Haka-infrastruktuuri

Kotiorganisaation käyttäjähallinnon kuvaus

Versio	Tekijä	Päiväys
1.0	Esa Mätäsaho	23.10.2009
1.1	Iikka Kupari	20.04.2010
1.2	Iikka Kupari	4.10.2010
1.3	Iikka Kupari	18.11.2010
1.4	Esa Mätäsaho	25.6.2014
1.5	Iikka Kupari	3.7.2014

Tässä dokumentissa kuvataan Lapin yliopiston käyttäjähallintoa. Käyttäjähallinnosta vastaa yliopiston ATK-palvelut yksikkö.

Käyttäjätietokannan tekninen toteutus on Windows-verkon käyttäjähakemisto (AD), mistä Identity Provider -palvelin noutaa attribuutit. Windows-verkon käyttäjähakemistoa ylläpidetään keskitetyn käyttäjähallinnon järjestelmän avulla (FIM), opiskelijarekisterin (Oodi) ja henkilökuntarekisterin (Personec.F) tietojen pohjalta.

1. Käyttäjätietokannan ja perusrekistereiden kytkentä

1.1. Opiskelijarekisteri

Lapin yliopiston opiskelijarekisterinä käytetään Oodi-järjestelmää. Käyttäjähallinnon kannalta olennaiset opiskelijatiedot synkronoidaan keskitetyn käyttäjähallinnon järjestelmään automaattisesti kerran vuorokaudessa ja Windows-verkon käyttäjähakemistoon viidesti viikossa (arkipäisivisin) käyttöpalveluhenkilöstön toimenpitein.

1.1.1. Uusi opiskelija

Uusille läsnä oleviksi ilmoittautuneille opiskelijoille perustetaan opiskelijarekisterissä olevien tietojen pohjalta uusi käyttäjätili käyttäjähakemistoon. Samalla opiskelijalle perustetaan sähköpostilaatikko organisaation sähköpostijärjestelmään. Käyttäjätunnukset aktivoidaan henkilökohtaisilla suomalaisilla verkkopankkitunnisteilla tai mobiilivarmenteella . Jos pankkitunnuksia tai mobiilivarmennetta ei ole käytössä, käyttäjä ottaa yhteyttä yliopiston opiskelijoiden Helpdeskiin.

Myös poissaolevaksi ilmoittautuneelle opiskelijalle luodaan käyttäjätili ja sähköpostitunnus ja ne ovat hänen käytettävissään myös poissaoloajan.

1.1.2. Opiskelijan tiedoissa tapahtuu muutos

Opiskelijarekisterissä muuttuneet tiedot päivitetään Windows-verkon käyttäjähakemistoon viidesti viikossa (arkipäisin).

1.1.3. Opiskelija lakkaa olemasta opiskelija

Organisaatio katsoo, että opiskelija lakkaa olemasta opiskelija

a) sen jälkeen kun opiskelija on valmistunut
b) keskeyttää opintonsa
c) kun opiskelija poistetaan kirjoilta muusta syystä

Päivittäisen tiedonsiirron yhteydessä tuodaan läsnäolo- tai valmistunut tieto opiskelijarekisteristä keskitetyn käyttäjähallinnon järjestelmään. 28 päivää opiskelijastatuksen päättymisestä käyttäjätunnus lukittuu, sen roolitiedot (eduPersonAffiliation) poistuvat ja sähköpostin vastaanottaminen loppuu. Nämä toimenpiteet tapahtuvat automaattisesti.

1.2. Henkilökuntarekisteri

Henkilökuntarekisteristä siirretään käyttäjähallinnon kannalta olennaiset henkilökuntatiedot keskitetyn käyttäjähallinnon järjestelmään kerran vuorokaudessa ja Windows-verkon käyttäjähakemistoon viidesti viikossa (arkipäivisin).

1.2.1. Uusi työntekijä

Uuden työntekijän tiedot saadaan henkilökuntarekisteristä niiden tallentamista seuraavana päivänä. Keskitetyn käyttäjähallinnon järjestelmän tietojen perusteella työntekijälle luodaan käyttäjätunnus automaattisesti. Jos uudella työntekijällä on ollut käyttäjätunnus (esim. työsuhde on keskeytynyt lyhyeksi aikaa), mutta ei käyttöoikeutta, saa hän saman tunnuksen uudelleen käyttöönsä.

1.2.2. Työntekijän tiedoissa tapahtuu muutos

Päivittäisen tiedonsiirron yhteydessä tuodaan tieto henkilökuntarekisteristä keskitetyn käyttäjähallinnon järjestelmään, josta tiedot päivitetään Windows-verkon käyttäjähakemistoon viidesti viikossa (arkipäivisin).

1.2.3. Työntekijä lakkaa olemasta työntekijä

Päivittäisen tiedonsiirron yhteydessä tuodaan tieto henkilökuntarekisteristä keskitetyn käyttäjähallinnon järjestelmään, josta tiedot päivitetään Windows-verkon käyttäjähakemistoon viidesti viikossa (arkipäivisin).

Työntekijä lakkaa olemasta työntekijä, kun hänellä ei ole voimassaolevaa työ- tai virkasuhdetta. Seitsemän päivää työsuhteen päättymisestä käyttäjätunnus lukittuu, sen roolitiedot (eduPersonAffiliation) poistuvat ja sähköpostin vastaanottaminen loppuu. Nämä toimenpiteet tapahtuvat automaattisesti.

