Kotiorganisaation käyttäjähallinnon kuvaus (Karelia)

Versio	Tekijä	Päiväys
0.1	OP, TH	14.11.2006
0.2	OP, TH	12.1.2007
0.3	OP	28.6.2007
0.5	TH, OP (1.3 tarkennus)	26.10.2007
0.6	OP, TH (primaryAffiliation)	27.9.2013
0.7	OP, TH (Karelian tekstiversio)	25.6.2015

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

Kotiorganisaatio asettaa tämän dokumentin www:hen kaikkien saataville ja päivittää sitä omaaloitteisesti, kun muutoksia tulee. 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?

Opiskelijoiden tiedot synkronoidaan opiskelijahallintojärjestelmästä (Winha) Novell eDirectoryyn (eDir), joka toimii Karelia ammattikorkeakoulun (amk) metahakemistona (meta). Winhaa ylläpitää opintotoimiston henkilöstö. Winhan tiedot päivittyvät kerran vuorokaudessa raporttikantaan, josta opiskelijoiden tiedot päivittyvät edelleen eDirectoryyn.

1.1.1. Uusi opiskelija

Miten uuden opiskelijan tiedot päivittyvät opiskelijarekisteristä käyttäjätietokantaan?
Koska uusi opiskelija saa käyttäjätunnuksen/opiskelijaroolin?
Mitä tunnukselle tapahtuu, jos uusi opiskelija ei ota opiskelupaikkaa vastaan, tai ottaa paikan vastaan mutta ilmoittautuu poissaolevaksi?

Opiskelijapalvelut lisäävät uuden opiskelijan opiskelijarekisteriin, tieto siirtyy opiskelijahallinnon raporttikantaan ja edelleen käyttäjätietokantaan kerran vuorokaudessa tapahtuvan eräajon avulla. Opiskelijarekisteristä saatavien tietojen perusteella opiskelijalle generoidaan käyttäjätunnus ja

sähköpostiosoite. Ottaessaan opiskelupaikan vastaan uusi opiskelija sitoutuu noudattamaan oppilaitoksen määrittelemiä sääntöjä. Tunnukset aktivoidaan uusille läsnä oleviksi ilmoittautuneille opiskelijoille ja kirjautumisohjeet annetaan opiskelijalle opiskelun alkaessa.

1.1.2. Opiskelijan tiedoissa tapahtuu muutos

Miten opiskelijan muuttuneet tiedot päivittyvät opiskelijarekisteristä käyttäjätietokantaan?

Tiedot päivitetään kerran vuorokaudessa automaattisesti opiskelijarekisteristä metahakemistoon.

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?

Opiskelija lakkaa olemasta opiskelija kun hän valmistuu, eroaa, opiskeluoikeus päättyy tai kun opiskelija ei ole ilmoittautunut läsnä olevaksi opiskelijaksi. Opiskelijan käyttäjätunnus asetetaan ”ei käytössä” -tilaan ja opiskelijarooli poistetaan (vuorokauden viive).

1.2. Henkilökuntarekisteri

Henkilökunnan osalta toimitaan vastaavasti kuin edellä. Henkilökunnan tietoja saadaan käyttölupahakemusjärjestelmästä (KH-lupakanta, EOS-järjestelmä) ja palkkahallintojärjestelmästä (Fortime) metahakemistoon.

1.2.1. Uusi työntekijä

Yksikön esimies lisää uuden työntekijän tiedot käyttölupahakemusjärjestelmään kun työsopimus tehdään. Tunnus muodostuu esimiehen antamien tietojen perusteella ja aktivoituu välittömästi. Tiedot päivittyvät automaattisesti metahakemistoon. Esimies tai hänen ilmoittamansa henkilö luovuttaa työntekijälle käyttäjätunnuksiin liittyvät tiedot.

1.2.2. Työntekijän tiedoissa tapahtuu muutos

Esimiehet voivat päivittää työntekijän tietoja käyttölupahakemusjärjestelmän kautta (esim. palvelussuhteen voimassaolotieto, sukunimi). Tiedot päivittyvät kerran tunnissa käyttäjähakemistoihin.

Työntekijän työsuhteen päättyminen tai pitkästä poissaoloista kertovat tiedot päivitetään henkilöstöhallinnon antamien tietojen perusteella käyttölupahakemusjärjestelmään. Sieltä tiedot päivittyvät käyttäjähakemistoihin.

1.2.3. Työntekijä lakkaa olemasta työntekijä

Kun henkilöllä ei ole voimassaolevaa työ/virkasuhdetta. henkilön käyttäjätunnus asetetaan ”ei käytössä”-tilaan ja henkilökuntarooli poistetaan metahakemistosta. Tiedot päivitetään henkilöstöhallinnon antamien tietojen perusteella käyttölupahakemusjärjestelmään. Sieltä tiedot päivittyvät käyttäjähakemistoihin.

1.3. Muut käyttäjät ja heidän henkilötietojensa ajantasaisuus

Onko organisaatiossa vielä jotain muita 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 kautta palveluihin tule sallia.

