



Kansallisen audiovisuaalisen instituutin käyttäjähallinnon kuvaus

Versio	Tekijä	Päiväys
1.0	ToLe	16.12.2015

1. Käyttäjätietokannan ja perusrekistereiden kytkentä

1.2. Henkilökuntarekisteri

LDAP-hakemiston tietoja ylläpidetään käyttäjätietokannan avulla Active Directoryssa ja päivitykset tehdään reaaliaikaisesti käyttäjätietojen muututtua. LDAPista haetaan Identity Provider-palvelimelle vain ne tunnukset, jotka ovat Haka-infrastruktuurin palvelusopimuksen mukaisia loppukäyttäjä, eli Kansalliseen audiovisuaaliseen instituuttiin (KAVI) työ-, virka- tai palvelussopimuksella palkatut henkilöt. Samat tunnukset toimivat myös VIRTU-tunnuksina. Virtu-käyttäjätunnistusjärjestelmä on Valtion tieto- ja viestintätekniikkakeskus Valtorin virastoille tarjoama palvelu. Identity Provider – palvelinta ylläpitää KAVI:lle Fujitsu Services ja se käyttää suoraan KAVI:n Active Directoryn henkilörekisteriä.

1.2.1. Uusi työntekijä

Uuden työntekijän tunnuspyynnöt tehdään esimiehen pyynnöstä tai henkilöstöhallinnon pyynnöstä IT-hallinnon kautta. Tällöin tieto päättyy myös käyttäjätietokantaan.

Tunnistaminen seuraavilla asiakirjoilla: henkilötodistus, passi tai ajokortti.

Uuden työntekijän tiedot siirtyvät LDAP-käyttäjätietokantaan, kun hänelle myönnetään esimiehen Tai henkilöstöhallinnon pyynnöstä ja IT-hallinnon toimesta lähiverkkotunnus.

Uusi työntekijä saa tunnuksen Kansallisen audiovisuaalisen instituutin mikroverkosta työsuhteen alkamisen jälkeen ilman turhia viivytyksiä siitä kun tunnuspyyntö on vastaanotettu.

1.2.2. Työntekijän tiedoissa tapahtuu muutos

Muutostapauksessa esimies tekee pyynnön muuttuneiden tietojen päivittämisestä. LDAP:ssä tehdään tällaisessa tapauksessa tunnuksen disablointi. Jos työntekijän etu- tai sukunimi vaihtuu, hänelle luodaan uusi lähiverkkotunnus, joka päivittyy välittömästi LDAP-tietovarantoon. Henkilön eduPersonPrincipalName muuttuu tuolloin vastaamaan henkilön uutta etu ja/tai sukunimeä.

Jos organisaatioon tulee myöhemmin henkilö jolla on sama nimi kuin aiemmin lopettaneella, hänelle ei anneta sellaista eduPersonPrincipalName-arvo joka on ollut aiemmin käytössä.

Esim.: "Matti Virtanen" ei saa eduPersonPrincipalName-arvokseen *matti.virtanen@kavi.fi*, vaan *matti.t.virtanen@kavi.fi* (jossa t on toisen ristimänimen 1.kirjain)



1.2.3. Työntekijä lakkaa olemasta työntekijä

Esimiehen tekemä tai henkilöstöhallinnon tekemä pyyntö tunnusten poistamisesta ja syy poistoon, joka tehdään ennen työsuhteen päättymistä. Tunnukset poistetaan työsuhteen päättymispäivänä.

1.3. Muut käyttäjät ja heidän henkilötietojensa ajantasaisuus

Muita käyttäjiä kuin virka- tai työsuhteessa olevia ovat siviilipalvelusmiehet, työharjoittelijat ja muu tilapäinen henkilökunta. Heidän tunnuksensa pyytää heidän esimiehensä, muuten heidän tehtävistään vastuullinen henkilö tai henkilöstöhallinto IT-hallinnolta. Käyttöoikeudet rajataan Active Directoryyn niin, että heillä ei ole oikeutta HAKA- tai VIRTU-tunnistautumiseen Identity Provider -palvelinten kautta. Käyttäjätietojen ajantasaisuudesta vastaa heidän esimiehensä tai heidän tehtävistään vastaava henkilö.

2. Henkilöllisyyden todentaminen

2.1. Käyttäjätunnuksen antamisen yhteydessä

Tunnistaminen seuraavilla asiakirjoilla: henkilötodistus, passi tai ajokortti. Esimies suorittaa todennuksen.

2.2. Kun käyttäjä kirjautuu käyttäjätunnuksensa avulla

Salasanatodennukseen liittyvät laatuvaatimukset:

- Salasanassa pitää olla vähintään 8 merkkiä.
- Salasana ei saa sisältää käyttäjätunnuksiasi eikä siinä saa olla tilin täydellisestä nimestä yli kahta perättäistä kirjainta (= Sukunimi Etunimi).
- Uudessa salasanassa pitää lisäksi olla vähintään kolme seuraavista neljästä kategoriosta: iso kirjain ja/tai pieni kirjain ja/tai numero ja/tai erikoismerkki.
- Salasanakierto on 5 edellistä salasanaa (eli muistetaan 5 viimeksi käytettyä salasanaa eikä näitä muistissa olevia salasanoja voida käyttää).
- Salasanan maksimivaihtoväli on 120 vuorokautta ja minimissään salasana on voimassa yhden vuorokauden.

Mahdolliset käytettävissä olevat salasanaa tukevat autentikointimenetelmät.

3. Käyttäjätietokannassa saatavilla olevat tiedot

Attribuutti	Saatavuus	Miten ajantasaisuus turvataan	Muuta (esim. tulkintaohje)
cn / commonName	Kyllä		MUST
description			
displayName	Kyllä		MUST
employeeNumber			
facsimileTelephoneNumber			



givenName	Kyllä		
homePhone			
homePostalAddress			
jpegPhoto			
l / localityName			
labeledURI			
mail	Kyllä		
mobile			
o / organizationName			
ou / organizationalUnitName	Kyllä		
postalAddress			
postalCode			
preferredLanguage			
seeAlso			
sn / surname	Kyllä		MUST
street			
telephoneNumber	Kyllä		
title			
uid			
userCertificate			
eduPersonAffiliation			Mitä arvoja on saatavilla?
eduPersonEntitlement			
eduPersonNickName			
eduPersonOrgDN			
eduPersonOrgUnitDN			
eduPersonPrimaryAffiliation			
eduPersonPrimaryOrgUnitDN			
eduPersonPrincipalName	Kyllä		MUST
eduPersonScopedAddiliation			
eduPersonTargetedID			
schacMotherTongue			
schacGender			
schacDateOfBirth			
schacPlaceOfBirth			
schacCountryOfCitizenship			
schacHomeOrganization	Kyllä	staattinen, idP:n kautta	MUST. Mikä arvo on käytössä?



schacHomeOrganizationType	Kyllä	staattinen, idP:n kautta	MUST Mikä arvo on käytössä?
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?
funetEduPersonHomeCity			
funetEduPersonEPPNTimeStamp			

4. Muuta

4.1. Kardinaliteetit



Yksi henkilöllisyys per tosielämän käyttäjä.

4.2. EduPersonPrincipalNamen revokointi ja kierrätys

EduPersonPrincipalName voi vaihtua, jos henkilön sukunimi vaihtuu.

Millä tavalla organisaatio kierrättää vapautuneita eduPersonPrincipalName-arvoja? Ei kierrätä.