Tunnistuslähteen päättelypalvelu

Discovery Service (DS) ratkaisee tunnistuslähteen päättelyongelman. Se selvittää, mikä tunnistuslähde (Identity Provider - IdP) voi tunnistaa käyttäjän ja antaa hänestä soveltuvimmat henkilötiedot. Yleensä tämä on käyttäjän oman kotiorganisaation tunnistuspalvelu. Joillakin käyttäjillä saattaa olla käyttäjätunnus useammassa kotiorganisaatiossa.

Perinteisesti käyttäjän tunnistaminen alkaa siitä, kun käyttäjä (käyttäjän selain) saapuu palveluun (Service Provider - SP). Tässä vaiheessa palvelu ei tiedä, mikä on käyttäjän kotiorganisaatio. Käyttäjän kotiorganisaation päätteleminen selaimen IP-osoitteen perusteella on mahdollista muttei kattavaa, koska käyttäjä saattaa tulla palveluun muualta kuin kotiorganisaationsa osoitteesta. Käyttäjän selain ei anna palvelulle sellaista tietoa, jonka perusteella käyttäjän tunnistuslähde selviäisi.

Hakan keskitetty DS-palvelu (ent. WAYF) on CSC:n ylläpitämä ja löytyy osoitteesta:

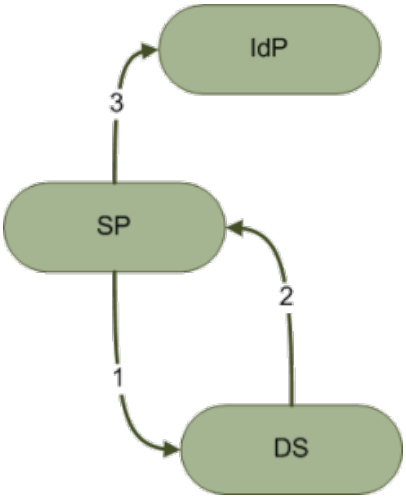
```
https://haka.funet.fi/
DS
```

Konfiguroi tämä osoite Service Provider:in asetuksiin, mikäli haluat käyttää keskitettyä WAYF/DS-palvelua.

Upotettu DS

Voit myös halutessasi integroida DS-palvelun oman palvelusi sivulle.

Keskitetty päättelypalvelu



Standardoimiskonsortio OASIS on julkaissut muiden SAML-määritysten ohella tunnistuslähteen päättelystä oman profiilinsa. "(Profiili) määrittelee yleisen selaimeen perustuvan protokollan, jolla voidaan toteuttaa palvelusta erillinen keskitetty päättelypalvelu, jolla kirjautumista pyytävälle palvelulle voidaan luovuttaa käyttäjän tunnistamiseen kykenevän tunnistuslähteen yksilöivä tunniste." [1]

Profiilissa määritelty palvelu tunnetaan myös nimellä WAYF - Where Are You From. Haka-luottamusverkostossa keskitettyä päättelypalvelua ylläpitää CSC.

Kuvassa esitetään profiilissa määritetty reitti palvelusta tunnistuslähteeseen DS:n kautta.

1. Palvelu ohjaa käyttäjän tunnistuslähteen päättelypalveluun
2. DS palauttaa palvelulle käyttäjän kertoman tunnistuslähteen EntityId:n
3. Palvelu tarkistaa tunnistuslähteen osoitteen SAML-metadatastaan ja ohjaa käyttäjän tunnistuspalveluun

Kuten pääsääntöisesti muutenkin SAML-tekniikassa, myöskään DS:n yhteydessä palvelun, päättelypalvelun ja tunnistuslähteen välillä ei välitetä tietoa suoraan, vaan tieto välittyy käyttäjän selaimessa. Edellä kuvatuissa askelissa käyttäjä siirtyy prosessissa eteenpäin uudelleenohjauksilla (HTTP-Redirect).

