Template: Description of the Identity Management of a Home Organization

Haka federation

Version	Author	Date

This document describes the identity management procedures of a home organisation to the extent that is sufficient for assessing the quality and freshness of the identity data in the home organization.

The home organization places this document in the public web and maintains it as the identity management of the institution changes. The document will be linked form Haka federation web pages.

In this document, ”user database” means the collection of attributes available for the Identity Provider server of the home organization. The implementation of the user database can be, for instance, an LDAP directory or a relational database, or any combination of the two.

1. The linking of the base registries and the user database

1.1. Student registry

The data in the student registry is expected to be up-to-date.

How is the user database linked to the student registry?

1.1.1. A new student starts

How do the data of a new student propagate from the student registry to the user database?
When does a new student get his user account or his student role?
What does happen to the user account if the student don’t start his studies or if he starts the studies but registers as being absent?

1.1.2. A change in a student's data

How do the changes in the student registry propagate to the user database?

1.1.3. A student ceases to be a student

When does the organisation decide, that a student isn’t any more a student

a) after he has graduated?
b) after the semester has ended and the student has not enrolled as being present for the next semester?
C) when the student decides to discontinue his studies?

After the event above, how long will it take for the IT services unit to close the student’s user account or to deactivate the ”student” role?

1.2. HR registry

As above.

1.2.1. A new emoployee starts

1.2.2. A change in an employee's data

1.2.3. An employee ceases to be an employee

1.3. Other end users and the freshness of their identity data

Does the organisation have other kind of end users (for example, researchers employed by the Academy of Finland; alumni; civil servants; emeritus professors; library patrons; subcontractors like restaurant staff) who
a) have user accounts, and
b) are allowed to use the Identity Provider to sign in to Service Providers in the Haka federation?

What kind of application procedure there is for their user accounts?
How do you ensure the freshnes of their identity data?

Users, who are not natural persons (for example, student associations, if they have separate accounts) are not considered as end users of Haka federation, and should not be allowed to log in.

2. Authentication

2.1. Initial authentication

How do you verify the identity of a person applying for a user account?

2.2. Authentication during log-in

Requirements for password quality.
Are there any stronger authentication means available?

3. Attributes available in the user database

More information on funetEduPerson schema (ver 2.0) is here.

Place ’X’ in the ’availability’ column if the attribute is up-to-date and thus available for the Identity Provider server.

If the home organization has any own (non-funetEduPerson) attributes, that are available for the Identity Provider server, you can add them to the end of the table, supplemented by a link to the attribute definition.

Attribute	Availability	How do you ensure freshness	Other information
cn / commonName			MUST
description			
displayName			MUST
employeeNumber			
facsimileTelephoneNumber			
givenName			
homePhone			
homePostalAddress			
jpegPhoto			
l / localityName			
labeledURI			
mail			
mobile			
o / organizationName			
ou / organizationalUnitName			
postalAddress			
postalCode			
preferredLanguage			
seeAlso			
sn / surname			MUST
street			
telephoneNumber			
title			
uid			
userCertificate			
eduPersonAffiliation			What values are available?
eduPersonEntitlement			
eduPersonNickName			
eduPersonOrgDN			
eduPersonOrgUnitDN			
eduPersonPrimaryAffiliation			
eduPersonPrimaryOrgUnitDN			

eduPersonPrincipalName			MUST
eduPersonScopedAddiliation			
eduPersonTargetedID			
schacMotherTongue			
schacGender			
schacDateOfBirth			
schacPlaceOfBirth			
schacCountryOfCitizenship			
schacHomeOrganization			MUST. What value is used?
schacHomeOrganizationType			MUST What value is used?
schacCountryOfResidence			
schacUserPresenceID			
schacPersonalUniqueCode			
schacPersonalUniqueID			
schacUserStatus			
funetEduPersonHomeOrganization			superseded
funetEduPersonStudentID			superseded
funetEduPersonIdentityCode			superseded
funetEduPersonDateOfBirth			superseded
funetEduPersonTargetDegreeUniversity			superseded
funetEduPersonTargetDegreePolytech			superseded
funetEduPersonTargetDegree			
funetEduPersonEducationalProgramUniv			superseded
funetEduPersonEducationalProgramPolytech			superseded
funetEduPersonProgram			
funetEduPersonMajorUniv			superseded
funetEduPersonOrientationAlternPolytech			superseded
funetEduPersonSpecialisation			
funetEduPersonStudyStart			
funetEduPersonPrimaryStudyStart			
funetEduPersonStudyToEnd			
funetEduPersonPrimaryStudyToEnd			
funetEduPersonCreditUnits			
funetEduPersonECTS			
funetEduPersonStudentCategory			
funetEduPersonStudentStatus			
funetEduPersonStudentUnion			What value(s) are used?
funetEduPersonHomeCity			
funetEduPersonEPPNTimeStamp			

4. Other issues

4.1. Cardinality

One identity per user or one identity per role (ie a person who is both a student and an employee has two identities)?

4.2. Revocation and reassignment of eduPersonPrincipalName

Can the eduPersonPrincipalName value of an end user change over time?
Do you reassign eduPersonPrincipalName values to new end users?