Usein kysytyt kysymykset

UKK

Historia

Mistä Haka nimi tulee ja miten se kirjoitetaan?

Haka-luottamusverkoston nimi om muotoutunut 2000-luvun alussa olleesta Hakemistot käyttäjähallinnossa -projektista. Siinä selvitettiin LDAP-hakemistojen yhteiskäyttöä korkeakouluissa. Projektissa alettiin tutkia myös lupaavaa Shibboleth-tekniikkaa. Aiemmin oli selvitetty mm. HST-korttien käyttöä korkeakoulissa sekä oli Käyttäjät ja todentaminen -projekti käyttäjätunnistamiseen liittyen.

Shibboleth-tekniikan ympärille muodostui korkeakoulujen käyttöön käyttäjätunnistamisen luottamusverkosto, jonka nimeksi jäi Haka. Haka nimenä oli tullut projektin kautta tutuksi laajemminkin, joten se katsottiin sopivaksi. Sittemmin Shibboleth-tekniikasta siirryttiin standardoituun SAML-protokollaan, mutta nimi Shibboleth elää edelleen ohjelmistona ja usein myös itse toimintaan viittaavana.

Haka kirjoitetaan isolla alkukirjaimella Hakan ollessa vakiintunut nimi. Alunperin sen voi ajatella olleen lyhennesana, joiden kirjoittamisesta on ohje Kotimaisten kielten keskulsella https://www.kotus.fi/nyt/kolumnit_artikkelit_ja_esitelmat/hyvaa_virkakielta/hyvaa_virkakielta_-palstan_arkisto_%282002_2014%29/lyhennesanat

Liittyminen ja rekisteröinti

Asiakkaamme haluaisi Haka-kirjautumisen palveluun mahdollisimman nopeasti, mutta liittymisprosessi on kesken. Miten sitä voisi nopeuttaa?

Ohjausryhmä hyväksyy Haka-kumppanit ja tämän lisäksi palvelusopimuksen allekirjoituskierrossa CSC:llä kuluu aikaa. Tätä prosessia ei voi nopeuttaa, vaan projektissa siihen kannattaa varata kalenteriaikaa 4-6 viikkoa (yleensä sopimiskierto on kuitenkin valmis jo muutamassa viikossa). Liittymisprosessi on kuvattu omalla sivullaan.

Samanaikaisesti sopimusprosessin edetessä Haka-kirjautumisen käyttöönottoa voi edistää teknisesti toteuttamalla ja testaamalla palvelun Haka-integraatio valmiiksi. Kaikki Hakaan liitettävät entiteetit testataan vasten operaattorin testipalvelimia ennen tuotantometadataan lisäämistä. Operaattori varmistaa ennen tuotantometadataan siirtämistä, että on onnistuneesti toteutettu kirjautuminen vasten testipalvelinta. Entiteetin SAML-profiilinmukaisuus tarkistetaan pintapuolisesti.

Testaamisen lisäksi tarvitaan myös vahvistus kumppanin tai jäsenen hallinnolliselta yhteyshenkilöltä. Valmistele yhteyshenkilö jo etukäteen, että hän arvioi vastuulleen kuuluvat asiat ajoissa ennen tuotantoon siirtymistä:

> *Luottamusverkoston jäsenen tai kumppanin hallinnollinen yhteyshenkilö varmistaa erityisesti, että*
>
> - *palvelu ei ole ristiriidassa luottamusverkoston toiminnan tarkoituksen kanssa (Liite 2: "Haka-luottamusverkoston toiminnan tarkoitus on tukea korkeakoulujen ja tutkimuslaitosten toimintaa")*
> - *hakemuksessa esitetyt henkilötiedot, joita palvelu katsoo tarvitsevansa loppukyttäjistä, ovat palvelun tuottamisen kannalta tarpeellisia (Henkilötietolaki 9 §)*

- Haka-palvelusopimus, liite 5, kohta 4 SAML-palvelun rekisteröiminen luottamusverkostoon

SAML-tekniikaan hyvin perehtynyt IT-asiantuntija toteuttaa teknisesti federoinnin muutaman kalenteriviikon kuluessa. Laajasti käytettyjä SAML-tuotteita, kuten Shibbolethia käytettäessä tekninen käyttöönotto voidaan tehdä muutamassa päivässä. Sovelluksen autentikaation ja sessionhallinnan toteutuksesta riippuu, miten helppoa sen federointi on. Projektin aikataulutuksessa on myös huomioitava muut ennakoivat työvaiheet, kuten tuotevalinta, henkilötietojen käsittelyn suunnittelu tai nykyisten käyttäjätilien liittäminen Haka-kirjautumisesta saatavaan identiteettiin. Joidenkin sovellusten kohdalla tai hankalien riippuvuussuhteiden hallitsemiseksi joskus joudutaan valmistautumaan laajemmin ja varamaan aikaa huomattavasti tässä mainittua enemmän.

Olemme tilaamassa järjestelmää, jossa ominaisuutena on federoitu kirjautuminen. Pitääkö toimittajan liittyä Haka-kumppaniksi? Kenen nimiin uusi palvelu rekisteröidään?

Haka-kumppaniksi liittyminen on maksutonta toimittajalle, mikäli järjestelmä tehdään jonkin Haka-jäsenen toimeksiannosta. Palvelu voidaan myös rekisteröidä järjestelmän tilaajan nimiin, jos niin halutaan. Rekisteröivä taho on oikeutettu tekemään muutoksia palvelun Haka-tietoihin. Rekisteröinti kannattaa yleensä käytännön syistä tehdä sen tahon nimiin, joka vastaa järjestelmän päivittäisestä ylläpidosta. Asiaa voi tarkastella myös siitä näkökulmasta, kuka vastaa palvelun muodostamasta henkilörekisteristä ja miten palvelun henkilötietojen käsittely on suunniteltu toteutettavan.