Keskitetyn päättelypalvelun ongelmat

Päättelypalvelu (WAYF/DS) on laajasti käytetty tekniikka, joka yleensä tuotetaan luottamusverkostossa keskitetysti. Kaikissa tilanteissa sen käyttö ei kuitenkaan ole ongelmatonta tai tarkoituksenmukaista. Esimerkiksi

- Tunnistukseen nojaava palvelu sallii pääsyn vain yhdestä tai muutamasta tunnistuslähteestä, mutta luottamusverkoston keskitetty päättelypalvelu sisältää luottamusverkoston kaikki tunnistuspalvelut
- Käskitetyn päättelypalvelun ulkoasu ja ilme poikkeaa tunnistukseen nojaavan palvelun ilmeestä, mikä saa loppukäyttäjän hämilleen. Käyttäjä ei välttämättä ymmärrä luottamusverkoston roolia kirjautumisessa.
- Tunnistukseen nojaava palvelu sallii pääsyn tunnistuslähteistä, jotka kuuluvat eri luottamusverkostoihin
- Käynti keskitetyssä päättelypalvelussa aiheuttaa käyttäjälle yhden tai usean ylimääräisen klikkauksen, mikä edustaa huonoa käytettävyyssuunnittelua

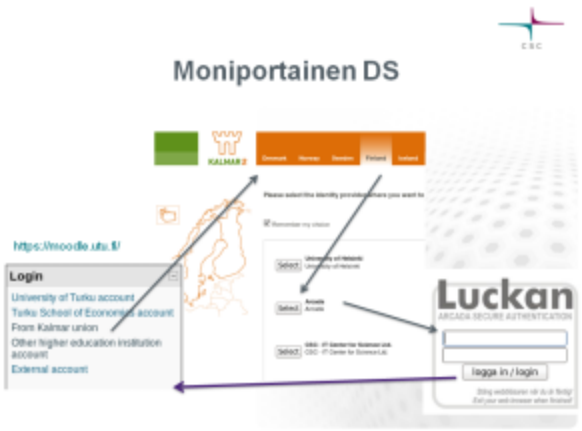
Kahdesta viimeisestä kohdasta on esimerkki oheisessa kuvassa, joka esittää kirjautumisen vaiheet Turun yliopiston Moodle-palveluun käyttäen Kalmarin unionin päättelypalvelua

1. Käyttäjä valitsee palvelun etusivulta kirjautumismenetelmän useasta eri vaihtoehdosta.
2. Päättelypalvelussa valitaan ensin maa, jonka federaatiota käytetään
3. Tämän jälkeen valitaan oma kotiorganisaatio
4. Oman kotiorganisaation tunnistautumispalvelussa tehdään varsinainen kirjautuminen
5. Käyttäjä ohjautuu lopulta palveluun kirjautuneena käyttäjänä

Moniportaisessa tunnistuslähteen päättelyssä korostuu myös alttius phishing-hyökkäyksille. Kirjautuminen tapahtuu aina kotiorganisaation tunnistuspalvelussa. Organisaation käyttäjätunnuksia ei saa antaa minnekään muualle. Kirjautumisen vaiheiden ollessa moninaiset käyttäjä saattaa olla houkutettu antamaan tunnuksensa valepalveluun, joka houkuttelee kirjautumisen helppoudella.

Päättelypalvelun sivuuttaminen

Päättelypalvelu voidaan ohittaa ohjaamalla käyttäjän selain suoraan toivotulle tunnistuslähteelle. Tämä toteutetaan tietyllä tavalla muotoillulla linkillä SP:n tai IdP:n tarkoitusta varten varattuun päätepisteeseen. Käytännölle ei ole vakiintunutta suomenkielistä termiä, mutta voidaan puhua vaikkapa kirjautumislinkeistä.



Kirjautumislinkkillä voidaan viitata SP:iin, jolloin puhutaan SP-initiated kirjautumisesta, tai tunnistuslähteeseen, jolloin puhutaan IdP-initiated kirjautumisesta. Tämä kirjautumistapa on esitelty SAML-profiilissa [2] nimellä 'Unsolicited Responce'. Hakan käyttämän Julkishallinnon yhteisen SAML-profiilin [3] perusteella SP:n on tuettava (MUST) tätä kirjautumistapaa.

Kirjautumislinkeillä palvelun etusivulle voidaan toteuttaa linkkilista, jossa linkkiä klikkaamalla valitaan, minkä kotiorganisaation tunnistuslähteellä halutaan kirjautua. Keinoa voi myös hyödyntää esimerkiksi aliverkkotunnuksien uudelleenohjauksilla, jossa osoite https://orgA.palvelu.tldn/ johtaa organisaatio A:n tunnistuslähteelle ja osoite https://orgB.palvelu.tldn/ johtaa organisaatio B:n tunnistuslähteelle.

