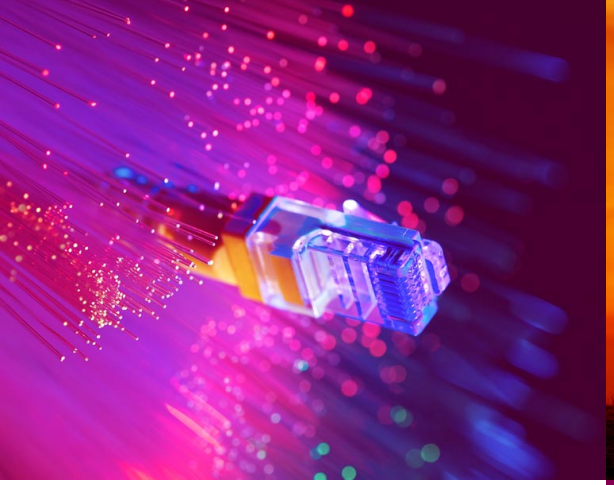


Haka MFA-työpaja
20.1.2016

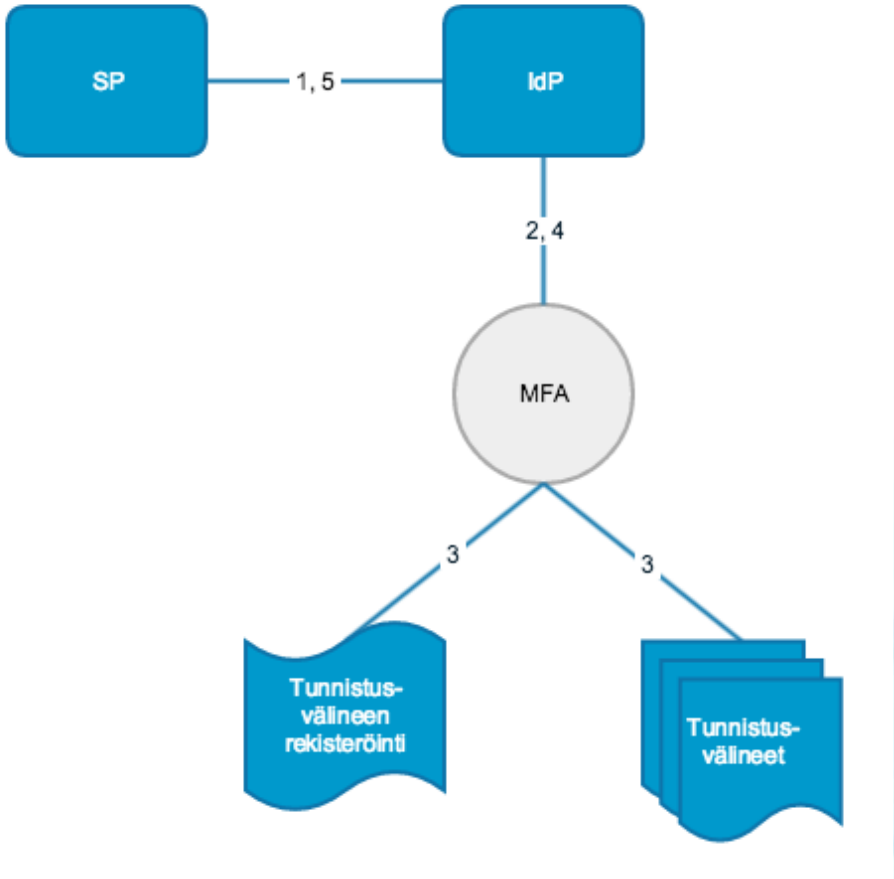
IdP

CSC – Suomalainen tutkimuksen, koulutuksen, kulttuurin ja julkishallinnon ICT-osaamiskeskus

Käyttötapaus

- Organisaatio haluaa vahvistaa osan tai kaikki tunnistustapahtumista vahvemmalla tunnistuksella
- Palveluiden ei tarvitse tehdä mitään muutoksia

Viestien vaihto



1. Autentikointipyyntö SAML2
2. Tunnistuspyyntö OpenID Connect
3. Tunnistaminen (+ rekisteröinti)
4. Tunnistusvastaus OpenID Connect
5. Tunnistusvastaus SAML2

Toiminta

- SP pyytää vahvempaa tunnistamista samalla tavalla kuin suorassa MFA-käyttötapauksessa
  - IdP ohjaa pyynnöt käyttäjätunnistuksen jälkeen MFA:lle hakemaan vahvistusta
- On kaavailtu myös konfigurointioptiota pakottaa tietty käyttäjäryhmä vahvempaan tunnistukseen ilman palvelulta tulevaa pyyntöä
  - Esim. Role = staff

IdP:n vaatimukset

- IdP:n tulee toimia OpenID Connect Relying Party roolissa
- Käytöstä sovitaan IdP:n ja MFA:n kahdenvälisellä sopimuksella
  - Haka-sopimus ei aiheuta rajoitteita käytölle

Miksi OpenID Connect IdP:n ja MFA:n välissä

- OpenID Connect on tunnettu standardi tunnistamisessa
  - Käytetään olemassa olevaa
  - Tunnettu protokolla, joten oletuksena ei aiheuta epäilyksiä
  - Kyseessä one-to-one luottosuhde, joten epäilyt OIDC:n skaalautumisesta eivät päde
- MFA:lle muodostuu OIDC-rajapinta
  - MFA voi tarjota jatkossa uudenlaisia palveluita, kuten mahdollistaa OIDC-protokollaa tukevien palveluiden liittäämisen Hakaan ilman muutoksia tunnistuspalveluihin
- Kyseinen protokolla tuettu MPASS-ratkaisussa, johon Haka MFA toteutus perustuu

MFA:n käyttöönotto

- Asennetaan tarvittavat lisäkomponentit IdP:lle
  - CSC:n kehittämiä avoimen lähdekoodin komponentit
- Muodostetaan luottosuhde IdP:n ja MFA:n välille käyttäen OpenID Connect –protokollaa
- Konfiguroidaan IdP suorittamaan vahvempi tunnistus

Tehtäviä työpajaan

1. Asennetaan vaadittavat komponentit IdP:lle
2. Konfiguroidaan uusi tunnistusmenetelmä IdP:lle
3. Testataan toimintaa eri tunnistusmenetelmillä