Jos järjestelmä tulee vain yhden Haka-jäsenen käyttöön, rekisteröinti voidaan suorittaa harkinnan mukaan joko toimittajan tai tilaajan nimiin. Jos järjestelmästä tulee useille Haka-jäsenille oma instanssi, yleensä tällöin kannattaa toimittajan liittyä Haka-kumppaniksi.

Määrittelemme järjestelmää X. Onko olemassa keskitetty rekisteri korkeakouluopiskelijoista / korkeakoulujen henkilökunnasta, jonka perusteella käyttäjätunnistus ja/tai käyttövaltuutus voitaisiin toteuttaa?

Haka on hajautettu järjestelmä, jossa kukin korkeakoulu vastaa omien käyttäjiensä tiedoista.Haka näyttää teknisesti palvelun kannalta yhdeltä järjestelmältä, mutta ei ole olemassa yhtä keskitettyä rekisteriä, josta käyttäjätietoja voi poimia.

Käyttäjistä saatavilla olevien tietojen määritykset löytyvät FunetEduPerson-skeemasta. Osa tiedoista on pakollisia, joita kaikkien Haka-jäsenten on ylläpidettävä, osa perustuu vapaaehtoisuuteen.

Palvelun on mahdollista määrittää myös omia käyttäjätietoja valtuutuksen tueksi. Tällöin on kuitenkin huomioitava, että käyttäjätiedot tulee tallentaa Hakaj-jäsenen järjestelmiin ja käyttäjätietojen ylläpitoon on oltava mekanismit. Yksittäisen palvelun voi olla vaikea saada Haka-jäsentä suostumaan tallettamaan ja ylläpitämään yhtä palvelua koskevia käyttäjätietoja.

Mitä tietoja resurssirekisteriin vähintään täytyy syöttää uudesta palvelusta (Service Provider)?

- Rekisteröijällä (registree) tarkoitetaan organisaatiota tai henkilöä, joka on lisäämässä palvelua testiin / Hakaan
- Rekisteröijän velvollisuus on pitää ilmoittamansa tiedot ajan tasalla ja ilmoittaa muutoksista - myös testipalvelun osalta
- Haka-resurssirekisterin rekisterinpitäjä on Tieteen tietotekniikan keskus - CSC, joka toimii Haka-operaattorina (katso Yhteystiedot)

Palvelun rekisteröimiseksi testiin tarvitaan vähintään:

- Palvelun nimi
- **Yksilöllinen** entity id
  - testiin ei hyväksytä localhost entity id:tä, vaan id:n on oltava **yksilöivä**
  - entity id:ksi suositellaan rekisteröijän virallisesti omistama URI. Esim. yleisesti tunnetun rekisterinpitäjän myöntämä verkkotunnus (domain name; esim. suomalaisen .fi -verkkotunnuksen rekisterinpitäjä on Viestintävirasto)
  - entity id:n ei tarvitse olla esim. toimiva www-sivu, vaan se on tarkoitettu yksilöimään palvelu muista
- SAML-viestien suojaamiseen tarkoitettu varmenne
- tekninen kontakti
- jos halutaan testi-idp:n luovuttavan attribuutteja, on resurssirekisterin syöttölomakkeelle kirjattava attribuuttipyynnöt
- toimiva assertion consumer service URL(riittää, että testaajan selaimelta on pääsy kyseiseen URL:iin)
  - URL:n on oltava yksilöllinen ja kohteen liittyä kyseiseen palveluun
  - muihin palveluihin (tai localhostiin) viittaavia URL:eja ei hyväksytä edes testiin
  - URL:n ei ole pakko resolvoida Internetin yleisessä DNS-palvelussa
  - Hakassa on käytössä vain HTTP-POST, joskin muita voidaan tarvita, jos samaa palvelua käytetään myös muualla, kuin Hakassa
- Jos rekisteröijän organisaatiota ei ole lueteltu resurssirekisterissä, voi testivaiheessa käyttää: "Haka testiorganisaatio"

Palvelun rekisteröimiseksi Hakaan tarvitaan edellisten lisäksi:

- palvelun nimi (kielillä fi, sv, en)
- laadukas kuvaus palvelusta (kielillä fi, sv, en - katso lisää: Metadatan käyttöliittymäelementit)
- tekninen ja support-kontaktit
- jos palvelu pyytää yksilöiviä henkilötietoja, tarvitaan tietosuojaselosteen URL
    - tietosuojaseloste on oltava julkisesti Internetissä saatavilla
- jos palvelussa käytetään Hakan keskitettyä DS-palvelua, tarvitaan DS-response URL
- attribuuttipyynnöt on perusteltava
    - organisaation hallinnollinen Haka-yhteyshenkilö tarvitsee tietoa tehdessään valistuneen päätöksen hyväksyä palvelu liitettäväksi Hakaan

Lisäksi suositellaan syöttämään:

- käyttöliittymäelementtien (MDUI) tiedot
- palvelun kirjautumissivun URL

Huomaa kertauloskirjautumisesta (SLO)

- SLO-endpointin rekisteröiminen ilmaisee SP:n tuesta kertakirjautumiselle
- SLO-tuen ilmoittaminen aiheuttaa lisävelvollisuuksia, jotka palvelun on täytettävä
- jos ei olla varmoja SLO-tuesta, suositellaan jättämään SLO-endpointin URL rekisteröimättä

Olemme rekisteröimässä kehitysympäristöä Hakaan

Yleisesti ottaen Haka-operoinnin vahva näkemys on, että kehitys- ja testivaiheessa ei pidä käyttää aitoja henkilötietoja. Lähtökohtaisesti Hakan tuotantometadataan ei pitäisi rekisteröidä testi- tai kehitysympäristöä, vaan testaaminen ja kehittäminen pitäisi toteuttaa Hakan testiympäristössä. Jos palvelun testaaminen on välttämätöntä toteuttaa tuotanto-IdP:n kanssa, pitäisi riskejä rajata vähintään niin, että luottosuhde tehdään paikallisesti kyseisen organisaation IdP:n ja testattavan palvelun välillä sen sijaan, että testattava palvelu rekisteröidään varsinaiseen Haka-metadataan.

