

## Kotiorganisaation käyttäjähallinnon kuvaus

### Satakunnan ammattikorkeakoulun käyttäjähallinnon kuvaus

Versio	Tekijä	Päiväys
1.6	Liisa Peltomäki	26.3.2013
1.5	Liisa Peltomäki	26.5.2010
1.4	Liisa Peltomäki	26.4.2010
1.3	Liisa Peltomäki	19.4.2010
1.2	Liisa Peltomäki	31.3.2010
1.1	Liisa Peltomäki	12.3.2010
1.0	Liisa Peltomäki	15.2.2010
0.01	Liisa Peltomäki	6.4.2009

*Tässä dokumentissa ollaan kiinnostuneita käyttäjätietokannan ja sen tietojen ajantasaisuuden toteutuksen yleisistä eriaatteista sellaisella tasolla, joka antaa riittävät tiedot käyttäjätietojen laadun ja ajantasaisuuden arvioimiseksi.*

*Kotiorganisaatio asettaa tämän dokumentin [www.hen](http://www.hen) kaikkien saataville ja päivittää sitä oma-aloitteisesti, kun uutoksia ulee. Dokumentti linkitetään Haka-infrastruktuurin kotisivulta.*

*Tässä dokumentissa käyttäjätietokannalla tarkoitetaan sitä loppukäyttäjien attribuuttien joukkoa, johon organisaation identity Provider-palvelin tukeutuu. Käyttäjätietokannan tekninen toteutus voi olla esim. LDAP-hakemisto tai relaatiotietokanta, tai niiden yhdistelmä niin, että Identity Provider -palvelin noutaa osan attribuuteista LDAP-hakemistosta ja osan JDBC:n yli opiskelijarekisteristä.*

## 1. Käyttäjätietokannan ja perusrekistereiden kytkentä

### 1.1. Opiskelijarekisteri

*Lähtöoletuksena on, että opiskelijarekisterin henkilötiedot ovat ajan tasalla.*

*Miten käyttäjätietokanta on kytketty opiskelijarekisteriin?*

Kerran vuorokaudessa opiskelijahallinto-rekisteristä (Winha) tehdään tietojen siirto muuttuneista tiedoista keskitettyyn käyttäjähallintaan.

#### 1.1.1. Uusi opiskelija

*Miten uuden opiskelijan tiedot päivittyvät opiskelijarekisteristä käyttäjätietokantaan?*

Uuden opiskelijan tiedot päivittyvät käyttäjätietokantaan kerran vuorokaudessa. Uudelle käyttäjälle muodostetaan opiskelijahallinto-rekisterin tietojen perusteella automaattisesti käyttäjätunnus.

*Koska uusi opiskelija saa käyttäjätunnuksen/opiskelijaroolin?*

Uusi opiskelija saa opiskelijanumeronsa mukaisen käyttäjätunnuksen opintojen alussa allekirjoitettuaan ensin tunnuksen liittyvän käyttösitoumus –lomakkeen.

*Mitä tunnukselle tapahtuu, jos uusi opiskelija ei ota opiskelu paikkaa vastaan, tai ottaa paikan vastaan mutta ilmoittautuu poissaolevaksi?*

Tunnusta ei luoda, mikäli opiskelupaikkaa ei oteta vastaan tai uusi opiskelija ilmoittautuu poissaolevaksi.

### **1.1.2. Opiskelijan tiedoissa tapahtuu muutos**

*Miten opiskelijan muuttuneet tiedot päivittyvät opiskelijarekisteristä käyttäjätietokantaan?*

Opiskelijan muuttuneet tiedot päivittyvät käyttäjätietokantaan kerran vuorokaudessa ajastetussa tietojen siirrossa.

