Muutoksenhallinta

Yleisiä huomioita SAML-entiteettien muutoksenhallinnassa

Entity Identifierin pysyvyys

Haka-operaattori viittaa seuraavissa suosituksissaan Shibboleth -projektin suosituksiin entiteettien nimeämisessä (entityId:n käytössä): https://wiki.shibboleth.net/confluence/display/SHIB/EntityNaming.

EntityId:tä käytetään opaakkien tunnisteiden (pysyvä nimitunniste - Persistent Name Identifier, eduPersonTargetedId) luomisessa. Opaakit tunnisteet muuttuvat entityId:n muuttuessa. EntityId:n muuttuminen voi myös joissakin tapauksissa aiheuttaa tarpeetonta ylläpitotyötä niissä järjestelmissä, jotka luottavat rekisteröitävään palveluun. Näistä syistä entityId:n **suositellaan** olevan mahdollisimman pysyvä ja muuttuvan vain perustellusta syystä.

EntityId:n **suositellaan** olevan enintään 1024 merkin pituinen URI. Yksilöllisyyden varmistamiseksi **suositellaan** käyttämään rekisteröivän organisaation omistamaa nimiavaruutta (esim. URL-muotoiseen verkkotunnukseen perustuva tai urn:oid). Minkään palvelun ei odoteta vastaavan entityId:n URL:n määrittämästä osoitteesta. Koska host-nimet muuttuvat, **ei suositella** rekisteröitävän palvelun tuottavan palvelimen nimeen perustuvaa entityId:tä.

Entity Identifierin nimenselvitys (Resolution)

EntityId:n määrittämän URI:n ei tarvitse resolvoitua (esim. ei tarvitse olla Internetin DNS-järjestelmässä), mutta sen **suositellaan** kuuluvan rekisteröijän omistamaan nimiavaruuteen. Koska entityId:n on pysyttävä pitkään muuttumattomana, rekisteröijän on syytä huomioida, että SAML2:ssa on mahdollista määritellä metadatan nouto käyttäen entityId:n määrittämää nimeä. Tällainen menetelmä ei ole Hakassa toistaiseksi käytössä, mutta on mahdollista, että se tulee käyttöön ajan kuluessa.

Henkilötietojen käsittelytarkoituksen muuttuminen palvelussa (SP)

Haka-palvelusopimuksen liitteessä 3 todetaan erityisistä vaatimuksista palveluntarjoajille:

> *Jos henkilötietojen käsittelytarkoitusta palvelussa muutetaan, toimitaan kuin jos palvelu kytkettäisiin luottamusverkostoon uutena palveluna.*

Henkilötietojen käsittelytarkoituksen muuttuessa palvelun entityId **suositellaan** vaihdettavan. Palvelun vastaanottamat opaakit tunnisteet muuttuvat ja palveluun suhtaudutaan luottamusverkosssa, kuin se olisi uusi, toinen palvelu.

Haka-metadatan päivitystahti

Haka-metadata päivitetään yleensä kerran kahden viikon kuluessa. Päivitystahti ei noudata tiettyä ennalta määritettyä aikataulua. Painavista syistä päivitystä voidaan aikaistaa. Kaikissa muutoksissa on huomoitava, että muutos tulee voimaan vasta seuraavassa metadatajulkaisussa siitä, kun muutos on operaattorin toimesta vahvistettu resurssirekisterissä. Ajoittain myös Haka-operoinnin helpdesk-palvelussa voi olla ruuhkaa, jolloin muutoksien käsittelyssä voi olla viiveitä.

Välittämästi metadataan tehdään tietoturvan varmistavat muutokset, kuten varmenteen poistaminen silloin, kun siihen liittyvä salausavain on joutunut vääriin käsiin tai entiteetin tilapäinen poistaminen jos se on esimerkiksi murrettu.

Useimpiin muutoksiin on mahdollista varautua ja valmistautua hyvissä ajoin niin, että metadata ehditään päivittää normaalin julkaisurytmin mukaisesti.

Tunnistuslähteen yliheitossa huomioitavaa

Eppn pysyvyys

EduPersonPrincipalName on scoped-attribuutti, jonka alkuosa yksilöi käyttäjän loppuosan määrittämässä toimialueessa. Palvelujen velvollisuus on tarkistaa, että attribuuttiluovutuksena saatu skooppi vastaa IdP:n metadataan ilmoitettua. IdP:lle voi ilmoittaa metadataan useamman skoopin. Näin esimerkiksi organisaatioiden fuusioituessa käyttäjien eppn-attribuuttit voivat pysyä ennallaan. Operaattorin tulkintaohjeen mukaisesti eppn-attribuutti saa muuttua vain painavista syistä. Jos attribuutti muuttuu, on organisaation velvollisuus tiedottaa tästä palveluille. Tiedottamisen tueksi Haka-wikissä on sivu: eppn-muutoksista. Muutoksen läpikäyneen organisaation on kyseiselle sivulle tai sen alasivulle kirjattava miten ja koska attribuutin arvot muuttuvat. EPPN:n käytössä on myös syytä muistaa, että sen kierrättäminen ei ole Hakassa sallittua.

