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
0.8	TH	12.3.2018
0.9	TH	10.9.2020
1.0	TH, JV	10.2.2022

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 oma-aloitteisesti, 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 LDAPhakemistosta 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 (Peppi) keskitettyyn käyttäjähakemistoon Active Directoryyn (AD). Opiskelijapalvelujen henkilöstö ylläpitää opiskelijoiden tietoja. Pepin tiedot päivittyvät kerran vuorokaudessa ns. connectorien avulla keskitettyyn käyttäjähakemistoon.

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 käyttäjätietokantaan kerran vuorokaudessa tapahtuvien eräajojen avulla. Opiskelijarekisteristä saatavien tietojen perusteella opiskelijalle generoidaan Kareliatunnus ja sähköpostiosoite. Ottaessaan opiskelupaikan vastaan uusi opiskelija sitoutuu noudattamaan oppilaitoksen määrittelemiä sääntöjä. Opiskelija voi aktivoida käyttäjätunnuksen tunnushallinnon palvelussa mobiilivarmenteella tai pankkitunnuksilla. Opiskelija voi käydä myös Helpdeskissä todistamassa henkilöllisyytensä virallisen henkilöasiakirjan kanssa tai Helpdesk tunnistaa henkilön videoyhteyden yli kuvallisesta henkilöllisyystodistuksesta, jonka jälkeen Helpdesk aktivoi tunnuksen. Poissaolevaksi ilmoittautuneen opiskelijan Kareliatunnus on aktiivinen, poissaolokausi huomioidaan eduPersonAffiliation ja eduPersonPrimaryAffiliation –attribuuteissa.

1.1.2. Opiskelijan tiedoissa tapahtuu muutos

Miten opiskelijan muuttuneet tiedot päivittyvät opiskelijarekisteristä käyttäjätietokantaan?

Tiedot päivittyvät kerran vuorokaudessa opiskelijarekisteristä keskitettyyn käyttäjähakemistoon.

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. Tutkintoon valmistuneen opiskelijan käyttäjätunnus on voimassa 14 vuorokautta valmistumispäivästä. Muussa kuin edellä mainituissa tapauksessa opiskelijan käyttäjätunnus asetetaan ”ei käytössä” -tilaan ja opiskelijarooli poistetaan 1 vrk:n kuluessa opinto-oikeuden päättymisestä.

1.2. Henkilökuntarekisteri

Henkilökunnan osalta toimitaan vastaavasti kuin edellä. Henkilökunnan tiedot saadaan henkilöstöhallinnon ylläpitämästä HR-tietojärjestelmästä (Personec).

1.2.1. Uusi työntekijä

Uuden työntekijän tiedot saadaan HR-tietojärjestelmästä sen jälkeen kun työsopimusprosessi on valmistunut. HR:stä saatujen tietojen perustella muodostuu työntekijälle Kareliatunnus ja sähköpostiosoite. Jos työntekijä on ollut aiemmin Kareliassa työntekijänä, saa hän käyttöönsä aiemman Kareliatunnuksen. Uusi työntekijä voi saada Kareliatunnuksen ennen työsopimuksen alkua, mikäli esimies katsoo sen tarpeelliseksi työtehtävien, kuten opetuksen valmistelutehtävien vuoksi. Esimies tai hänen ilmoittamansa henkilö luovuttaa työntekijälle käyttäjätunnuksiin liittyvät tiedot. Työntekijän Kareliatunnus on mahdollista aktivoida tunnushallinnon palvelussa mobiilivarmenteella tai pankkitunnuksilla. Työntekijä voi käydä myös Helpdeskissä osoittamassa henkilöllisyytensä virallisen henkilöasiakirjan kanssa, jonka jälkeen Helpdesk aktivoi tunnuksen.

1.2.2. Työntekijän tiedoissa tapahtuu muutos

Työntekijän työsuhteen päättymispäivämäärä päivittyy HR-järjestelmän tietojen perusteella käyttäjähakemistoon.

1.2.3. Työntekijä lakkaa olemasta työntekijä

Henkilöstöhallinnon järjestelmästä saadaan henkilön työsuhteen päättymispäivä, jolloin henkilön käyttäjätunnus muuttuu ”ei käytössä”-tilaan. Tiedot päivittyvät kerran vuorokaudessa.

