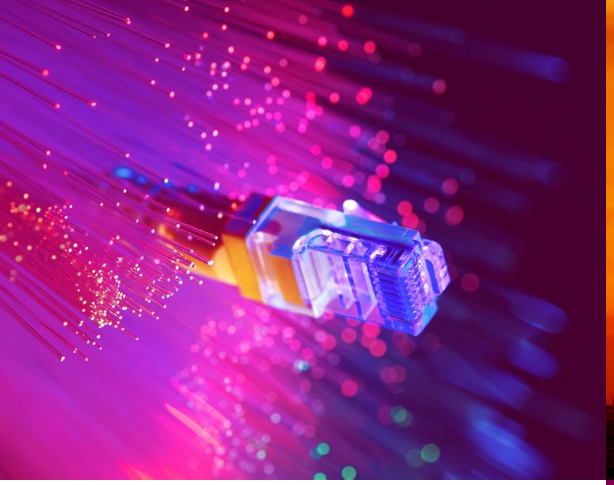


Haka MFA-työpaja 20.1.2016

Yleisesittely ja SP-konfigurointi

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

Tilaisuuden tarkoitus

- Esitellään ensimmäinen versio Haka MFA:sta
- Näytetään esimerkkiasennukset niin SP:lle kuin IdP:lle
- Keskustellaan MFA:n ominaisuuksista
- Otetaan vastaan kommentteja, kritiikkiä, toiveita ja ennen kaikkea ilmoittautumisia pilottitestaukseen

Valmistelut

- Kokonaisuuden käyttötapaukset
  - https://wiki.eduuni.fi/pages/viewpage.action?pageId=29753927
- Tarkastetaan valmistelut
  - https://wiki.eduuni.fi/display/CSCHAKA/Esitiedot
- SP-osio ohjeet
  - https://wiki.eduuni.fi/display/CSCHAKA/SP+konfigurointi
- IdP-osion ohjeet
  - https://wiki.eduuni.fi/display/CSCHAKA/IdP+konfigurointi

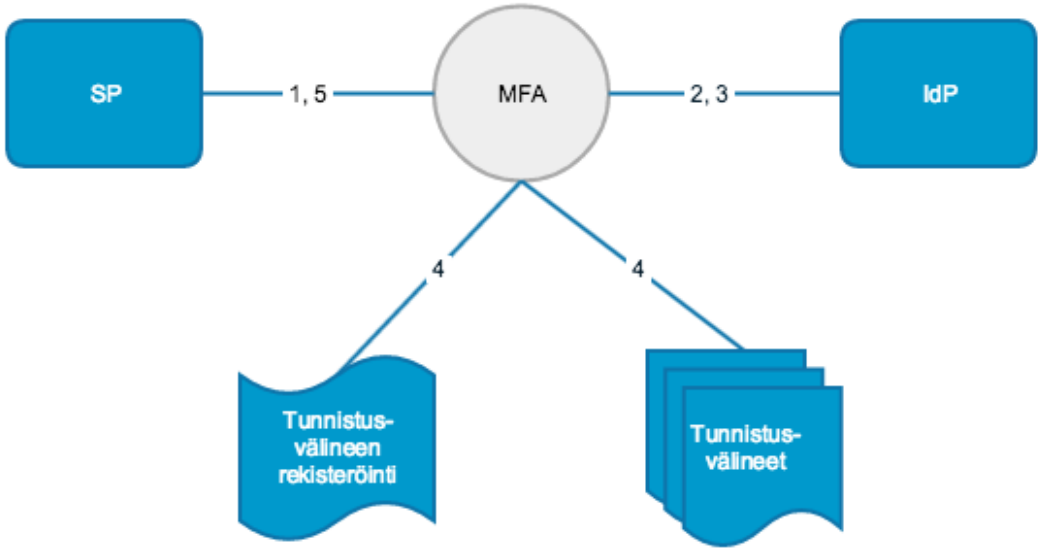
Service Provider käyttöönotot Haka MFA:n kanssa

1. Käyttötapauksen läpikäynti
2. Service Providerissa tehtävät toimenpiteet
   a. Luottosuhteen muodostaminen
   b. Tunnistusvälineen pyytäminen
3. Kokonaisuuden testaaminen

Käyttötapaus

- Palvelun omistaja kaipaa vahvempaa tunnistusta
- Tehdään riippumatta käyttäjien organisaatiosta
  - Käyttäjät voivat olla eri organisaatioista
- Käyttäjä vastaa tunnistusvälineestään
- Haka yhteensopiva eli SP:n ei tarvitse tehdä suuria muutoksia palveluunsa

