

Vahvemman tunnistamisen sanasto

Hakan tekninen ryhmä hyväksyi monivaiheiseen tunnistamisen tukemiseen REFEDS:in määrittämän sanaston. Sanaston avulla mahdollistetaan erilaisten tunnistusvälineiden, erityisesti monivaiheisen tunnistaminen, tehokkaampi ja helpompi käyttö Haka-palveluissa.

Sanastoa voidaan käyttää mm. seuraavissa käyttötapauksissa:

- Palvelu (SP) pyytää tiettyä tunnistusvälinettä tiettyyn tunnistustapahtumaan ja tunnistuspalvelimen (IdP) on tätä pyyntöä kunnioitettava
- Tunnistuspalvelin ilmoittaa millä tavalla käyttäjä on tunnistettu vaikka palvelu ei olisi mitään tiettyä pyytänyt

Uudet tunnistusmenelmät

- <https://refeds.org/profile/sfa>
- <https://refeds.org/profile/mfa>

Toimenpiteet

Tunnistuspalvelimet

Tunnistuspalvelimen ylläpitäjien tulee lisätä tukemansa REFEDS-sanasto osaksi oman tunnistuspalvelimensa tukemia tunnistusmenetelmiä mikäli tuki niille tunnistuspalvelimesta löytyy. Jokaisen tunnistuspalvelimen tulee vertailla omaa käytäntöään REFEDS-menetelmiin ja aktivoida ne, jotka tosiasiallisesti ovat tunnistuspalvelimessa tuettuja.

1. Vertaa oman ympäristösi käytäntöjä <https://refeds.org/profile/sfa> ja <https://refeds.org/profile/mfa> määrittämiin.
2. Aktivoi ne, jotka vastaavat ympäristöäsi
 - a. Mikäli tunnistuspalvelin tukee monivaiheista tunnistamista REFEDS-määritysten mukaisesti, aktivoi mfa-arvo.
 - b. Jos salasanan tunnistaminen noudattaa REFEDS-määrittämissä asetettuja ehtoja, aktivoi sfa-arvo

Tarvittaessa kysy lisätietoja haka@csc.fi

Palvelut

Mikäli palvelu tarvitsee jotain tiettyä tunnistusmenetelmää, tulee se ilmaista osana tunnistuspyyntöä AuthenticationContextClass -arvolla. Jos millekään tietylle menetelmälle ei ole tarvetta, ei tule pyytää mitään vaan antaa tunnistuspalvelimen suorittaa tunnistaminen haluamallaan tavalla Hakan yleisten vaatimusten puitteissa.

Tulee myös huomioida, että SAML2-määritysten mukaisesti tunnistuspalvelin palauttaa virheen, mikäli tunnistuspalvelin ei kykene täyttämään pyydettyä tunnistusvälinettä.