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 yksiköiden esimiehet. Muita tunnuksia voivat pyytää yksiköiden esimiehet tai ylin johto tekemällä tunnuspyynnön Helpdesk-järjestelmään. 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 yksi vuosi eteenpäin. Mikäli muut käyttäjät -ryhmään kuuluvan tunnuksen käyttötarve lakkaa aiemmin kuin on arvioitu tunnusta myönnettäessä, tunnuksesta vastaava henkilö ilmoittaa päättymispäivämäärän Helpdeskiin. Muut käyttäjät -ryhmään kuuluville tunnuksille määritetään aina vastuuhenkilö.

2. Henkilöllisyyden todentaminen

2.1. Käyttäjätunnuksen antamisen yhteydessä

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

Kareliatunnus on mahdollista aktivoida verkkopalvelussa sähköisesti tai henkilökohtaisella käynnillä Helpdeskissä todistamalla henkilöllisyys kuvallisella henkilöasiakirjalla.

2.2. Kun käyttäjä kirjautuu käyttäjätunnuksensa avulla

Salasanatodennukseen liittyvät laatuvaatimukset.
Mahdolliset käytettävissä olevat salasanaa tukevammat autentikointimenetelmät.

Salasanan minimipituus on 10 merkkiä, salasanassa tulee olla merkkejä vähintään kolmesta eri merkkiryhmästä. Salasanan vaihtoväli 6 kk.

3. Käyttäjätietokannassa saatavilla olevat tiedot

Lisätietoja funetEduPerson-skeemasta (ver 2.4) 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	x		henkilökunta
displayName	x	rekistereistä kerran vuorokaudessa	MUST
employeeNumber	x	rekistereistä kerran vuorokaudessa	henkilökunta
facsimileTelephoneNumber			
givenName	x	rekistereistä kerran vuorokaudessa	
homePhone			
homePostalAddress			
jpegPhoto			
l / localityName			
labeledURI			
mail	x	rekistereistä kerran vuorokaudessa	
mobile			
o / organizationName			
ou / organizationalUnitName			
postalAddress			
postalCode			
preferredLanguage			
seeAlso			
sn / surname	x	rekistereistä kerran vuorokaudessa	MUST
street			
telephoneNumber			
title	x	rekistereistä kerran vuorokaudessa	henkilökunta
uid	x	rekistereistä kerran vuorokaudessa	MUST
userCertificate			
eduPersonAffiliation	x	rekistereistä kerran vuorokaudessa	Mitä arvoja on saatavilla? student, faculty, staff,

			employee, member, affiliate, alumn
eduPersonEntitlement	x	vakiotieto	https://info.funet.fi
eduPersonNickName			
eduPersonOrgDN			
eduPersonOrgUnitDN			
eduPersonPrimaryAffiliation	x	rekistereistä kerran vuorokaudessa	joku näistä: student, faculty, staff, member
eduPersonPrimaryOrgUnitDN			
eduPersonPrincipalName	x	rekistereistä kerran vuorokaudessa	MUST
eduPersonScopedAffiliation	x	rekistereistä kerran vuorokaudessa	
eduPersonTargetedID			
schacMotherTongue			
schacGender			
schacDateOfBirth			
schacPlaceOfBirth			
schacCountryOfCitizenship			
chacHomeOrganization	x	vakiotieto	MUST, Vakioarvo: pkamk.fi
schacHomeOrganizationType	x	vakiotieto	MUST, Vakioarvo: fi:polytechnic
schacCountryOfResidence			
schacUserPresenceID			
schacPersonalUniqueCode			
schacPersonalUniqueID	x	rekistereistä kerran vuorokaudessa	
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			
funetEduPersonHomeCity			
funetEduPersonEPPNTimeStamp			
funetEduPersonGivenNames	x	rekistereistä kerran vuorokaudessa	
funetEduPersonFullName	x	rekistereistä kerran vuorokaudessa	
funetEduPersonLearnerId	x	rekistereistä kerran vuorokaudessa	

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 eduPersonPrincipalNamearvoja?

eduPersonPrincipalName muuttuu vain perustellusta syystä (esim. sukunimen vaihtuminen henkilökunnalla). Jos opiskelijasta tulee työntekijä, muuttuu eduPersonPrincipalName. eduPersonPrincipalName-arvoja ei kierrätetä henkilöltä toiselle henkilölle. Henkilö voi saada saman ePPN arvon kuin hänellä on ollut aiemmin käytössään.