Viestit



1. Autentikointipyyntö
2. Autentikointipyyntö
3. Tunnistusvastaus
4. Vahvempi tunnistus (+ rekisteröinti tarvittaessa
5. Tunnistusvastaus

Luottosuhteen muodostaminen

- Haka MFA on SP:lle kuten mikä tahansa muukin IdP
  - Tavoitteena, että MFA on aikanaan Haka-metadatassa kuten muutkin IdP:t
  - Pilotointi hoidetaan kahdenvälisillä sopimuksilla
  - Nykyisen Haka-sopimuksen mukaan Haka-jäsen saa tuodan yhden IdP:n Hakaan
- MFA noudattaa Hakan SAML2-profiilia
  - Autentikointimenetelmän pyytäminen poikkeaa totutusta Hakasta
  - Attribuuttien käsittelyssä tarkennuksia esim. eppn:n osalta

Tunnistusmenetelmän pyytäminen

- SAML2 SP voi pyytää tiettyä tunnistusmenetelmää autentikointipyynnössään
- Tunnistusmenetelmä esitetään RequestedAuthnContext –elementin sisällä
- SAML2 määrityksissä suuri joukko valmiita arvoja, mutta myös omia voi käyttää
  - MFA:lle määritellään oma(t) arvonsa
  - Jos MFA:lta ei pyydetä tunnistusmenetelmänä, se ei suorita vahvennusta
- MFA:n tunnistusmenetelmät käytössä vain jos tunnistukset ohjataan MFA:lle
  - MFA huolehtii DS-palveluun ohjaamisesta

Tunnistusmenetelmän pyyntöviesti

```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
                    AssertionConsumerServiceURL="https://testsp.funet.fi/Shibboleth.sso/SAML2/POST"
                    Destination="https://mfapilot.funet.fi/idp/profile/SAML2/Redirect/SSO"
                    ID="_08bb7179aee50d79337729824b3110d1"
                    IssueInstant="2017-01-05T11:20:39Z"
                    ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
                    Version="2.0"
                    >
    <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://testsp.funet.fi/shibboleth</saml:Issuer>
    <samlp:NameIDPolicy AllowCreate="1" />
    <samlp:RequestedAuthnContext>
        <saml:AuthnContextClassRef xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">urn:test:stepup</saml:AuthnContextClassRef>
    </samlp:RequestedAuthnContext>
</samlp:AuthnRequest>
```

Tunnistusmenetelmän pyytäminen

- IdP palauttaa käytetyn tunnistusmenetelmästä tiedon tunnistusvastauksessa
  - Jos mitään ei ole pyydetty, tarjoaa IdP jotain tunnistusmenetelmää käyttäjälle
  - Pyynnöllä, IdP tekee pyydetyn tunnistuksen ja palauttaa vastauksessa tiedon käytetystä menetelmästä

```
<saml2:AuthnContext>
    <saml2:AuthnContextClassRef>urn:test:stepup</saml2:AuthnContextClassRef>
</saml2:AuthnContext>
```

Tehtäviä työpajaan

1. Muodostetaan SP:lta luottosuhden MFA:lle
2. Pyydetään vahvempaa tunnistusmenetelmää
3. Käyttöliittymän sopeuttaminen haluttuun toimintaan
4. Tarkastetaan viestien liikkuminen ja sisältö

Tunnetut puutteet

- MFA ei vielä noudata kaikkia SAML2 IdP Proxy toiminnallisuuden vaatimuksia
  - Esim. eppn-scope asia vielä kesken
- Ulkoasu on kehityksen alla
- Tunnistusvälineinä vain TOTP
- Viilausta siellä, täällä ja tuolla

Promiseware

- MFA voisi toimia
  - Protokollamuuntimena Hakaan: OpenID Connect –palvelut voisivat tulla Hakaan
  - Proxyna palveluille, jotka tukevat vain yhtä IdP:ia
  - Keskitettynä suomi.fi tunnistuksen rajapintana Hakaan
    - Suomi.fi tunnistus + Hakasta käyttäjäattribuutit
    - Pelkkä suomi.fi -rajapinta
  - IdP:na organisaatiolle hakemiston liittämisellä MFA:iin

Seuraavaksi

- Koulutuksessa käytettävä mfapilot.funet.fi julkaistaan vapaaseen käyttöön lähitulevaisuudessa
- Aloitetaan tuotannon valmistelut
  - Tarkka aikataulu riippuu ensimmäisistä liittyjistä (haluttu käyttötapaus, tunnistusväline jne.)