

Haka-käyttäjätunnistuksen määrittäminen kilpailutuksessa

This document in english: [Request for tender templates](#)

Tällä sivulla esitetään mallilausekkeita Haka-käyttäjätunnistuksen määrittämiseksi. Annettuja esimerkkivaatimuksia voi soveltaen käyttää osana kilpailutusta. Esimerkeissä annetaan myös toisilleen vaihtoehtoisia vaatimuksia, joiden käyttö on arvioitava tapauskohtaisesti. Tarkkoja ohjeita kaikkiin tilanteisiin on mahdoton laatia tuntematta kulloistakin sovellusta.

Tekninen rajapinta käyttäjätunnistusta varten

Hakan hyödyntäminen edellyttää tiettyjä ominaisuuksia tukevan ohjelmistokomponentin. Yleistasolla puhutaan SAML2-protokollaan tukevasta ohjelmistosta. Hakalla on omat tarkennetut määrittäykset SAML2-protokollasta, joiden noudattaminen on edellytyksenä Haka-yhteensopivuudelle.

 Käyttäjien tunnistaminen tulee tapahtua Haka-luottamusverkoston ([Haka-käyttäjätunnistusjärjestelmä](#)) avulla. Hankittavaan järjestelmään tulee sisältyä Hakan käyttöä varten SAML 2.0-protokollan ja Haka-määrittysten ([SAML-profiili](#)) mukainen SAML Service Provider.

Mikäli kaikilla järjestelmän käyttäjillä ei ole Haka-tunnistus käytössään, voidaan rinnalla tarjota perinteinen käyttäjätunnukseen ja salasanaan perustuva käyttäjätunnistus.

 Järjestelmään tulee voida kirjautua myös suoraan ilman Haka-kirjautumista. Ominaisuuden tulee olla käytettävissä samanaikaisesti Haka-kirjautumisen rinnalla.

Hakasta saatavien käyttäjätietojen hyödyntäminen

Haka-käyttäjätunnistuksen yhteydessä voidaan käyttäjästä siirtää käyttäjätietoja. Tällaisia tietoja voivat olla mm. henkilön nimi ja sähköpostiosoite tai rooli organisaatiossa. Tarkat tiedot hyödynnettävistä käyttäjätiedoista eli attribuuteista löytyy: [funetEduPerson-skeema](#).

Käyttäjätietojen hyödyntäminen ja käyttäjien liittäminen sovelluksen käyttäjätileihin tai rooleihin tulee tarkastella aina tapauskohtaisesti sovelluksen teknisten mahdollisuuksien ja paikallisten käytäntöjen valossa.

 Käyttäjien oikeuksien asettamisessa sekä käyttäjätietojen ylläpidossa tulee hyödyntää Haka-käyttäjätunnistuksen yhteydessä saatavia attribuutteja.

Käyttäjälle muodostuu Haka-tunnistuksessa käyttäjäkohtainen tunniste, joka voidaan usein liittää sovelluksessa olemassa oleviin käyttäjätileihin. Yleisimmin tunnisteena käytetään eduPersonPrincipalName-attribuuttia.

 Käyttäjän Haka-tunniste tulee liittää sovelluksessa olemassa oleviin käyttäjätileihin.

Pääsynvalvonta

Sovelluksen pääsynvalvontaa voidaan suorittaa sovelluksissa asetettavilla oikeuksilla tai hyödyntää Hakasta saatavia tietoja.

 Sovellukseen tulee sallia pääsy vain nimettyjen Haka-tunnistuslähteiden käyttäjiltä.

 Sovelluksen pääsynvalvonta tulee perustua Hakan attribuutteihin.

 Sovelluksen käyttöroolit tulee saada Hakan käyttäjäattribuuteista.

Tunnistuslähteen päättely

Hakassa on kullakin organisaatiolla oma tunnistuslähte. Palvelun tulee ohjata käyttäjä tunnistautumaan käyttämäänsä tunnistuslähteeseensä.

Palvelussa on tehtävä valinta toteutetaanko tunnistuslähteen valinta palvelussa esim. valintalistana tai käyttäen herätteenä osoitetta, johon käyttäjä saapuu vai käytetäänkö Hakan keskitettyä päättelypalvelua.

 Tunnistuslähteen valinta tulee suorittaa palvelun käyttöliittymässä.

 Tunnistuslähde määritellään argumenttina palvelun URL:ssa.

 Tunnistuslähteen valintaan käytetään Hakan keskitettyä päättelypalvelua.

 Palvelu ohjaa käyttäjän kirjautumaan tietylle ennalta määritetylle tunnistuslähteelle.

Käyttäjätietojen provisiointi

Sovelluksien käyttäjätilit voidaan luoda ilman käyttäjän toimia Hakaa käytettäessä tai muilla kirjautumismenetelmillä. Sovelluksen käyttäjätili tulee liittää käyttäjän Haka-tunnisteeseen.

 Käyttäjätilit luodaan hallintaliittymän kautta käyttäjien Haka-tunnisteisiin perustuen. Käyttäjän kirjautuessa ensimmäistä kertaa käyttäjätiliin ollessa olemassa, sallitaan käyttäjälle sovelluksen käyttö.

Sovelluksen käyttäjätili voidaan muodostaa myös automaattisesti käyttäjän kirjautuessa ensimmäistä kertaa Hakan avulla sovellukseen. Tämän jälkeen käyttäjään voidaan kohdistaa käyttöoikeuksien muokkaamista, mikäli Hakan tarjoamat käyttäjätiedot eivät riitä oikean käyttäjäroolin asettamiseen.

 Käyttäjätili muodostuu käyttäjän kirjautuessa ensimmäistä kertaa sovellukseen Hakan avulla.

 Käyttäjätileihin voidaan asettaa lisäoikeuksia hallintaliittymän kautta.