CSC

ICT Solutions for Brilliant Minds

IdP4 Webinaari 6.5.2020

Shibboleth IdP4 Webinaari 6.5.2020

- Katsaus ajankohtaisiin asioihin, joita IdP4 julkaisu tarkoittaa Haka-ylläpitäjille
- Kohdeyleisönä IdP-ylläpitäjät, joilla aiempi Shibboleth IdP3 asennus olemassa
- Tilaisuuden tarkoitus toimia herätteenä:
  - Minun ehkä pitää jotain tehdä tänä vuonna

Käytännön järjestelyt

- Kysyä voi missä vaiheessa vain
  - Räpylä ylös Zoomissa
  - Viesti chat-ikkunaan
- Mikrofonit kiinni paitsi puhuessa
- Aikaa varattu 13-15.
  - Lopetamme, kun valmista

Aikataulu

- Shibboleth IdP4 julkaistiin 11.3.2020
- Shibboleth IdP3 tuki loppuu 31.12.2020
  - Spring 4 EOL 31.12.2020, joten Shibboleth-projektilla ei ole asiassa paljonkaan vaihtoehtoja
- Käytännössä kaikkien Shibboleth IdP käyttäjien tulee päivittää IdP4-tasolle siihen mennessä varmistaakseen mm. turvapäivitysten saatavuuden

Dokumentaatio

- Shibboleth IdP4 oma wiki-sivusto: https://wiki.shibboleth.net/confluence/display/IDP4/Home
- Kun, teet päivitystä/asennusta varmista olevasi oikeassa wikissä. Hakutulokset voivat viedä väärään wikiin.

Dokumentaatio

- Pääasiallinen tukikanava Shibbolethille on edelleen shibboleth-users sähköpostilista
  - https://shibboleth.net/mailman/listinfo/users
- Haka@csc.fi tarjoaa mahdollisuuksien mukaan apuja erityisesti Hakaan liittyvissä asioissa
- CSC ja Haka osana Nordunetiä on Shibboleth-konsortion jäsen, joten CSC:n kautta pystytään lähestymään Shibboleth-kehittäjiä suoraan maksullisen tuen kanavia pitkin

Uudet ominaisuudet

- IdP4 ei kovin paljoa tuo uusia ominaisuuksia, jotka ylläpitäjät huomaavat puhumattakaan käyttäjistä
- Paljon sisäisiä muutoksia IdP:ssa, jotka luovat pohjaa versiolle viisi

Ainakin huomionarvoisia muutoksia

- Alustalle uusia vaatimuksia
- Proxy-tuki
- Oletusasetuksissa joitakin muutoksia
  - XML kryptauksen algoritmit
  - Osa SAML2 ominaisuuksista (joita ei käytössä ainakaan Hakassa ja SAML 1.1 oletuksena pois päältä
  - Logout oletuksena käytössä
- Attribute Registry
- Cross-Site Request Forgery (CSRF) suojausta IdP:lle

Alusta

- IdP4 vaatii Java 11 ja Jetty 9.4 on suositeltu
- https://wiki.shibboleth.net/confluence/display/IDP4/SystemRequirements

Päivitys

- Voidaan päivittää uusimman 3.4.6 päälle
- Alla tulee olla sopiva IdP4 vaatimusten mukainen sovelluspalvelin
- Kaikki lokeissa näkyvät “Deprecated” varoitukset tulee korjata ennen päivitystä
- https://wiki.shibboleth.net/confluence/display/IDP4/Upgrading

Asennus

- Noudattaa edellisten versioiden tapaa
  - Sovelluspalvelin kuntoon
  - Asennusskriptin ajo
  - Konfigurointi
- Aiemman version konfiguraatiotiedostoja ei voi kopioida uuteen versioon vaan tulee käyttää uuden version konfiguraatiotiedostoja

XML allekirjoituksen algoritmi

- Oletusasetuksilla IdP salaa viestit siten, että iso osa muuta kuin Shibbolethia käyttävistä Service Providereista ei niitä pysty avaamaan
- IdP4:ssa on asetus, jolla voidaan palauttaa aikaisempi salausmenetelmä
- Jos haluaa käyttää turvallista algoritmia, voi joutua tekemään poikkeuksia
- https://wiki.shibboleth.net/confluence/display/IDP4/GCMEncryption

OpenID Connect

- OpenID Connect Shibboleth Plugin on nyt osa Shibboleth konsortiota
- Tarjotaan vielä erillisenä pakettina, mutta tuki on konsortion kautta
- Versio 2 on IdP4:lle, versio 1 IdP3:lle

OpenID Connect

- Käyttöönotto isossa mittakaavassa vielä korkeakoulumaailman federaaatioissa odottaa
- OpenID Federation määritys versiossa 1.0 draft 11 23.4.2020
- https://openid.net/specs/openid-connect-federation-1_0.html

Attribuutit

- IdP3:ssa ja aiemmissa muodostettavat attribuutit rakennettiin attribute-resolver.xml –tiedostossa
- Annettiin attribuutille id, nimi SAML2-viesteissä sekä miten attribuutti enkoodattiin

Attribute Registry

- IdP4:ssa attribuutit konfiguroidaan attribuuttirekisteriin
  - Jos päivität, attribute-resolver pysyy käytössä kuten ennenkin
- https://wiki.shibboleth.net/confluence/display/IDP4/AttributeRegistryConfiguration

