User Administration Described

Metropolia University of Applied Sciences user administration described

This document discusses the general principles of the implementation of the up-to-dateness of the user database and its data at a level that yields information sufficient to judge the quality and freshness of user information.

The home organization posts this document in the www accessible to everyone and updates it as changes occur. A link to it will be placed on the Haka infrastructure's home page.

In this document the term "user database" refers to the end user attributes' collection available to the organization's Identity Provider server. The technical implementation of the user database can be e.g. an LDAP directory or a relational database or a combination of the two in such a way that the Identity provider server can import some of the attributes from the LDAP directory and some of them from over the JDBC from the student register.

1. The link between the user database and the base register

1.1. Base register

The starting assumption is that Base register personal data is up-to-date.

How is the user database linked to Base register?

Base register is a relational database, that is linked to the user database in real-time with triggers initiating data synchronization.

1.1.1 A new student

How is a new student's data updated from Base register to the user database?

A new student's data is updated in the user database in real-time. A username is created on the basis of the data automatically. If the person already has a username, a new username is not created.

When does a new student get a username/student role?

A new student gets a username after accepting the offer of admission. She will get a student role after registering as present.

What happens to the username if the new student does not accept the offer of admission or accepts it but registers as absent?

A username is not created if the student does not accept the offer. The username of a student registering as absent remains valid.

1.1.2 A change in a student's data

How do changes in a student's information propagate from the student register to the user database?

A student's changed information is updated in the user database in real-time.

1.1.3 A student ceases to be a student

When does the organization (e.g. student administration) consider that a student no longer is a student...

a) after graduation?

b) after the beginning of a new term when the student has not registered as present?

c) after the student reports that she has terminated her studies?

How long does it take after the above mentioned events until the organization (e.g. student administration) close the student's user account or removes the student role?

a) Graduation is recorded in the study register after graduation meeting.

b) approximately 2 months after the beginning of the fall term

c) the termination of studies is recorded in the study register immediately after the case has been processed

Logging in to the Haka infrastructure will be prevented immediately after the above recordings.

1.2. The staff register

The personal data register is the HR system's relational database, and it is linked to the user database via a user interface showing the latest changes which are polled after short scheduled intervals.

1.2.1. A new employee

A new employee's data is updated in the user database almost in real-time. A username is created for the user on the basis of the data. If the person already has a username, a new username is not created.

1.2.2. A change in an employee's data

Changed data is updated in the user database almost in real-time.

1.2.3. An employee ceases to be an employee

An employee ceases to be an employee after she no longer has a current work contract. At the same time also the permission to use the username in that role ends and logging in to the Haka infrastructure is prevented immediately.

1.3. Other users and the up-to-dateness of their identity data

Are there other users in the organization who have a username and who can log in via the Identity Provider server to the Haka infrastructure services (The Academy of Finland researchers? the restaurant staff? persons undergoing non-military service? Docents? Alumni? Professors emeriti? Library clients?). What kind of application and acceptance procedure do these usernames have? How is the users' user data freshness and closing/updating of role data ensured? Users who are not natural persons (e.g. student organizations) are not end users as meant by the Haka infrastructure and their logging in via the Identity Provider server must not be allowed.

Only Metropolia students and staff can log in to the Haka infrastructure services.

2. Confirming identity

2.1 When providing the username

How is a new user's identity confirmed when she is provided with a username?

A user gets infromation about her username by authenticating with a finnish netbanking account or a mobile certificate at http://salasana.metropolia.fi.

A student or an employee (who doesn´t have *finnish netbank or mobile certificate*) gets her user information by other means (instructions)

2.2. When a user logs in using a username

Quality requirements of password authentication. Possible other authentication methods stronger than password authentication.

The minimum length of the password is 8 characters.

3. Data available in the user database

Attribute	Availability	How is freshness secured	Else (e.g. interpretation guide)
cn / commonName	x	updated in real-time	MUST
description			
displayName	x	updated in real-time	MUST
employeeNumber			
facsimileTelephoneNumber			
givenName			
homePhone			
homePostalAddress			
jpegPhoto			
l / localityName			
labeledURI			
mail	x		
mobile	x		
nationalIdentificationNumber	x		
o / organizationName			
ou / organizationalUnitName			
postalAddress			

postalCode			
preferredLanguage	x		
seeAlso			
sn / surname	x	updated in real-time	MUST
street			
telephoneNumber			
title			
uid	x		
userCertificate			
eduPersonAffiliation	x		What values available?
eduPersonEntitlement			
eduPersonNickName			
eduPersonOrgDN			
eduPersonOrgUnitDN			
eduPersonPrimaryAffiliation	x		
eduPersonPrimaryOrgUnitDN			
eduPersonPrincipalName	x		MUST
eduPersonScopedAddiliation	x		
eduPersonTargetedID	x		
schacMotherTongue			
schacGender			
schacDateOfBirth			
schacPlaceOfBirth			
schacCountryOfCitizenship			
schacHomeOrganization	x		MUST. metropolia.fi
schacHomeOrganizationType	x		MUST. urn:mace: terena.org:schac: homeOrganizationType: fi:polytechnic
schacCountryOfResidence			
schacUserPresenceID			
schacPersonalUniqueCode			
schacPersonalUniqueID	x		
schacUserStatus			
funetEduPersonHomeOrganization			superseded
funetEduPersonStudentID			superseded
funetEduPersonIdentityCode			superseded
funetEduPersonDateOfBirth			superseded
funetEduPersonTargetDegreeUniversity			superseded
funetEduPersonTargetDegreePolytech			superseded
funetEduPersonTargetDegree			
funetEduPersonEducationalProgramUniv			superseded
funetEduPersonEducationalProgramPolytech			superseded
funetEduPersonProgram	x	updated in real-time	
funetEduPersonMajorUniv			superseded
funetEduPersonOrientationAlternPolytech			superseded
funetEduPersonSpecialisation			
funetEduPersonStudyStart			

funetEduPersonPrimaryStudyStart			
funetEduPersonStudyToEnd			
funetEduPersonPrimaryStudyToEnd			
funetEduPersonCreditUnits			
funetEduPersonECTS			
funetEduPersonStudentCategory			
funetEduPersonStudentStatus			
funetEduPersonStudentUnion			What values are available?
funetEduPersonHomeCity			
funetEduPersonEPPNTimeStamp			

4. Other issues

4.1. Cardinality

One identity per real-life user, or one identity per role (e.g. a student-employee with two usernames)?

One identity per real-life user.

4.2. EduPersonPrincipalName revocation and recycling

Can a eduPersonPrincipalName change? How does the organization recycle freed eduPersonPrincipalName values?

A username and an eduPersonPrincipalName is changed only on founded grounds.

Freed eduPersonPrincipalNames are kept reserved for two years minimum.

Käyttäjähallinnon kuvaus