1.3. Muut käyttäjät ja heidän henkilötietojensa ajantasaisuus

Käyttäjätunnus voidaan myöntää myös Lapin yliopiston ulkopuoliselle henkilölle, joka perustellusta syystä tarvitsee tunnusta. Tavallisimpia ryhmiä ovat sivutoimiset tuntiopettajat, emeritukset ja huoltohenkilökunta. Nämä tunnukset ovat aina määräaikaisia. Näiden tunnuksien myöntämisestä päättää niitä anovan tiedekunnan tai erillislaitoksen henkilökunta.

Ulkopuolisten käyttäjien (ufo-käyttäjät) tiedot talletetaan ufo-käyttäjärekisteriin. Ulkopuolisen käyttäjän tunnuksen anoja kirjataan ufo-rekisteriin myönnetyn identiteetin omistajaksi. Tunnus sulkeutuu välittömästi anotun käyttöoikeuden päättymispäivän jälkeen.

Ulkopuolisten käyttäjien tiedot päivittyvät Windows-verkon käyttäjähakemistoon ajastettujen tiedonsiirtojen yhteydessä.

2. Henkilöllisyyden todentaminen

2.1. Käyttäjätunnuksen antamisen yhteydessä

Opiskelija saa käyttäjätunnustiedot lukukauden alussa tapahtuvassa tunnustenjakotilaisuudessa ja sen jälkeen ICT-HelpDeskistä. Opiskelijan henkilöllisyys todennetaan kuvallisella henkilötodistuksella (ajokortti, passi, viranomaisen antama henkilötodistus) ennen tietojen luovuttamista.

Työntekijöiden ja ufojen käyttäjätunnustiedot lähetetään sisäisessä postissa laitoksen sihteerille, joka välittää tiedot eteenpäin. Henkilötietojen tarkastus on tehty työsopimuksen allekirjoituksen yhteydessä.

2.2. Kun käyttäjä kirjautuu käyttäjätunnuksensa avulla

Salasanavaatimuksena on: vähintään kahdeksan merkkiä pitkä, muistetaan kolme viimeistä salasanaa ja salasana vanhenee 6 kuukaudessa.

Lisäksi tiedotuksella ohjeistetaan käyttämään salasanassa isoja ja pieniä kirjaimia, numeroita ja erikoismerkkejä.

3. Käyttäjätietokannassa saatavilla olevat tiedot

Attribuutti	Saatavuus	Miten ajantasaisuus turvataan	Muuta (esim. tulkintaohje)
cn / commonName	x	Viisi kertaa viikossa	MUST
description			
displayName	x	Viisi kertaa viikossa	MUST
employeeNumber	x	Viisi kertaa viikossa	Henkilökuntanumero
facsimileTelephoneNumber			
givenName			
homePhone			
homePostalAddress			

jpegPhoto			
l / localityName			
labeledURI			
mail	x	Viisi kertaa viikossa	
mobile			
o / organizationName			
ou / organizationalUnitName			
postalAddress			
postalCode			
preferredLanguage	x	Manuaalinen ylläpito	Lisätään tarvittaessa ”fi” tai ”en”
seeAlso			
sn / surname	x	Viisi kertaa viikossa	MUST
street			
telephoneNumber			
title			
uid			
userCertificate			
eduPersonAffiliation	x	Viisi kertaa viikossa	Member, Affiliate, Student, Faculty, Alumn, Faculty Affiliate, Staff
eduPersonEntitlement	x	Manuaalinen ylläpito	CSC:n tietohallintoroolin määritys
eduPersonNickName			
eduPersonOrgDN			
eduPersonOrgUnitDN			
eduPersonPrimaryAffiliation			
eduPersonPrimaryOrgUnitDN			
eduPersonPrincipalName	x	Viisi kertaa viikossa	Uniikki, staattinen
eduPersonScopedAddiliation			
eduPersonTargetedID			
schacMotherTongue			
schacGender			

schacDateOfBirth			
schacPlaceOfBirth			
schacCountryOfCitizenship			
schacHomeOrganization	x	Viisi kertaa viikossa	ulapland.fi
schacHomeOrganizationType	x	Viisi kertaa viikossa	university
schacCountryOfResidence			
schacUserPresenceID			
schacPersonalUniqueCode	x	Viisi kertaa viikossa	Opiskelijanumero
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	x	Viisi kertaa viikossa	”absent” tai ”present”
funetEduPersonStudentUnion			

funetEduPersonHomeCity			
funetEduPersonEPPNTimeStamp			

4. Muuta

4.1. Kardinaliteetit

Yhdellä luonnollisella henkilöllä on yksi identiteetti käyttäjähallintojärjestelmässä, lukuun ottamatta ylläpitohenkilöstöä, joilla on tavallisen käyttäjätunnuksen lisäksi ylläpitotunnus.

Käyttäjän roolitiedot ja käyttöoikeudet muuttuvat automaattisesti opinto-oikeuksien ja työsuhteiden alkaessa ja päättyessä.

4.2. EduPersonPrincipalNamen revokointi ja kierrätys

Tunnus ei voi vaihtua ellei synnytetä uutta identiteettiä. Käyttäjätunnusta ei vaihdeta ilman erityisen painavaa syytä.
Tunnusoikeuden poistuttua, tunnus lukitaan kuudeksi kuukaudeksi, minkä jälkeen se poistetaan.
Mikäli sama henkilö palaa työ- tai opintosuhteeseen, sama tunnus aktivoidaan hänen käyttöönsä.
Tunnuksia ei kierrätetä.