Attribute Registry

- Sisältää samat asiat kuin aiemmin
  - Nimi
  - Id
  - SAML2 Encoder
  - OpenId Encoder
  - Selkokielinen nimi eri kielillä
- Sijaitsee IDP_HOME/conf/attributes hakemistossa

Attribute Registry

- Asennuspaketissa tulee valmiina
  - eduPerson.xml
  - inetOrgPerson.xml
  - eduCourse.xml
  - samlSubject.xml
- Tulee lisätä itse
  - FunetEduPerson
  - Schac
- Haka-spesifit attribuutit kannattaa yhteistyössä tehdä ja jakaa

Esimerkki

```
<bean parent="shibboleth.TranscodingProperties">
    <property name="properties">
        <props merge="true">
            <prop key="id">displayName</prop>
            <prop key="transcoder">SAML2StringTranscoder SAML1StringTranscoder</prop>
            <prop key="saml2.name">urn:oid:2.16.840.1.113730.3.1.241</prop>
            <prop key="saml1.name">urn:mace:dir:attribute-def:displayName</prop>
            <prop key="displayName.en">Display name</prop>
            <prop key="displayName.de">Anzeigename</prop>
            <prop key="displayName.fr">Nom</prop>
            <prop key="displayName.it">Nome</prop>
            <prop key="displayName.ja">表示名</prop>
            <prop key="description.en">The name that should appear in white-pages-like applications for this person.</prop>
            <prop key="description.de">Anzeigename</prop>
            <prop key="description.fr">Nom complet d'affichage</prop>
            <prop key="description.it">Nome</prop>
            <prop key="description.ja">アプリケーションでの表示に用いられる英字氏名</prop>
        </props>
    </property>
</bean>
```

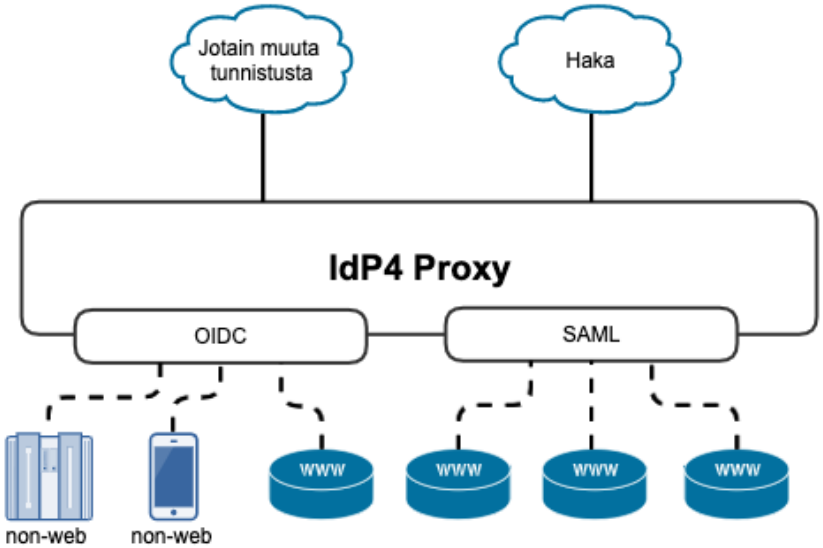
Autentikointimenetelmät

- Samat käytössä kuin aiemmin, mutta menetelmästä riippuen niissä on joitakin pieniä muutoksia
- Uusi autentikaatiomenetelmä on SAML

SAML2-autentikointi

- IdP:iin voidaan kytkeä toinen SAML2 IdP tunnistuslähteeksi
- Käyttötapauksia
  - Vain OpenId:ta tukevan palvelun tuominen Hakaan (protokollamuunnin)
  - Organisaatio tunnistaa käyttäjänsä tunnistuspalvelimessa, joka osaa SAML2:ta, mutta se ei kykene toimimaan federaatiossa -> IdP4 proxy hoitamaan federaatioiden metadatan hallinta ja SAML2-viestit
- Toiminnallisuus tunnetaan nimellä IdP Proxy

IdP Proxy


Jotain muuta tunnistusta
Haka
IdP4 Proxy
OIDC
SAML
www
www
www
www
non-web
non-web

SAML2-autentikointi

- IdP:lle muodostetaan vastaava tunnistusvuo kuin esim. LDAP ja vaiheet ovat samat
- Konfiguroidaan missä IdP:ssa käyttäjä tunnistetaan
- Tunnistavalta IdP:lta saadaan käyttäjätunniste sekä mahdollisesti attribuutteja
- IdP4:ssa parsitaan saadut tiedot tunnistavalta IdP:lta ja voidaan hakea lisäinformaatiota lisälähteistä

Jatkossa

- Alunperin oli tarkoitus pitää päivän workshop IdP4:sta asennuksesta ja päivityksestä, mutta nykytilanne sotki suunnitelman
- On mahdollista, että sellainen pidetään syksyllä, mutta mahdotonta tässä vaiheessa tietää
- Ei kannata siis jäädä odottamaan vaan ryhtyä toimeen

Käytännön juttuja

- Attribuuttirekisterin tiedostojen koostaminen ja jakelu
- Asennusdokumentaationa päälähteenä Shibboleth Wiki
- CSC tekee omaan käyttöönsä IdP-asennusskriptejä
  - https://github.com/CSCfi/