### **1.1.3. Opiskelija lakkaa olemasta opiskelija**

*Koska organisaatio (esim. opintoasiainhallinto) katsoo, että opiskelija lakkaa olemasta opiskelija a) sen jälkeen kun opiskelija valmistuu?*

*b) sen jälkeen kun lukukausi vaihtuu, ja opiskelija ei ole ilmoittautunut läsnä olevaksi?*

*c) sen jälkeen kun opiskelija ilmoittaa keskeyttävänsä opinnot?*

*Kuinka kauan yllä olevien tapahtumien jälkeen kestää, että organisaatio (esim. tietohallinto) sulkee opiskelijan käyttäjätunnuksen tai poistaa opiskelijaroolin?*

a) valmistumispäivän jälkeisenä päivänä tunnus sulkeutuu

b) syyskuun laskentapäivänä (20.9), ilmoittautumisvelvollisuutensa laiminlyöneiden tunnus sulkeutuu laskentapäivänä

c) erotiedon merkitsemisen jälkeisenä päivänä tunnus sulkeutuu

## **1.2. Henkilökuntarekisteri**

Henkilörekisterinä toimii opiskelijahallintorekisteri (Winha).

### **1.2.1. Uusi työntekijä**

Uuden työntekijän tiedot päivittyvät käyttäjätietokantaan kerran vuorokaudessa. Käyttäjälle muodostetaan Winhan tietojen perusteella automaattisesti käyttäjätunnus.

Uusi työntekijä saa käyttäjätunnuksen perehdytyksen yhteydessä ja allekirjoitettuaan ensin tunnuksen liittyvän käyttösitoumus –lomakkeen

### **1.2.2. Työntekijän tiedoissa tapahtuu muutos**

Työntekijän muuttuneet tiedot päivittyvät käyttäjätietokantaan kerran vuorokaudessa.

### **1.2.3. Työntekijä lakkaa olemasta työntekijä**

Työntekijä lakkaa olemasta työntekijä, kun hänellä ei ole voimassaolevaa työ- tai virkasuhdetta. Tunnus sulkeutuu työsuhteen päättymisen jälkeisenä päivänä.

## **1.3. Muut käyttäjät ja heidän henkilötietojensa ajantasaisuus**

*Onko organisaatiossa vielä jotainmuuta käyttäjiä, joilla on käyttäjätunnus ja jotka voivat kirjautua Identity Provider -palvelimen kautta Haka-infrastruktuurin palveluihin (Suomen Akatemian tutkijat? Ravintolahenkilökunta? Siviilipalvelusmiehet? Dosentit? Alumnit? Emeritukset? Kirjaston asiakkaat?). Minkälainen haku- ja hyväksymismenettely näihin tunnuksiin liittyy? Miten heidän käyttäjätietojensa ajantasaisuus ja sulkeutuminen/roolitiedon päivittyminen on varmistettu?*

*Sellaiset käyttäjät, jotka eivät ole luonnollisia henkilöitä (esim. ainejärjestöt), eivät ole myöskään Haka-infrastruktuurin tarkoittamia loppukäyttäjiä, eikä heidän kirjautumistaan Identity Provider -palvelimen kauttapalveluihin tule sallia.*

Ainoastaan SAMKissa opiskelevat ja SAMKin henkilökunta voivat kirjautua Haka-infrastruktuurin palveluihin.

## **2. Henkilöllisyyden todentaminen**

### **2.1. Käyttäjätunnuksen antamisen yhteydessä**

*Millä tavalla uuden käyttäjän henkilöllisyys todennetaan, kun hänelle annetaan käyttäjätunnus?*

Opiskelijoiden käyttäjätunnukset jaetaan helpdeskistä, opintotoimistosta tai tutoropettajalta opintojen alkaessa. Opiskelijat saavat tunnuksen käyttöönsä osoitettuaan henkilöllisyytenä poliisin hyväksymästä asiakirjasta. Ulkomaalaisten opiskelijoiden henkilöllisyys todennetaan passista.

Työntekijä saa käyttäjätunnuksen helpdeskistä tai toimistosta. Työntekijän henkilöllisyys todennetaan poliisin hyväksymästä asiakirjasta ennen kuin tunnus luovutetaan henkilölle.

