Käyttäjähallinnon kuvaus

Metropolia Ammattikorkeakoulun käyttäjähallinnon kuvaus

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. Perusrekisteri

Lähtöoletuksena on, että Perusrekisterin henkilötiedot ovat ajan tasalla.

Miten käyttäjätietokanta on kytketty Perusrekisteriin?

Perusrekisteri on relaatiotietokanta, joka on kytketty käyttäjätietokantaan reaaliaikaisesti triggereiden käynnistäessä tietojen synkronoinnin.

1.1.1. Uusi opiskelija

Miten uuden opiskelijan tiedot päivittyvät Perusrekisteristä käyttäjätietokantaan?

Uuden opiskelijan tiedot päivittyvät käyttäjätietokantaan reaaliaikaisesti. Käyttäjälle muodostetaan näiden tietojen perusteella automaattisesti käyttäjätunnus. Jos henkilöllä on jo käyttäjätunnus, uutta tunnusta ei luoda.

Koska uusi opiskelija saa käyttäjätunnuksen/opiskelijaroolin?

Uusi opiskelija saa käyttäjätunnuksen otettuaan opiskelupaikan vastaan ja opiskelijaroolin ilmoittauduttuaan läsnäolevaksi.

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

Tunnusta ei luoda mikäli opiskelupaikkaa ei oteta vastaan. Poissaolevaksi ilmoittautuvan opiskelijan tunnus pysyy toiminnassa.

1.1.2. Opiskelijan tiedoissa tapahtuu muutos

Miten opiskelijan muuttuneet tiedot päivittyvät Perusrekisteristä käyttäjätietokantaan?

Opiskelijan muuttuneet tiedot päivittyvät käyttäjätietokantaan reaaliaikaisesti.

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?

a) valmistuminen merkitään opintorekisteriin valmistumiskokouksen jälkeen
b) n. 2kk syyslukukauden alkamisen jälkeen
c) opintojen keskeyttäminen merkitään opintorekisteriin heti kun asia on käsitelty

Kirjautuminen Haka-infrastruktuurin palveluihin estyy välittömästi näiden merkintöjen teon jälkeen.

1.2. Henkilökuntarekisteri

Henkilörekisteri on HR-järjestelmän relaatiotietokanta, joka on kytketty käyttäjätietokantaan lyhyin väliajoin pollattavan, viimeiset muutokset näyttävän näkymän kautta.

1.2.1. Uusi työntekijä

Uuden työntekijän tiedot päivittyvät käyttäjätietokantaan lähes reaaliaikaisesti. Käyttäjälle muodostetaan näiden tietojen perusteella automaattisesti käyttäjätunnus. Jos henkilöllä on jo käyttäjätunnus, uutta tunnusta ei luoda.

1.2.2. Työntekijän tiedoissa tapahtuu muutos

Työntekijän muuttuneet tiedot päivittyvät käyttäjätietokantaan lähes reaaliaikaisesti.

1.2.3. Työntekijä lakkaa olemasta työntekijä

Työntekijä lakkaa olemasta työntekijä, kun hänellä ei ole voimassaolevaa työ- tai virkasuhdetta. Tällöin myös oikeus käyttäjätunnukseen päättyy tämän roolin perusteella ja kirjautuminen Haka-infrastruktuurin palveluihin estyy välittömästi.

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.

Ainoastaan Metropolian opiskelijat ja henkilökunta voivat kirjautua Haka-infrastruktuurin palveluihin.

2. Henkilöllisyyden todentaminen

2.1. Käyttäjätunnuksen antamisen yhteydessä

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

Käyttäjätunnuksen saa tunnistautumalla pankkitunnusten tai mobiilivarmenteen avulla osoitteessa http://salasana.metropolia.fi

Sekä opiskelija, että työntekijä (jolla ei ole suomalaisia pankkitunnuksia) voi saada aktivointiin tarvittavat tunnus- ja aktivointitiedot muilla tavoin (ohje)

2.2. Kun käyttäjä kirjautuu käyttäjätunnuksensa avulla

Salasanatodennukseen liittyvät laatuvaatimukset. Mahdolliset käytettävissä olevat salasanaa tukevammat autentikointimenetelmät.

Salasanan minimipituus on 8 merkkiä.

3. Käyttäjätietokannassa saatavilla olevat tiedot

3. Käyttäjätietokannasta luovutettavat tiedot
Attribuuttitestipalvelu: https://rr.funet.fi/attribute-test/
Palvelussa voi tarkistaa mitä tietoja Metropolian IdP-palvelin omalta käyttäjätunnukselta luovuttaa.

4. Muuta

4.1. Kardinaliteetit

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

Yksi henkilöllisyys per tosielämän käyttäjä.

4.2. EduPersonPrincipalNamen revokointi ja kierrätys

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

Käyttäjätunnus ja eduPersonPrincipalname vaihdetaan vain erittäin painavasta syystä.

Vapautuneet eduPersonPrincipalname:t pidetään varattuna vähintään kaksi vuotta.