Huomioi testaamisessa mm. se, että

- Hakan tuotantoympäristössä ei ole yleiskäyttöisiä testitunnuksia
- käyttäjätunnuksia luovutetaan vain tosielämän henkilöille ja näistä luovutetaan vain paikkaansa pitävää, ajantasaista tietoa.
- aitojen henkilötietojen käyttö on suunniteltava ja käsittelyssä on noudatettava huolellisuutta
- palvelu ei voi samaan aikaan esiintyä Hakan tuotantometadatassa ja testiympäristössä

Hakaan on lisätty ohjausryhmän päätökseen perustuen joitakin QA-ympäristöjä (Quality Assurance), joiden tarkoituksena on toteuttaa hyväksyntätestaus ennen varsinaista käyttöönottoa tai versiopäivitystä. Tällaiseen QA-ympäristöön on jo tehty varsinainen kehitystyö ja järjestelmätestaus. Hyväksyntätestauksen jälkeen päivitys viedään tuotantoympäristöön, jonka jälkeen QA- ja tuotantoympäristöt ovat ohjelmistoteknisesti identtisiä.

QA-ympäristön kypsyydestä huolimatta sillä on oltava oma, erillinen tietosuojaseloste. Palvelun nimi, kuvaus ja tietosuojaselosteessa kerrottu henkilötietojen käyttötarkoitus eivät voi olla samoja QA-ympäristössä (jossa suoritetaan hyväksymistestausta) ja tuotantoympäristössä (jossa tuotetaan palvelua loppukäyttäjille).

QA-ympäristöä on myös muuten ylläpidettävä samalla tarkkuudella, kuin tuotantoympäristöä. Henkilötietojen käsittely on suunniteltava tuotantoympäristöstä erikseen ja käsittelyä on toteutettava muutenkin samalla huolellisuudella, kun muissakin tuotantopalveluissa, jossa käsitellään aitoja henkilötietoja. Henkilötietojen käsittely voi noudattaa saman tyyppisiä prosesseja, kuin tuotantoympäristössä, mutta henkilötietoja ei esimerkiksi voi ehkä säilyttää yhtä pitkään, kuin tuotantoympäristössä. Tiedot on ehkä poistettava hyväksyntätestauksen valmistuttua, kun tuotantoympäristössä pidempiaikainen tallentaminen saattaa olla perusteltua.

Hakan käyttö

Yritin kirjautua Hakalla palveluun X, mutta kirjautuminen epäonnistui

Haka-operoinnin tukipalvelu on tarkoitettu Haka-palvelujen ja kotiorganisaatioiden tunnistuslähteiden SAML-palvelimien tekniselle ylläpitohenkilöstölle.

Yleisin syy loppukäyttäjän kirjautumisvirheisiin on väärä käyttäjätunnus tai salasana. Loppukäyttäjän käyttäjätunnuksiin liittyvissä ongelmissa on otettava yhteyttä oman kotiorganisaation IT-helpdeskiin.

Haka on hajautettu järjestelmä, jossa loppukäyttäjät kirjautuvat palveluihin oman kotiorganisaationsa tunnuksilla. Joskus saattaa olla yhteensopivuusongelmia henkilötietojen välittämisessä kotiorganisaation tunnistuslähteen ja palvelun välillä. Tällaisissa tilanteissa joko palvelu tai kotiorganisaation tunnistuslähde antaa näkyville virheilmoituksen, joka on teknisen ylläpitohenkilöstön ensimmäinen vihje vian löytämiseen. Loppukäyttäjän voi olla mahdollista jo vikailmoituksesta päätellä, onko syytä ottaa yhteys omaan kotiorganisaatioon, vai palvelun ylläpitoon.

Vikailmoituksessa järjestelmän antaman virheilmoituksen lisäksi ensiarvoisen tärkeää on ilmoittaa päivämäärä ja tarkka kellonaika (sekä ulkomailla aikavyöhyke), jolloin vika ilmeni. Tarkan kellonajan lisäksi voit liittää vikailmoitukseesi kuvakaappauksen saamastasi virheilmoituksesta. Liitä mukaan myös selkeä kuvaus siitä, mitä olit tekemässä ja missä vaiheessa kirjautumisprosessia vika ilmaantui.

Viat ovat harmillisia ja olemme luonnollisesti pahoillamme kohtaamastasi haitasta. Vaikka olemme varautuneet lähes kaikkeen mahdolliseen, toisinaan eteen tulee tilanteita, jotka ylittävät odotuksemme. Tekemäsi selkeä ja kattava vikailmoitus on sijoitus seuraavaa vastaavaa tilannetta varten, jossa joku muu on ehtinyt jo tehdä hyvän vikailmoituksen sinun puolestasi ennen kuin edes huomaat mitään vikaa olleenkaan.

Eikös tämän pitänyt olla kertakirjautumista? Miksi minua pyydetään kirjautumaan uudelleen?

