Kotiorganisaation käyttäjähallinnon kuvaus (Poliisiammattikorkeakoulu ja Pelastusopisto)

Versio	Tekijä	Päiväys
0.1	EL	8.12.2016
1.0	EL	27.3.2017
1.1	TL	29.3.2017
2.0	EL	4.4.2017
2.1	TL	6.4.2017

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 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?

Active Directory tiedot päivitetään eräajona opiskelijahallinnan järjestelmästä.

1.1.1. Uusi opiskelija

Miten uuden opiskelijan tiedot päivittyvät opiskelijarekisteristä käyttäjätietokantaan?
Koska uusi opiskelija saa käyttäjätunnuksen/opiskelijaroolin?

Opiskelijatiedot luodaan ensin opiskelijarekisteriin, josta opiskelijatiedot siirretään erillisellä tiedostolla AD:hen ja uudet tunnukset luodaan ja käyttäjän tiedot lisätään AD:hen.

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

Tunnukset luovutetaan henkilökohtaisesti opiskelijalle. Mikäli opiskelija ei saavu paikalle hänelle ei luovuteta tunnuksia.

1.1.2. Opiskelijan tiedoissa tapahtuu muutos

Miten opiskelijan muuttuneet tiedot päivittyvät opiskelijarekisteristä käyttäjätietokantaan?

Opiskelijan tiedot päivitetään virkailijan toimesta opiskelijahallintojärjestelmään ja AD:hen.

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

Kuinka kauan ylläolevien 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 muutetaan passiiviseksi ja lukitaan 3 arkipäivän kuluessa.

1.2. Henkilökuntarekisteri

Henkilökunnan osalta menettelymalli on sama kuin opiskelijoilla. Henkilön statustiedot saadaan erillisinä ilmoituksina henkilöstöhallinnon järjestelmästä.

1.2.1. Uusi työntekijä

Uuden käyttäjän tunnuksenluontipyyntö tulee henkilöstöhallinnon järjestelmästä tietohallinnon tikettijärjestelmään ja tunnus luodaan manuaalisesti.

1.2.2. Työntekijän tiedoissa tapahtuu muutos

Palvelussuhdetietojen muutokset tehdään tietohallinnon tikettijärjestelmään muutostilanteissa ja tiedot päivitetään oppilaitoksen AD:hen.

1.2.3. Työntekijä lakkaa olemasta työntekijä

Kun henkilöllä ei ole voimassaolevaa virkasuhdetta. Henkilön käyttäjätunnus muutetaan passiiviseksi ja lukitaan viimeistään 3 arkipäivän kuluessa.

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.

Muiden organisaatioiden käyttäjiksi lasketaan siviilipalvelusmiehet, apurahatutkijat ja korkeakouluharjoittelijat, Pelastusopiston vartijat sekä harjoitusalueen tekninen henkilöstö. Heidän tunnuspyynnöt ja muutostiedot tulevat kyseisten sopimusten omistajilta. Muilla käyttäjillä ei ole pääsyä HAKA palveluihin.

2. Henkilöllisyyden todentaminen

2.1. Käyttäjätunnuksen antamisen yhteydessä

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

Käyttäjältä tarkistetaan henkilöllisyys tunnuksen luovutuksen yhteydessä.

2.2. Kun käyttäjä kirjautuu käyttäjätunnuksensa avulla

Salasanatodennukseen liittyvät laatuvaatimukset.

Salasana pituus vähintään 12 merkkiä, vähintään 3 seuraavista: iso-, pieni kirjain, numero tai erikoismerkki.

Mahdolliset käytettävissä olevat salasanaa tukevammat autentikointimenetelmät.

Käytössä on toimikorttikirjautuminen ja kaksivaiheinen tunnistaminen osassa palveluita kampusverkon ulkopuolelta.

3. Käyttäjätietokannassa saatavilla olevat tiedot

Lisätietoja funetEduPerson-skeemasta on täällä.

Rasti kohtaan "Saatavuus", jos kyseinen henkilötieto on ajantasalla 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	Kohdat 1.1, 1.2	MUST
description			
displayName	X	Kohdat 1.1, 1.2	MUST
employeeNumber			
facsimileTelephoneNumber			
givenName	X	Kohdat 1.1, 1.2	
homePhone			
homePostalAddress			
jpegPhoto			
l / localityName			
labeledURI			
mail	X	Kohdat 1.1, 1.2	
mobile			
o / organizationName			
ou / organizationalUnitName			
postalAddress			
postalCode			
preferredLanguage			
seeAlso			
sn / surname	X	Kohdat 1.1, 1.2	MUST
street			
telephoneNumber			
title			
uid			
userCertificate			
eduPersonAffiliation			

eduPersonEntitlement			
eduPersonNickName			
eduPersonOrgDN			
eduPersonOrgUnitDN			
eduPersonPrimaryAffiliation			
eduPersonPrimaryOrgUnitDN			
eduPersonPrincipalName	X	Kohdat 1.1, 1.2	MUST
eduPersonScopedAddiliation			
eduPersonTargetedID			
schacMotherTongue			
schacGender			
schacDateOfBirth			
schacPlaceOfBirth			
schacCountryOfCitizenship			
schacHomeOrganization	X	Organisaatiotason tieto, muutetaan käsin.	MUST. polamk.fi, pelastusopisto.fi
schacHomeOrganizationType	X	Skeemassa määritelty, muutetaan tarvittaessa.	MUST. 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			
funetEduPersonHomeCity			
funetEduPersonEPPNTimeStamp			

4. Muuta

4.1. Kardinaliteetit

Yksi henkilöllisyys per rooli (esim. opiskelija-työntekijällä kaksi käyttäjätunnusta)?

Yksi käyttäjätunnus / rooli. Roolit ovat opiskelija ja henkilökunta. Yhdellä henkilöllä on 1-2 kpl käyttäjätunnusta.

4.2. EduPersonPrincipalNamen revokointi ja kierrätys

Voiko eduPersonPrincipalName vaihtua?

Ei voi vaihtua.

Millä tavalla organisaatio kierrättää vapautuneita eduPersonPrincipalName-arvoja?

Varoaika vapautuneille arvoille on kaksi vuotta.