Kotiorganisaation käyttäjähallinnon kuvaus – Kotus

Versio	Tekijä	Päiväys
1.0	Tarmo Rahikainen	1.6.2018

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

Kotimaisten kielten keskuksen (Kotus) käyttäjätietokannan tekninen toteutus on Valtorin Valtti-päätelaitepalvelun Microsoft Active Directory (AD), josta Valtorin Virtu Identity Provider -palvelin noutaa useimmat attribuutit. Käyttäjän perustietoja saadaan käyttäjätietokantaan valtionhallinnon yhteisestä Kieku-järjestelmästä ja Valtorin TOP-palvelupyyntöjärjestelmästä, mutta toistaiseksi automaattista kytkentää ei ole.

Kieku-tiedonsiirtoon Valtorissa on parhaillaan menossa Avain-palveluun perustuva automatiikka, joka synkronoi Kiekun tietoja AD:n tietoihin. Tämän toiminnallisuuden pitäisi tulla käyttöön vuoden 2018 loppuun mennessä.

1.1. Henkilökuntarekisteri

Suoraa yhteyttä henkilöstöhallinnon järjestelmiin ei toistaiseksi ole.

1.1.1. Uusi työntekijä

Esimies täyttää ja lähettää Kotuksen intranetissa olevan uutta työntekijää koskevan sähköisen käyttölupalomakkeen Kotuksen tietohallinnolle. Lomakkeen käyttö vaatii kirjautumisen, jolla esimies tunnistetaan. Kotuksen tietohallinnon työntekijä täyttää Valtorin TOP-palvelupyyntöjärjestelmässä esimiehen lomakkeella antamilla tiedoilla ja joillakin lisätiedoilla käyttäjätunnushakemuksen ja pyytää tarvittavat käyttöoikeudet uudelle työntekijälle.

Valtorin käyttövaltuushallinto luo käyttäjätunnuksen uudelle työntekijälle ja antaa tarvittavat käyttöoikeudet. Käyttäjätunnus ja salasana lähetetään työntekijän esimiehelle erillisillä turvaposteilla.

1.1.2. Työntekijän tiedoissa tapahtuu muutos

Työntekijä tekee Valtorin TOP-palvelupyyntöjärjestelmässä muutosta koskevan pyynnön, joka lähetetään työntekijän esimiehelle hyväksyttäväksi.

1.1.3. Työntekijä lakkaa olemasta työntekijä

Toistaiseksi voimassa olevan työsuhteen päättyessä työntekijän esimies täyttää Valtorin TOP-palvelupyyntöjärjestelmässä henkilön lähtölomakkeen, jonka käsittelyn myötä työntekijän käyttäjätunnus jäädytetään ja käyttöoikeudet poistetaan. Määräaikaisen työntekijän käyttäjätunnus jäädytetään käyttölupahakemuksessa kerrottuna käyttöluvan päättymispäivänä.

1.2. Muut käyttäjät ja heidän henkilötietojensa ajantasaisuus

Siviilipalvelusmiesten, palkkiopohjaisten työntekijöiden ja palkattomien harjoittelijoiden kohdalla toimitaan samoin kuin työntekijöidenkin, eli esimies hyväksyy lupahakemuksen ja muutokset. Käyttölupahakemukseen merkitään käyttöluvan päättymispäivä.

2. Henkilöllisyyden todentaminen

2.1. Käyttäjätunnuksen antamisen yhteydessä

Työntekijän henkilöllisyys todennetaan virallisesta henkilötodistuksesta tai ajokortista. Käyttäjätunnuksen luovuttaa työntekijälle hänen esimiehensä.

2.2. Kun käyttäjä kirjautuu käyttäjätunnuksensa avulla

Peruskäyttöoikeuden haltija kirjautuu järjestelmiin käyttämällä käyttäjätunnusta ja salasanaa tai Väestörekisterikeskuksen varmentamaan Kotuksen organisaatiokortilla olevaa varmennetta ja henkilökohtaista tunnuslukua (PIN). Käyttäjätunnus ja salasana sekä organisaatiokortti ja PIN-tunnusluvut ovat henkilökohtaisia, eikä niitä saa luovuttaa toisen henkilön käyttöön. Käyttäjätunnuksella ja salasanalla tai organisaatiovarmenteella avattua istuntoa tai yhteyttä ei saa luovuttaa toisen henkilön käyttöön. Salasana tulee vaihtaa vähintään 90 päivän välein. Salasanan tulee noudattaa seuraavaa muotoa:

- Merkkejä on oltava vähintään 10 kpl.
- Sisällettävä isoja sekä pieniä kirjaimia.
- Sisällettävä numeroita ja/tai erikoismerkkejä.
- Salasana ei saa olla sama, kuin käyttämäsi viimeisimmät 12 salasanaa.

3. Käyttäjätietokannassa saatavilla olevat tiedot

Alla olevassa taulukossa näkyvät attribuutit, jotka näkyvät ulospäin Valtorin Virtu Identity Provider -palvelimesta (displayName ei näy ulospäin Virtu-palvelimesta, saadaan suoraan AD:sta). Virtu IdP -palvelin noutaa useimmat attribuutit AD-käyttäjätietokannasta.

Attribuutti	**Miten ajantasaisuus turvataan**	**Muuta (esim. tulkintaohje)**
cn / commonName	ks. kohta 1.1.	Kutsumanimi Sukunimi (AD:n cn-attribuutti)
displayName	ks. kohta 1.1.	Kutsumanimi Sukunimi (AD:n displayName-attribuutti)

givenName	ks. kohta 1.1.	Kutsumanimi (AD:n givenName-attribuutti)
mail	ks. kohta 1.1.	Sähköpostiosoite (AD:n mail-attribuutti)
sn / surname	ks. kohta 1.1.	Sukunimi (AD:n sn-attribuutti)
eduPersonPrincipalName	ks. kohta 1.1. ja 4.2.	tunnus@kotus.fi (muodostetaan Virtu-skeeman attribuuttien virtuLocalID [AD:n samaccountname] ja virtuHomeOrganizationType avulla)
schacHomeOrganization	vakio	kotus.fi (Virtu-skeeman virtuHomeOrganization-attribuutti)
schacHomeOrganizationType	vakio	other

4. Muuta

4.1. Kardinaliteetit

Yhtä käyttäjätunnusta vastaa yksi tosielämän käyttäjä.

4.2. EduPersonPrincipalNamen revokointi ja kierrätys

Kotuksen työntekijän käyttäjätunnus (Kieku-numero) on yksilöllinen ja pysyvä eikä sitä vaihdeta, joten myös eduPersonPrincipalName on pysyvä.

Kerran annettua käyttäjätunnusta eikä siten myöskään eduPersonPrincipalName-arvoa kierrätetä toiseen käyttöön.