Webin ytimessä toimivaa HTTP-protokollaa kutsutaan tilattomaksi. Sivulatauksiin liittyvät kutsut ovat sikäli toisistaan irrallisia, että kahden eri sivulatauksen välillä ei pelkän pyynnön perusteella välity tieto siitä, kuka palvelua käyttää (ellei sitä erikseen pyynnössä jollain tavalla ilmaista). Tätä varten web-tekniikassa käytetään erilaisia istunnonhallinnaksi kutsuttuja menetelmiä käyttäjätiedon selvittämiseksi turvallisesti sivulatausten yhteydessä. Yleisin tapa on käyttää selaimeen tallennettuja evästeitä (cookie). Perusohjeistus on, että evästeet unohtuvat, kun selain suljetaan. Avaimesi avoimiin istuntoihin siis häviävät muistista, kun suljet selaimen. Avattuasi selaimen uudelleen, joudut myös kirjautumaan uudelleen.

SAML-kirjautumisen yhteydessä sinulla on istunto paitsi omassa tunnistuslähteessäsi, myös niissä palveluissa, joihin olet kirjautunut tekniikkaa käyttäen. Näiden istuntojen pituudet vaihtelevat. Jokainen organisaatio ja palvelu määrittelee istunnon maksimipituuden (session lifetime) ja ajan, jonka se voi olla joutilaana (session inactivity). Palvelu voi myös erikseen vaatia uudelleenkirjautumista siitäkin huolimatta, että istunto tunnistuslähteellä on vielä voimassa.

Palvelu ei tarjoa mahdollisuutta kirjautua ulos. Miten varmistan, että muut eivät pääse tietoihin käsiksi?

Paras tapa kirjautua ulos Haka-palvelusta on sulkea selain. Sulkemalla selaimen kirjaudut ulos kaikista palveluista, joita olet käyttänyt. Huomaa, että välilehden sulkeminen ei riitä, vaan koko selain tulee sulkea.

Kirjauduin ulos palvelusta, mutta mennessäni toiseen palveluun tai samaan palveluun uudelleen, minulta ei kysytä tunnusta ja salasanaa! Onko tämä turvallista?

Haka perustuu SAML-tekniikkaan, jonka ytimessä on kertakirjautuminen. Niin pitkään, kuin istuntosi (kts. edellinen kohta) on tunnistuslähteellä voimassa, sinun ei tarvitse kirjautua uudelleen ellei palvelu sitä erikseen pyydä. Jokainen organisaatio ja palvelu määrittelee oman tietoturvapolitiikkansa perusteella, kuinka pitkään istunto on voimassa.

Kertakirjautuminen on kohtuullisen helppo toteuttaa, mutta uloskirjautuminen kaikista palveluista ja tunnistuslähteeltä ei ole aivan yhtä suoraviivaista. Tähän liittyvät ongelmat on kuvattu hyvin Shibboleth-ohjelmiston wiki-sivulla englannin kielellä.

Olen toteuttamassa uutta Haka-ominaisuutta palveluumme. Voinko saada teiltä testitunnukset ominaisuuden testaamiseen?

Tuotantotunnistuslähdettä vasten testaamiseen tarvitaan henkilö, jolla on Haka-tunnukset. Varsinaisessa Hakan tuotantoympäristössä, eli Hakan varsinaiseen tuotantometadataan liitettyjen palvelujen ja tunnistuslähteiden verkostossa ei ole mahdollista saada nk. pseudotunnuksia, vaan Haka IdP:t saavat luovuttaa vain ajantasaista ja oikeaa tietoa tosielämän henkilöistä. Joistakin palveluista on lisätty Hakaan nk. esituotanto- (pre-production) tai laadunvarmistusympäristöjä (Quality Assurance). Näissäkin palveluissa henkilötietojen käsittely suunnitellaan ja toteutetaan Haka-palvelusopimuksen ja Suomen hekinlötietolain vaatimusten mukaisesti.

Hakan jäsenorganisaatiot määrittävät ja kuvaavat käyttäjähallinnon kuvauksissaan, minkälaisille henkilöille tunnuksia luovutetaan. Testaamiseen osallistuville henkilöille voidaan luovuttaa tunnuksia organisaation kuvaamien periaatteiden mukaisesti, mutta tunnistuslähteen luovuttamien tietojen on oltava oikeita ja ajantasaisia. Esim. eduPersonAffiliation attribuutin arvoa "student" ei voi luovuttaa, jos henkilö ei tosiasiassa ole ilmoittautunut läsnäolevaksi organisaatiossa järjestettävään tutkintoon johtavaan koulutusohjelmaan.

CSC tarjoaa tuotannosta erillisen testiympäristön, jonka palvelimien avulla voi testata ennen tuotantoon siirtymistä. Lisätietoja testipalvelimista on tällä alisivulla. Testiympäristöön voi liittää myös esituotanto- tai kehitysympäristön. Testiympäristössä ei käsitellä aitoja henkilötietoja ja testitulokset ovat luonteeltan julkisia. Testituloksia ja testipalvelimien tietoja voidaan esimerkiksi vaihtaa sähköpostitse testiin osallistuvien kehittäjien kanssa jouduttamaan Haka-integraation toteuttamista ja palvelun kehittämistä.

En muista Haka-tunnustani. Voitteko lähettää minulle uuden salasanan?

Haka on hajautettu käyttäjätunnistusjärjestelmä, jossa käyttäjät kirjautuvat palveluihin oman kotiorganisaationsa käyttäjätunnuksella. Hakan operaattorina toimii CSC, joka tuottaa verkoston keskitetyt palvelut, kuten metadatan hallinnan ja jakelun sekä tunnistuslähteen päättelypalvelun. Operaattori tuottaa myös tukipalvelua Hakaan liittyneiden jäsen- ja kumppaniorganisaatioiden teknisille yhteyshenkilöille.