Käyttölupien myöntämisestä päättävät toimipisteiden esimiehet. Muita tunnuksia voivat tehdä yksiköiden esimiehet edellä mainitun käyttölupahakemusjärjestelmän kautta. Muihin käyttäjiin luetaan vierailevat luennoitsijat, harjoittelijat, tietojärjestelmätoimittajat, palvelutoimittajat ja sellaiset yhteistyökumppanit, joilla ei ole työsuhdetta organisaatiossa, mutta jotka kuitenkin tarvitsevat tunnuksen työtehtävän tai projektiin osallistumisen vuoksi.

Muut tunnukset tehdään aina määräajaksi ja ne saavat eduPersonAffiliation arvon ”Affiliate”.

Kun uusi tunnus tehdään ryhmään muut tunnukset, voi sen voimassaoloksi määrittää korkeintaan kaksi vuotta eteenpäin. Mikäli muut käyttäjät -ryhmään kuuluvan tunnuksen käyttötarve lakkaa aiemmin kuin on arvioitu tunnusta myönnettäessä, merkitsee tunnuksesta vastaava henkilö uuden päättymispäivämäärän käyttölupahakemusjärjestelmään. Muut käyttäjät -ryhmään kuuluville tunnuksille määritetään aina hyväksyjä ja vastuuhenkilö.

2. Henkilöllisyyden todentaminen

2.1. Käyttäjätunnuksen antamisen yhteydessä

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

Käyttäjätunnus aktivoidaan sen jälkeen kun henkilön identiteetti on varmistunut (esim. hakujärjestelmän tai muun vastaavan palvelun tunnistamisen tai henkilöllisyystodistuksen avulla).

2.2. Kun käyttäjä kirjautuu käyttäjätunnuksensa avulla

Salasanatodennukseen liittyvät laatuvaatimukset.
Mahdolliset käytettävissä olevat salasanaa tukevammat autentikointimenetelmät.

Salasanan minimipituus on 8 merkkiä, salasanassa tulee olla merkkejä vähintään kolmesta eri merkkiryhmästä. Salasanan vaihtoväli 6 kk.

3. Käyttäjätietokannassa saatavilla olevat tiedot

Lisätietoja funetEduPerson-skeemasta (ver 2.0) on täällä.

Rasti kohtaan "Saatavuus", jos kyseinen henkilötieto on ajan tasalla ja siten saatavilla Identity Provider -palvelimen yli.
Kohtaan "Miten ajantasaisuus turvataan" esimerkiksi viittaus luvun 1. järjestelmiin.

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	Saatavuus	Miten ajantasaisuus turvataan	Muuta (esim. tulkintaohje)
cn / commonName	x	rekistereistä kerran vuorokaudessa	MUST
description			
displayName	x	rekistereistä kerran vuorokaudessa	MUST
employeeNumber			
facsimileTelephoneNumber			
givenName	x	rekistereistä kerran vuorokaudessa	
homePhone			
homePostalAddress			
jpegPhoto			
l / localityName			
labeledURI			
mail			
mobile			
o / organizationName			
ou / organizationalUnitName			
postalAddress			
postalCode			
preferredLanguage			
seeAlso			

sn / surname	x	rekistereistä ker-ran vuorokaudessa	MUST
street			
telephoneNumber			
title			
uid			
userCertificate			
eduPersonAffiliation	x	rekistereistä ker-ran vuorokaudessa	Mitä arvoja on saa-tavilla? student, facul-ty, staff, employee, member, affiliate, alumn
eduPersonEntitlement			
eduPersonNickName			
eduPersonOrgDN			
eduPersonOrgUnitDN			
eduPersonPrimaryAffiliation	x	rekisteristä ker-ran vuorokaudessa	Joku näistä: student, faculty, staff, member
eduPersonPrimaryOrgUnitDN			
eduPersonPrincipalName	x	rekistereistä ker-ran vuorokaudessa	MUST
eduPersonScopedAffiliation			
eduPersonTargetedID			
schacMotherTongue			
schacGender			
schacDateOfBirth			
schacPlaceOfBirth			
schacCountryOfCitizenship			
chacHomeOrganization	x	vakiotieto	MUST. Mikä arvo käytössä? pkamk.fi
schacHomeOrganizationType	x	vakiotieto	MUST Mikä arvo on käytös-sä? fi:polytechnic
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			Mikä arvo on käytössä? Ei mitään.
funetEduPersonHomeCity			
funetEduPersonEPPNTimeStamp			

4. Muuta

4.1. Kardinaliteetit

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

Yksi käyttäjätunnus per rooli. Jos henkilö on opiskelija sekä työntekijä, on hänellä kaksi käyttäjätunnusta.

4.2. EduPersonPrincipalNamen revokointi ja kierrätys

Voiko eduPersonPrincipalName vaihtua?
Millä tavalla organisaatio kierrättää vapautuneita eduPersonPrincipalName-arvoja?

eduPersonPrincipalName muuttuu vain perustellusta syystä (esim. sukunimen vaihtuminen). Jos opiskelijasta tulee työntekijä, muuttuu eduPersonPrincipalName.

Vanhoja eduPersonPrincipalName-arvoja kierrätetään, kiertoväli on 24 kk.