Kirjautumislinkki toteutetaan lisäämällä sille attribuutteina kotiorganisaation tunnistuslähteen entityId ja se osoite, johon käyttäjä halutaan ohjata kirjautumisen jälkeen.

Seuraavassa on esimerkki Shibboleth-tuotteelle SP-initiated linkistä, jolla kirjaudutaan Hakan testipalvelun IdP:llä attribuuttitestipalveluun:

- https://testsp.funet.fi/haka/Shibboleth.sso/Login?entityID=https://testidp.funet.fi/idp/shibboleth&target=https://testsp.funet.fi/haka/

Seuraavassa on esimerkki vastaavasta IdP-initiated linkistä:

- https://testidp.funet.fi/idp/profile/SAML2/Unsolicited/SSO?providerId=https://testsp.funet.fi/shibboleth&target=https://testsp.funet.fi/attribute-test/

Palveluun upotettu tunnistuslähteen päättely

Edellä esitetyt kirjautumislinkit voidaan sovelluksessa tuottaa ohjelmallisesti. Yleensä niitä käytetään palveluissa, joihin on tarve kirjautua vain muutamalla tunnistuslähteellä. Niinpä niiden ylläpito on usein käsityötä. Käsityö voidaan välttää käyttämällä tarkoitusta varten kehitettyjä sovelmia.

Tunnistuslähteen päättely voidaan upottaa palveluun javascript-sovelmilla. Palvelun etusivulle lisätään skripti, joka tuo päättelypalvelun osaksi etusivua. Käyttäjän näkökulmasta päättelypalvelu on osa varsinaista palvelua ja hän siirtyy tunnistuslähteeseen suoraan palvelusta.

Shibboleth-projektin Embedded Discovery Service (EDS) on itsenäinen sivulle lisättävä komponentti.

Upotettavat päättelypalvelut tukeutuvat vahvasti uusiin metadatan MDUI-elementteihin, joilla parannetaan päättelypalvelun käytettävyyttä.

Shibboleth Embedded Discovery Service (EDS)

Shibbolethiin upotettu päättelypalvelu toimii luontevimmin osana Shibboleth SP -ohjelmistoa. SP:ssä on valmiina päätepiste, josta EDS saa tiedot tunnistuslähteistä. EDS käyttää samaa SAML-metadataa, kuin SP-ohjelmisto. EDS:n valintalistalle tulee siis kaikki ne ja toisaalta vain ne tunnistuslähteet, joiden kanssa SP:lla on luottosuhde. Tämä on hyödyllistä silloin, kun SP luottaa vain osaan federaation tunnistuslähteistä tai se on muodostanut federaation lisäksi luottosuhteen kolmannen osapuolen tunnistuslähteisiin.

Shibboleth EDS on riippumaton ulkoisista palveluista. Se tarvitsee toimiakseen vain SP:n, jolta se lataa metadatan tunnistuslähteistä.

Tarkempaa tietoa EDS:stä ja sen asentamisesta löytyy tästä linkistä: https://shibboleth.atlassian.net/wiki/spaces/EDS10/overview

Haka-EDS

Myös Hakan keskitetyn päättelypalvelun voi upottaa palvelun sivulle. Lisää ohjeita täällä.

Seamless Access Service (Edugain)

https://seamlessaccess.org/

https://seamlessaccess.atlassian.net/wiki/spaces/DOCUMENTAT/pages/84738141/Discovery+Service+Integration

Muuta

Uudet palvelut tarjoavat uusia mahdollisuuksia, joihin voidaan tarttua, kun SP-palvelua kehitetään. Uudet vaihtoehdot ovat otollisia harkita myös uutta palvelua perustettaessa.

julkishallinnon SAML-profiilin vaatimus Discovery Response URL:n lisäämisestä metadataan, jos keskitettyä päättelypalvelua käytetään. Näin keskitetty päättelypalvelu tarkistaa metadatasta sille ilmoitetun URL:n. Tämä rajoittaa tietynlaisten phishing-hyökkäyksien mahdollisuutta.

Hakan tunnistuslähteen ylläpitäjä voi edistää uusien päättelypalvelujen toimintaa ja tuoda organisaationsa paremmin näkyville syöttämällä tunnistuslähteestään MDUI-tiedot Haka-resurssirekisteriin.

Viitteet

1. Oasis, Identity Provider Discovery Service Protocol and Profile
2. Oasis, Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0
3. SAML 2.0 protocol deployment profile