BELNET R&E federation
Technical policy

Version 1.0

Version	*Date*	
0.1	11/03/09	First draft for advisory committee
0.2	11/05/09	Added attribute schema; changes after 1st meeting
0.3	01/07/10	Changed metadata signing certificate CN
0.4	19/7/2010	Changed metadata URL
0.5	10/8/2010	Changed sections 4.1 & 4.3
0.6	20/8/2010	Spell checks & URL checks.
0.7	1/10/2010	Changes after Advisory Committee 26/8
1.0	14/11/2010	Final version for federation launch

1 Introduction

This document describes technical requirements and procedures for the BELNET R&E federation. It is a technical complement to the BELNET R&E federation agreement. Wherever this document is not consistent with the legal agreement, the legal agreement takes precedence.

2 Terminology

Below is a list of common terminology used in the area of identity federation. Wherever the terminology is not consistent with the legal agreement, the legal agreement takes precedence.

Federation

In general, a federation is a loosely coupled group of organisations sharing a common set of policies and practices. More specifically, the BELNET R&E Federation is about identity federation, where identity management is the subject of common policies and practices.

Federation operator

The entity coordinating federation operations and running the federation core services. BELNET is the Federation operator for the BELNET R&E Federation.

Identity provider (IdP)

The role within the federation providing identity information (attributes) to service providers. Only Belgian R&E institutions connected to BELNET are allowed to take the identity provider role. Further eligibility to this role is described in the legal agreement.

Service provider (SP)

The role within the federation consuming identity information (attributes) in order to decide authorisation to the service. Eligibility to this role is described in the legal agreement.

SAML

Security Assertion Markup Language. SAML is an open standard describing security assertions or claims. The relevant version of the specification is SAML 2. SAML is an OASIS[1] standard.

SAML entity

A SAML entity or SAML endpoint is a party sending or receiving SAML messages. Both IdP's and SP's are SAML entities.

Federation Metadata

Federation metadata is a collection of entity metadata, i.e. the collection of metadata for all identity providers and all service providers in the federation. As such, the federation metadata serves as the technical definition of the federation.

Entity Metadata

Entity metadata is SAML metadata for a single SAML entity.

Attributes

A person's identity is a collection of his or her attributes. Examples are someone's date of birth, name, color of his or her eyes, etc... Exchange of attributes is the essence of SAML: the identity provider knows a number of attributes about people; service providers need a subset of a these attributes to decide whether this person is authorized for the service concerned.

1 http://www.oasis-open.org/

The SAML protocol describes how to exchange such information between identity provider and service provider.

Attribute Release Policy

The Attribute Release Policy is the policy, set by the identity provider, describing which attributes are 'released' to the service provider whenever the service provider requests authentication. A policy can be set as a general default, or it can be set for individual service providers. In the latter case the personal data released to the service provider can be limited to what the service provider needs.

3 Protocols used

The BELNET R&E federation uses the SAML2 protocol, more specifically the 'Web SSO Profile'[2] and the 'IdP Discovery Service Profile'[3]. Use of Shibboleth 2.x software is recommended for mitigating incompatibility risks, but not mandatory.

3.1 SAML Protocol messages

SAML messages will be exchanged between identity providers and service providers. SAML messages MUST be signed. The receiving end of a SAML message (identity provider or service provider) MUST verify the signature against the certificate of the sending end, as published in the most recent metadata. If a SAML message is not signed, or if a signature can't be verified against the federation metadata, the message MUST be refused by the receiving end.

3.2 SAML entity certificate requirements

Every SAML entity needs a certificate in order to sign and/or encrypt SAML messages. Usually a self-signed certificate is created during a default install. The certificate is part of the entity metadata, and will have to be published as part of the federation metadata (see further).

- Every federation member (IdP or SP) MUST notify the federation operator whenever a certificate key pair is compromised. The entity involved will then be removed from the federation metadata. When the issue is fixed, the new endpoint metadata will be included in the federation metadata. An on-site audit might be required for verification of the fix.
- Entity metadata will be removed when the certificate is older than 3 years.
- SPs/IdPs that cease operations will be removed from the federation metadata. A notification MUST be sent to federation@belnet.be.
- A minimum key size of 1024 bits is required.

4 Federation metadata

One of the core services is the publication and distribution of SAML 2.0 metadata. The metadata is a collection of all identity providers and all service providers in the federation, including technical elements like URL's and X.509 certificates.

2 http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf
3 http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-idp-discovery.html

4.1 Publication

BELNET will publish the federation metadata at https://federation.belnet.be/metadata/re/metadata.xml. It is mandatory to refresh the metadata in your IdP and SP installation every 6 hours, or at a higher refresh frequency.

4.2 Digital signature

The federation operator will sign the federation metadata before publication. The federation operator will use a certificate from BELNET's digital certificate service using the common name 'federation.belnet.be'.

4.3 Submitting entity metadata

Every IdP and every SP has its own piece of metadata (the 'entity metadata'), which is usually generated at installation of the software. To submit or revoke entity metadata from the R&E Federation, please visit (tbc:) https://federation.belnet.be/md-mgmt/ .

5 Attribute Schema

SAML 2.0 transmits identity data from IdPs to SPs in the form of attributes, defined in attribute schema. Identity and service providers are free to use any attributes in any schema that fits their needs, but to make the federation truly interoperable, it is mandatory to use following schema for the limited set of object classes and attributes mentioned:

5.1 Object class inetOrgPerson

inetOrgPerson is an LDAP object class, standardised by the IETF (RFC2798[4] and RFC2256[5]) in order to have a common schema for personal data. This schema is included in most directory implementations.