Loppukäyttäjiä tunnusasioissa tukee heidän oma kotiorganisaationsa (korkeakoulu tai tutkimuslaitos). Yhteystiedot oman organisaation IT-tukeen, salanan nollaamiseen tai tunnuksen saamiseen löytää usein organisaation omilta www-sivuilta tai intranet-sivustolta. Haka-operaattori CSC ei pysty salasanoja tai käyttäjätunnuksia käsittelemään.

Tarvitsen pääsyn Haka-palveluun. Mistä saan Haka-tunnuksen?

Haka on hajautettu käyttäjätunnistusjärjestelmä, jossa käyttäjät kirjautuvat palveluihin oman kotiorganisaationsa käyttäjätunnuksella. Erillistä Haka-tunnusta ei ole, vaan omassa kotiorganisaatiossasi avataan pääsy Haka-palveluihin niille henkilöille, jotka ovat organisaation Haka-kirjautumisen piirissä. Jos organisaatiosi on asettanut tunnistuspalvelun Hakaan, mutta tunnuksellasi ei pysty kirjautumaan organisaatiosi tunnistuspalvelussa, ole yhteydessä oman organisaatiosi IT-tukeen kysyäksesi mahdollisuutta avata Haka-käyttö tunnuksellesi.

Jos et ole jäsenenä organisaatiossa, joka kuuluu Hakaan, et voi kirjautua Hakaa käyttäen. Joissakin palveluissa on Haka-kirjautumisen rinnalla myös muita kirjautumisvaihtoehtoja. Näistä kannattaa kysyä lisätietoa palvelun käyttäjätuesta.

SAML-profiili

Autentikaatiopyynnön allekirjoittaminen

Hakassa noudatetaan julkishallinnon yhteistä SAML 2.0 profiilia muutamin täydennyksin. Profiili edellyttää, että palvelu (SP) allekirjoittaa autentikaatiopyynnöt. Oletusarvoisesti Shibboleth-ohjelmisto ei allekirjoita autentikaatiopyyntöä. Allekirjoituksen saa päälle esim. asettamalla shibboleth2.xml -tiedostossa ApplicationDefaults -elementin signing-attribuutti asentoon "true" tai "front".

Autentikaatiopyynnön allekirjoitus shibboleth2.xml

```
<ApplicationDefaults entityID="https://testsp.nonexistent.tldn/shibboleth"
                     REMOTE_USER="eppn persistent-id targeted-id"
                     signing="front" encryption="false">
```

Haka ja SAML vaikuttavat monimutkaiselta kokonaisuudelta!

Haka on SAML-protokollaa käyttävä palvelu. Monesti on helpointa ensin hahmottaa mikä on SAML, ja sen jälkeen tarkastella mitkä ovat Hakan erityispiirteitä eli miten sovellan SAML-protokollaa Hakan yhteydessä.

- SAML V2.0 Executive Overview on Oasiksen, eli SAML:n standardoiman yhteisön oma johdon tiivistelmä SAML-määrityksistä ja SAML:n eduista
- http://www.switch.ch/aai/demo/ on Sveitsin käyttäjätunnistusverkoston Shibbolethiin perustuva demo käyttäjätunnistusverkoston toiminnasta. Demon kuvituksesta käy hyvin ilmi SAML:n perustoiminta.
- Haka-käyttäjien tapaamisissa on perinteisesti ollut vapaaehtoinen esiseminaari, jossa esitellään federoidun identiteetinhallinnan perusteet. Viimeisimmän seminaarin materiaali löytyy täältä. Vuoden 2010 seminaari on videoitu ja linkit myös esiseminaarin videoihin löytyy täältä.
- Shibboleth-ohjelmisto on avoimeen lähdekoodiin perustuva ja laajimmin Hakassa käytetty. Ohjelmisto on perusteellisesti dokumentoitu Shibboleth-wikissä. Perusteisiin tutustuminen on hyvä aloittaa wikin kohdasta UnderstandingShibboleth.
- Hakaan on mahdollista asettaa palvelu käyttäen SAML2-määritykset täyttävää ohjelmistoa, joka täyttää Haka-profiilin vaatimukset. Toteutuksia on paljon. Wikipediassa on luettelo, josta voi lähteä liikkeelle vertailussa.

Vaikka SAML-määritysten kokonaisuus tuntuu laajalta ja alkuun pääsemisen kynnys voi tuntua jyrkältä, kannattaa aloittaa testaamalla. Oppiminen yrityksen ja erehdyksen, eli tekemisen kautta on SAML-tekniikan kannalta ehkä helpoin tie.

Mikä on ACS URL?

Assertion consumer service URL on se, johon käyttäjän selain palautetaan, kun IdP on tunnistanut käyttäjän, hakenut ja suodattanut attribuutit sekä muodostanut vastauksen SP:n (palvelu, eli Service Provider) autentikaatiopyyntöön. IdP palauttaa SP:lle käyttäjän selaimessa HTTP-POST:lla autentikaatiovastauksen jonka mukana kulkee käyttäjän henkilötiedot sisältävä assertio. ACS-URL on ilmoitettava metadataan, että IdP voi tarkistaa sen olevan SP:n asiallinen URL. Tällä tarkistuksella ehkäistään henkilötietojen vuotaminen; että kuka tahansa ei voi pyytää IdP:ltä henkilötietoja mihin tahansa.

