Interoperability Profile Version 1.0. Members must ensure that the Edugate Federation Metadata is applied when their identity or services systems are first commissioned. Where the federation operator has notified members of a change to the metadata the changes to the Federation Metadata must be applied within (2) two working days.

Members must nominate a contact person and contact email address that will be embedded within the Federation Metadata, these details may be used by members to identify the person who has responsibility for a fellow member's federation service.
The organisation names, as declared on the relevant Identity Member or Provider Member agreement will be used to fulfil the organisation element for the member in the Federation Metadata.

Members must ensure that the validity periods declared within the Federation Metadata are enforced by their service of identity systems.

5.1 Certificates

The use of CA issued certificates is required for any endpoint that is secured by SSL or TLS where that endpoint will be invoked in a users web-browser during authentication and authorization.
The use of self signed certificates is permitted for the exchange of SAML messages, these certificates will be added to the federation Metadata. The federation Metadata will not include a list of CA certificates. Members must ensure that the expiry dates of certificates are monitored and certificates renewals are submitted to the federation operator at least one week before the expiry date.

6 Discovery or Where are you from service (WAYF).

The federation operator will provide a Discovery Service compatible with the

OASIS Identity Provider Discovery Service Protocol and Profile[iii]. Provider Members may operate their own discovery services. Provider Members may agree with other identity provider on how discovery will be handled, where such an agreement does not exist the service provider must provide a discovery service that will instigate an authentication request that conforms to the requirements on SAML2 AuthenticationRequest's as set out in the Interoperable SAML 2 Web Browser SSO Deployment Profile.

7 Logging

Identity Members must maintain logs with sufficient detail so as to correlate its users with a SAML2 authentication statement. These logs must be maintained for a minimum period of one month. Identity Members may maintain logs for longer periods to meet the organisations policy on log retention or to meet any requirements as set out in Irish law.

[i] http://saml2int.org/profile/
[ii] http://middleware.internet2.edu/eduperson/docs/internet2-mace-dir-eduperson-200806.html
[iii] http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-idp-discovery.pdf