### **2.2. Kun käyttäjä kirjautuu käyttäjätunnuksensa avulla**

*Salasanatodennukseen liittyvät laatuvaatimukset.*

*Mahdolliset käytettävissä olevat salasanaa tukevat autentikointimenetelmät.*

Käyttäjähallinta sekä AD valvovat salapolitiikan noudattamista. Käyttäjien salasanat ovat

- Vähintään 8 merkkiä pitkä
- Pitää sisältää muitakin merkkejä kuin kirjaimia
- Eivät voi sisältää käyttäjä tunnusta, etu- tai sukunimeä
- Pitää olla erilainen kuin 24 edellistä salasanaa

### 3. Käyttäjätietokannassa saatavilla olevat tiedot

*Jos organisaatiolla on omia (ei siis funetEduPersonin mukaisia) attribuutteja, jotka näkyvät ulospäin Identity Provider-palvelimesta, lisää ne taulukon loppuun. Tarvittaessa linkki dokumenttiin, joka tarkemmin kuvailee omien attribuuttien skeeman.*

Attribuutti	Saata -vuus	Miten ajantasaisuus turvataan	Muuta (esim. tulkintaohje)
cn / commonName	X	päivittyy /vrk	MUST
description			
displayName	X	päivittyy /vrk	MUST
employeeNumber			
facsimileTelephoneNumber			
givenName	X	päivittyy /vrk	
homePhone			
homePostalAddress			
jpegPhoto			
l / localityName			
labeledURI			
mail	X	päivittyy /vrk	
mobile			
o / organizationName			
ou / organizationalUnitName	X		
postalAddress			
postalCode			
preferredLanguage	X		
seeAlso			
sn / surname	X	päivittyy /vrk	MUST
street			
telephoneNumber	X		
title			
uid	X		
userCertificate			
eduPersonAffiliation	X		Staff (2), Student (1), Affiliate (3)
eduPersonEntitlement			

eduPersonNickName			
eduPersonOrgDN			
eduPersonOrgUnitDN			
eduPersonPrimaryAffiliation			
eduPersonPrimaryOrgUnitDN			
eduPersonPrincipalName	X	päivittyy /vrk	MUST
eduPersonScopedAffiliation	X		
eduPersonTargetedID	X		
schacMotherTongue			
schacGender			
schacDateOfBirth			
schacPlaceOfBirth			
schacCountryOfCitizenship			
schacHomeOrganization	X		MUST: samk.fi
schacHomeOrganizationType	X	vakio	MUST: urn:mace:terena.org:schac:homeOrganizationType:fi:polytechnic
schacCountryOfResidence			
schacUserPresenceID			
schacPersonalUniqueCode			
schacPersonalUniqueID			
schacUserStatus			
funetEduPersonHomeOrganization			
funetEduPersonStudentID			
funetEduPersonIdentityCode			
funetEduPersonDateOfBirth			
funetEduPersonTargetDegreeUniversity			
funetEduPersonTargetDegreePolytech			
funetEduPersonTargetDegree			
funetEduPersonEducationalProgramUniv			
funetEduPersonEducationalProgramPolytech			
funetEduPersonProgram	X	päivittyy 1/vrk	

funetEduPersonMajorUniv			
funetEduPersonOrientationAltern Polytech			
funetEduPersonSpecialisation			
funetEduPersonStudyStart			
funetEduPersonPrimaryStudyStart			
funetEduPersonStudyToEnd			
funetEduPersonPrimaryStudyToE nd			
funetEduPersonCreditUnits			
funetEduPersonECTS			
funetEduPersonStudentCategory			
funetEduPersonStudentStatus			
funetEduPersonStudentUnion			Mikä arvo on käytössä?
funetEduPersonHomeCity			
funetEduPersonEPPNTimeStamp			
logout-url	X	vakio	https://idp.samk.fi:8443/idp/logout

## 4. Muuta

### 4.1. Kardinaliteetit

*Yksi henkilöllisyys per tosielämän käyttäjä, vai Yksi henkilöllisyys per rooli (esim. opiskelija-työntekijällä kaksi käyttäjätunnusta)?*

Yksi henkilöllisyys roolia kohden

### 4.2. EduPersonPrincipalNamen revokointi ja kierrätys

*Voiko eduPersonPrincipalName vaihtua?*

*Millä tavalla organisaatio kierrättää vapautuneita eduPersonPrincipalName-arvoja?*

Käyttäjätunnus (eduPersonPrincipalname) vaihdetaan henkilökunnalle vain erittäin painavasta syystä. Vapautuneet eduPersonPrincipalname:t pidetään varattuna