ACS URL muodostuu jokaisessa SAML-tuotteessa eri tavalla. Shibbolethissa ACS URL on oletuksena muotoa: "http(s):// + hostname + [:port] + handlerURL + /SAML2/POST". Eli jos Shibbolethin handlerURL on oletus: "Shibboleth.sso" ja palvelun URL on: "https://service.tldn", olisi ACS-URL: "https://service.tldn/Shibboleth.SSO/SAML2/POST".

Lisätietoa löytyy Shibbolethin wikistä: NativeSPSession, NativeSPAssertionConsumerService. Lisätietoa kirjautumisprosessin etenemisestä on: FlowsAndConfig, Web Browser SSO Profile.

Mikä on NameID ja mitä tulisi käyttää?

NameID on SAML2-standardissa määritetty tunniste, jota käytetään ainakin sitomaan käyttäjän istunto palvelussa kirjautumistapahtumaan tunnistuspalvelimessa. Se voi olla myös joissa tilanteissa käyttäjästä palvelussa käytettävä tunniste. SAML2-standardi määrittää useita vaihtoehtoisia NameID:ta, joista Hakassa käytetään transient- ja persistent-typpiisiä. Monet sovellukset olettavat NameID-kentässä käyttäjän sähköpostiosoitetta, mutta se ei ole tuettu tapa Hakassa.

Transientid on käyttäjästä jokaisella tunnistuskerralla muuttuva tunnistemerkkijono, jolla ei ole muuta tarkoitusta kuin pystyä liittämään käyttäjä istunto palvelussa tunnistuspalvelimen tapahtumiin. Tämä on oletus, jota Hakassa käytetään, koska käyttäjän tunnisteena lähes aina käytetään eduPersonPrincipalName-attribuuttia.

Persistent on käyttäjästä palvelukohtainen tunniste, joka on tietyllä käyttäjällä tiettyyn palveluun mentäessä aina sama. Eli palvelu voi muodostaa tämän avulla profiilin palvleuun, mutta persistentid ei paljasta käytttäjän henkilöllisyyttä, jos muita attribuutteja ei ole käytössä. Tällä voidaan tehdä siis tunnistettuja, mutta anonyymeja palveluita. Kaikki Haka IdP:t eivät persistentid:tä tue, tukevat tunnistuspalvelut selviävät Haka-metadatasta kunkin IdP:n kohdalta.

Jos siis ei ole perusteltua syytä poiketa, valitse transientid palvelua rekisteröitäessä. Jos valitset persistentid:n, varmista, että ymmärrät sen käyttötarkoituksen.

Tekniset ongelmat (SP / IdP)

SP ei saa attribuutteja IdP:ltä (Haka)

Haka IdP:n on ylläpidettävä attribuuttien luovutussääntöä. Vain palvelun tarvitsemia attribuuteja saa luovuttaa. Hakassa useat IdP:t tukeutuvat attribuuttien luovutussäännöissä SP:n Haka-metadatan yhteydessä ilmoittamiin attribuutti-pyyntöihin (RequestedAttribute). Palvelut (SP) kirjaavat Hakan resurssirekisteriin palvelun tarvitsemat attribuutit, eli tekevät attribuuttipyynnön. Osa Hakaan rekisteröidyistä IdP:istä luottaa metadatan attribuuttipyyntöihin, eli perustavat luovutussääntönsä metadataan.

IdP:ille on ohjeistettu käyttämään tuoretta Haka-metadataa. Historiallisista tai teknisistä syistä jotkin IdP:t saattavat päivittää luovutussääntönsä käsityönä ylläpitäjän toimesta. Joissain tapauksissa uuden palvelun (SP) luovutussäännöt eivät tule IdP:llä voimaan ennen IdP:n uudelleenkäynnistämistä.

Jos palvelun (SP) tarvitsemat attribuutit on lueteltu Haka-metadatassa, mutta IdP ei luovuta pyydettyjä attribuutteja, kannattaa palvelun (SP) ylläpitäjän olla yhteydessä suoraan IdP:n ylläpitäjään metatiedoista löytyviin yhteystietoihin. Myös Haka-operoinnin tukeen voi olla yhteydessä.

Edugainiin rekisteröityyn palveluun ei pysty kirjautumaan organisaatiomme IdP:llä

SP ei saa attribuutteja IdP:ltä (eduGAIN)

Sähköpostiosoite käyttäjän yksilöimisessä

mail-attribuutin käyttäminen käyttäjän yksilöintiin ei ole hyvä idea. Vuoden 2016 alusta lähtien mail-attribuutti muuttuu Hakassakin suositelluksi, jolloin käytännössä kaikkien IdP:iden pitäisi populoida arvo käyttäjähakemistoonsa. Attribuuttien yleisenä luovuttamisen edellytyksenä on, että sille on perusteltu käyttötarkoitus palvelussa.

Sähköpostiosoite on huono tieto käyttäjän yksilöintiin. Yhdellä käyttäjällä saattaa olla useita sähköpostiosoitteita. Toisaalta mikään ei takaa, että Haka IdP:n luovuttamaa sähköpostiosoitetta ei luovutettaisi useammalle käyttäjälle. Käyttäjähakemistoon tallennettu sähköpostiosoite voi olla käyttäjän itsensä määrittämä, jolloin siihen liittyy virhemahdollisuus. Organisaation velvollisuus on luovuttaa vain virheettömiä tietoja, mutta erikseen ei ole määritetty, miten sähköpostiosoitteen tarkistaminen pitäisi organisaatiossa tehdä.