5.1.1 givenName

From RFC2256: "The givenName attribute is used to hold the part of a person's name which is neither their surname nor middle name." In Belgium this is known as first name ('voornaam' or 'prénom').

5.1.2 sn (surname)

From RFC2256: "This is the X.500 surname attribute, which contains the family name of a person."

4 http://www.ietf.org/rfc/rfc2798.txt
5 http://www.ietf.org/rfc/rfc2256.txt

5.1.3 preferredLanguage

From RFC2798: "Used to indicate an individual's preferred written or spoken language. This is useful for international correspondence or human-computer interaction. Values for this attribute type MUST conform to the definition of the Accept-Language header field defined in [RFC2068] with one exception: the sequence "Accept-Language" ":" should be omitted. This is a single valued attribute type." See also ISO 639 for permissible language codes. Common values in Belgium will be 'nl' and 'fr'.

5.1.4 mail

From RFC1274, referenced in RFC2798: "The [mail] attribute type specifies an electronic mailbox attribute following the syntax specified in RFC 822. Note that this attribute should not be used for greybook or other non-Internet order mailboxes."

5.2 Object class eduPerson

The eduPerson object class[6] is defined as an extension to the inetOrgPerson object class, adding attributes relevant for persons in an educational environment.
Atrributes affiliation, primaryAffiliation and scopedAffiliation are subject to a controlled vocabulary: only a limited set of values with specific meanings can be used here. See next section for details.

5.2.1 Controlled vocabulary for 'affiliation' attributes

The permissible values for affiliation attributes are: faculty, student, staff, alum, member, affiliate, employee, library-walk-in. Semantics of these values are described here, and it is based on the original specification where appropriate, and according to an international comparison of affiliation semantics in R&E federations[7].

faculty

This affiliation can be assigned to workers whose primary role is teaching or research.

student

This affiliation can be assigned to those who are studying at undergraduate or postgraduate level.

staff

This affiliation can be assigned to workers other than teachers or researchers. In Belgium this is generally equivalent to 'administrative & technical personnel'.

6 http://middleware.internet2.edu/eduperson/
7 http://www.terena.org/mail-archives/refeds/docsPFfgEskDv.doc

alum

Referring to alumnus or alumni. This affiliation can be assigned to those who are former students of the organisation. Some variation is common, in whether individuals who did not complete their course are considered alumni.

member

Defined in eduPerson specification: "intended to include faculty, staff, student, and other persons with a basic set of privileges that go with membership in the university community (e.g., they are given institutional email and calendar accounts). It could be glossed as "member in good standing of the university community.""

affiliate

Defined in eduPerson specification: "intended to apply to people with whom the university has dealings, but to whom no general set of "community membership" privileges are extended."

library-walk-in

Defined in eduPerson specification: "This value is intended to facilitate the handling of a fairly widely encountered agreement between an institution and licensed resource providers that e-resources may be made accessible to students, faculty, staff and library walk-ins. This term originally indicated people who were physically present in a library facility. In recent years the library walk-in provision has been extended to cover other cases such as library users on the campus network, or those using on-campus workstations. Licensed resource providers have often been willing to interpret their contracts with licensees to accept this broader definition of "library-walk-in," though specific terms may vary. Under appropriate licensing terms, it is valid to assert an affiliation of "library-walk-in" for members of this broader class of users. The affiliation "library-walk-in" is independent of any other affiliation value. In other words, having the affiliation "library-walk-in" has no effect, positive or negative, on any of the other defined affiliation values. Similarly, no other affiliation value implies or precludes the affiliation "library-walk-in"."

5.2.2 eduPersonAffiliation

From the spec: "Specifies the person's relationship(s) to the institution in broad categories such as student, faculty, staff, alum, etc."

5.2.3 eduPersonPrimaryAffiliation

From the spec: "Specifies the person's PRIMARY relationship to the institution in broad categories such as student, faculty, staff, alum, etc. (...) Appropriate if the person carries at least one of the defined eduPersonAffiliations. The choices of values are the same as for that attribute. (...) Think of this as the affiliation one might put on the name tag if this person were to attend a general institutional social gathering. Note that the single-valued eduPersonPrimaryAffiliation attribute assigns each person in the directory into one and only one category of affiliation."

5.2.4 eduPersonScopedAffiliation

From the spec: "Specifies the person's affiliation within a particular security domain in broad categories such as student, faculty, staff, alum, etc. The values consist of a left and right component separated by an "@" sign. The left component is one of the values from the eduPersonAffiliation controlled vocabulary.This right-hand side syntax of eduPersonScopedAffiliation intentionally matches that used for the right-hand side values for eduPersonPrincipalName since both identify a security domain. Multiple "@" signs are not recommended, but in any case, the first occurrence of the "@" sign starting from the left is to be taken as the delimiter between components. Thus, user identifier is to the left, security domain to the right of the first "@". This parsing rule conforms to the POSIX "greedy" disambiguation method in regluar expression processing."

Scoped affiliation is not mandatory but might be required for some applications.

5.2.5 eduPersonEntitlement

From the spec: "URI (either URN or URL) that indicates a set of rights to specific resources. (...) A simple example would be a URL for a contract with a licensed resource provider. When a principal's home institutional directory is allowed to assert such entitlements, the business rules that evaluate a person's attributes to determine eligibility are evaluated there. The target resource provider does not learn characteristics of the person beyond their entitlement. The trust between the two parties must be established out of band."

Example values for this attribute are 'http://xstor.com/contracts/HEd123' or 'urn:mace:washington.edu:confocalMicroscope'.