Sähköpostiosoite muuttuu herkemmin, kuin varsinaiset yksilöintiin tarkoitetut tunnisteet. Esimerkiksi käyttäjän nimen muuttuessa usein myös sähköpostiosoite muuttu, mutta yksilöllinen tunniste pysyy entisellään. Suomalaisilla on paljon täyskaimoja, henkilöitä, joilla on sama etu- ja sukunimi. Lyhyenkin ajan sisällä voi käydä niin, että tietyn sähköpostiosoitteen haltija vaihtuu. Haltijan vaihtuminen voi tapahtua ilman, että palvelu saa siitä tiedon tai voi muutoin olettaa osoitteen haltijan vaihtuneen.

Sähköpostiosoitteen sijasta Hakassa parempi tunniste käyttäjän yksilöintiin on eduPersonPrincipalName-attribuutti (eppn).

Palveluni tulisi sallia pääsy vain tietyistä Haka-organisaatioista

Haka-metadatassa luetellaan kaikkien Haka-organisaatioiden tunnistuspalvelimet IdP:t. Lähtökohtaisesti Haka-palvelun tulisi luottaa näihin kaikkiin. Luottosuhde muodostuu lataamalla metadatatiedosto käyttöön palvelussa. On kuitenkin tilanteita, joissa vain joistakin organisaatioista sallitaan pääsy palveluun.

Paras tapa estää joistakin organisaatioista pääsy palveluun on tehdä se sovelluksessa. Tällöin sovelluksen sisällä voidaan ohjeistaa käyttäjää, että palvelu ei ole hänelle käytettävissä ja miten hänen tulisi toimia tilanteessa.

Myös sovelluksen alla toimivassa web-palvelimessa voidaan tehdä pääsynhallintaa ja estää/sallia joistakin organisaatioista pääsy. Shibbolethia käytettäessä tähän löytyy ohjeita Shibboleth Wikistä. Näin toimittaessa on syytä varmistaa web-palvelimen antamien virhesivujen sisältö.

Sallittaessa pääsy vain joistakin organisaatioista pääsy palveluun, on suositeltavaa toteuttaa tunnistuspalvelimen valinta palvelun omassa käyttöliittymässä. Palveluun siis tehdään tunnistuspalvelimen valintapalvelu eikä käytetä keskitettyä Haka DS:ia, jossa on listattuna kaikki organisaatiot. Tällä vältytään tarpeettomilta tunnistuksilta ei-sallittujen organisaatioden käyttäjissä.

Huonoin vaihtoehto on metadatatasolla estää luottosuhteiden muodostuminen tiettyihin organisaatiohin. Tässä tilanteessa on vaarana hallitsemattomat virhetilanteet käyttäjien kirjautumisissa. Jos metadatatasolla estetään luottosuhde johonkin organisaatioon, on erittäin tärkeää huolehtia tunnistuspalvelimen valinnasta palvelun omassa käyttöliittymässä, jotta vältytään luottosuhteeseen perustuvista virheistä.

Päivitin IdP:n versioon neljä ja joihinkin palveluihin estyi pääsy

Shibboleth IdP4:ssa on oletuksena käytössä GCM-algoritmi XML-viestien salaamisessa. Tätä algoritmia eivät kaikki varsinkaan vanhemmat palvelut Hakassa tue. Ensimmäinen ja paras vaihtoehto on, että palvelu päivittäisi SP:nsa tukemaan GCM-algoritmia

Mikäli SP:ssa tukea ei saada toteutettua, tunnistuspalvelimen voi kuitenkin helposti konfiguroida tukemaan myös vanhempia algoritmejä, joita ei kuitenkaan suositella käytettäväksi laajemmin. Tarkat ohjeet IdP:n konfigurointiin löytyvät: https://wiki.shibboleth.net/confluence/display/IDP4/GCMEncryption

Alla on listattu palveluita (Haka, eduGAIN), joiden tiedämme etteivät tue GCM-algoritmia salauksessa. Voit ilmoittaa omista havainnoistasi haka@csc.fi.

metadata-providers.xml

```
<MetadataProvider backingFile="%{idp.home}/metadata/haka-metadata.xml" id="HTTPHakaMetadata" maxRefreshDelay="
PT2H" metadataURL="https://haka.funet.fi/metadata/haka-metadata.xml" refreshDelayFactor="0.5" xsi:type="
FileBackedHTTPMetadataProvider">
  <MetadataFilter certificateFile="%{idp.home}/credentials/haka-sign-v5.pem" xsi:type="SignatureValidation"/>
  <MetadataFilter xsi:type="EntityRoleWhiteList">
    <RetainedRole>md:SPSSODescriptor</RetainedRole>
  </MetadataFilter>
  <MetadataFilter xsi:type="Algorithm">
    <md:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"/>
    <Entity>http://fse.eduuni.fi/adfs/services/trust</Entity>
        <Entity>https://login.aka.fi:443/uas</Entity>
    <Entity>https://e-learn.csc.fi/saml/sp</Entity>
    <Entity>http://adfs.eta.csc.fi/adfs/services/trust</Entity>
    <Entity>http://fs.findata.csc.fi/adfs/services/trust</Entity>
    <Entity>https://virkailija.opintopolku.fi/service-provider-app/saml/metadata/alias/hakasp</Entity>
        <Entity>https://auth.oamk.fi/simplesaml/module.php/saml/sp/metadata.php/haka</Entity>
        <Entity>https://video.lamk.fi</Entity>
         <Entity>https://savonia.alma.exlibrisgroup.com/mng/login</Entity>
    <Entity>https://moodle.karelia.fi/auth/saml2/sp/metadata.php</Entity>
    <Entity>https://www.jobiili.fi/</Entity>
    <Entity>https://testihallinta.amkvalintakoe.fi</Entity>
    <Entity>https://hallinta.amkvalintakoe.fi</Entity>
    <Entity>https://hallinta.korkeakouluun.fi</Entity>
    <Entity>https://mooc.helsinki.fi/auth/saml2/sp/metadata.php</Entity>
    <Entity>http://fs.thinking1.com/adfs/services/trust</Entity>
    <Entity>https://certia.efectecloud.com:443/idm</Entity>
    <Entity>https://rekry.saima.fi/vismahakasp</Entity>
    <Entity>https://www.kopi.fi/</Entity>
    <Entity>https://ipr.mrooms.net/auth/saml2/sp/metadata.php</Entity>
    <Entity>https://virkailija.testiopintopolku.fi/service-provider-app/saml/metadata/alias/hakasp</Entity>
    <Entity>https://edu.flinga.fi/saml</Entity>
 </MetadataFilter>
 </MetadataProvider>
<MetadataProvider backingFile="%{idp.home}/metadata/edugain-metadata.xml" id="HTTPEdugainMetadata"
maxRefreshDelay="PT2H" metadataURL="https://haka.funet.fi/edugain-nightly/gen-edugain/idp-[X]-metadata-eduGain.
xml" refreshDelayFactor="0.5" xsi:type="FileBackedHTTPMetadataProvider">
  <MetadataFilter certificateFile="%{idp.home}/credentials/haka-edugain-sign.csc.fi.2020.pem" xsi:type="
SignatureValidation"/>
  <MetadataFilter xsi:type="EntityRoleWhiteList">
    <RetainedRole>md:SPSSODescriptor</RetainedRole>
  </MetadataFilter>
  <MetadataFilter xsi:type="Algorithm">
    <md:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"/>
    <Entity>http://adfs.eta.csc.fi/adfs/services/trust</Entity>
    <Entity>http://fs.findata.csc.fi/adfs/services/trust</Entity>
    <Entity>https://terena.org/sp</Entity>
  </MetadataFilter>
</MetadataProvider>
```

Varmenteet

SAML-varmenne on vanhenemassa / jo vanhentunut, mutta uusi varmenne on vasta haussa!

Hakassa käytettävän SAML-viestien vaihdon suojaamiseen tarkoitetun varmenteen uusimiseen on varattava aikaa n. kuukausi. Tähän ei sisälly varmenteen tekemiseen tai hankkimiseen tarvittava aika. Varmenteen vaihtaminen tehdään niin, että se ei aiheuta katkoa tai haittaa palvelun käytölle. Vaihtoprosessi on kuvattu tarkemmin erillisessä ohjeessa.

SAML-varmenne julkaistaan muille verkoston entiteeteille Haka-metadatassa. Hakassa metadatan normaali julkaisusykli on noin kerran kahden viikon aikana. Metadatan julkaisua voidaan aikaistaa painavasta syystä. Hakassa on lähes 450 entiteettiä, joiden varmenteet uusitaan säännöllisesti. Varmenteen vanhenemiseen on mahdollista varautua etukäteen ja tästä syystä varmenteen vanhenemista ei yleisesti katsota painavaksi syyksi poiketa normaalista metadatan julkaisusyklistä.

Varmennekäytännössä on määritetty, minkälaisia varmenteita Hakassa voidaan käyttää. Huomaa, että käyttäjälle näkyvän HTTP-liikenteen suojaamiseen käytettävän SSL-varmenteen ei tarvitse olla sama, jota käytetään Hakassa SAML-viestien suojaamiseen. Kiiretilanteessa kannattaa uudistaa SSL-varmenne erikseen ja SAML-varmenne rauhassa prosessin mukaisesti.

Määritysten mukaan toimivat SAML-tuotteet toimivat myös vanhentunutta varmennetta käytettäessä. Metadata-iop toteaa seuraavaa:

> *"In the case of an X.509 certificate, there are no requirements as to the content of the certificate apart from the requirement that it contain the appropriate public key. Specifically, the certificate may be expired, not yet valid, carry critical or non-critical extensions or usage flags, and contain any subject or issuer. The use of the certificate structure is merely a matter of notational convenience to communicate a key and has no semantics in this profile apart from that. However, it is RECOMMENDED that certificates be unexpired."*

Esim. Shibboleth-ohjelmistoa käyttävät entiteetit toimivat ongelmitta myös vanhentuneella varmenteella.

Haluan uudistaa SAML-varmenteen lennosta noudattamatta prosessia, onnistuuko se?

SAML-varmenteen voi uusia myös "lennosta" korvaamalla vanha varmenne uudella. Tämä aiheuttaa katkon palvelun käyttöön, sillä verkoston muut entiteetit on ohjeistettu päivittämään metadatansa vähintään kerran vuorokaudessa. Entiteetit päivittävät metadatansa eri aikaan ja ennen kuin uusi varmenne on tullut kaikkien muiden entiteettien tietoon, tarvitaan aikaa vähintään vuorokausi. Jos kyse on palvelusta, jota käytetään vain muutamasta organisaatiosta, on mahdollista sopia näiden kanssa, että ne päivittävät metdatansa välittömästi sen julkaisemisen jälkeen.

Jos päätät uudistaa varmenteen lennosta,

- neuvottele Haka-operoinnin kanssa metadatan julkaisuajankohdasta
- SP:n ollessa kyseessä sovi palvelua käyttävien organisaatioiden kanssa, että niiden IdP:t noutavat uuden metadatan välittömästi sovitun julkaisuajankohdan jälkeen
- IdP:n ollessa kyseessä sovi keskeisten palvelujen kanssa, että ne noutavat uuden metadatan välittömästi sovitun julkaisuajankohdan jälkeen
- vaihda SAML-tuotteesi varmenne samaan aikaan, kun uusi metadata julkaistaan