Opaakkien nimiattribuuttien pysyvyys

Opaakkeja nimiattribuutteja ovat eduPersonTargetedId (eptid) ja SAML-assertion subjectissa välitettävä pysyvä nimitunniste (persistent nameidentifier). Jokaiselle henkilölle luodaan yksi opaakki tunniste jokaista IdP-SP yhdistelmää kohden. Näin siis yhden IdP:n kahdelle eri SP:lle luovuttamat nimitunnisteet ovat erilaisia sen varmistamiseksi, että palvelut eivät voi identifioida käyttäjää vertailemalla saamiaan nimitunnisteita. Nimitunniste voidaan luoda ensimmäisen kirjautumisen yhteydessä ja tallentaa IdP:n tietokantaan. Nimitunnisteet voidaan myös tallentaa henkilöhakemistoon, mutta tällöinkin on huolehdittava vaatimuksesta, jossa jokaiselle palvelulle on käyttäjästä luovutettava erilainen nimitunniste.

Nimitunnisteet ovat pysyviä, eli ne eivät saa muuttua. Nimitunnisteen muuttuminen aiheuttaa, että käyttäjä menettää käyttäjäprofiilinsa sellaisessa palvelussa, joka tukeutuu nimitunnisteeseen. Nimitunnisteet ovat sidoksissa SP:n ja IdP:n entityId:hen, joten toisen muuttuessa myös nimitunniste muuttuu. Tästä syystä IdP:n yliheitossa entityId:n ei pitäisi muuttua.

EntityId:n säilyminen ei yksistään varmista tunnisteiden pysymistä, vaan yliheitossa on uudelle palvelimelle siirrettävä myös mahdollinen nimitunnisteiden tietokanta. Jossain tapauksessa pelkästään tiivistefunktion muodostamisessa käytettävän suolamerkkijonon (salt) ennallaan säilyttäminen riittää varmistamaan nimitunnisteiden pysyvyyden. On myös huomioitava, että SAML-tuotteet voivat muodostaa nimitunnisteet eri mekanismeilla, joten nimitunnisteita voi olla vaikea tai mahdoton säilyttää ennallaan tuotevaihdon yhteydessä.

Tunnistuslähteen (IdP) palvelinvaihdos

Metadatassa IdP-palvelimen tiedoissa voi olla kerrallaan vain yksi HTTP-redirect -tyyppinen SSO-URL -osoite. Tästä syystä osoitteen vaihdos on tehtävä niin, että sekä uusi, että vanha palvelin ovat yliheitossa muutaman vuorokauden rinnakkain käytössä. Kerralla vaihtaminen on mahdollista säilyttämällä varsinainen SSO-URL -osoite ennallaan ja tehdä palvelinvaihdos IP-osoitteen tasolla käyttäen kuormantasaajaa tai DNS-muutosta. Seuraavassa on eräs esimerkki prosessista, jolla IdP-palvelimen osoitteen muutos voidaan tehdä:

1. Asennetaan ja testataan IdP-palvelu uudella palvelimella / uudessa osoitteessa (vanha palvelin on edelleen käytössä rinnalla)
2. Kun uuden IdP-palvelimen toiminta on varmistettu, vaihdetaan Resurssirekisterissä IdP-palvelun SSO-URL osoittamaan uuteen palvelimeen / osoitteeseen. Neuvotellaan Haka-operoinnin kanssa DS-palvelun päivittäminen yhdessä metadatapäivityksen kanssa.
3. Odotetaan metadatan ja DS-palvelun päivittymistä (sekä uusi, että vanha IdP palvelin ovat toiminnassa)
4. Uuden metadatan julkaisun jälkeen palvelut päivittävät käyttämänsä Haka-metadatan vuorokauden kuluessa. Kyseisen vuorokauden aikana kirjautumiset tapahtuvat rinnakkain uudella ja vanhalla IdP-palvelimella. Palvelut (SP) siirtyvät käyttämään uutta IdP-palvelinta sitä mukaa, kun päivittävät metadatansa.
5. Vuorokauden kuluttua metadatan päivittymisestä varmistetaan, että vanhalle palvelimelle ei enää ohjaudu autentikaatiopyyntöjä. Mikäli autentikaatiopyyntöjä ohjautuu, selvitetään mistä palveluista ne tulevat ja pyydetään näitä palveluja päivittämään metadatansa.
6. Kun on varmistettu, että kaikki palvelut käyttävät uutta IdP-palvelinta, voidaan vanha poistaa käytösä.

Palvelun (SP) palvelinvaihdos

Palvelun (SP) assertion consumer service URL (ACS-URL) voi muuttua esimerkiksi, kun palvelu siirretään alustalta (palvelimelta) toiselle. Tässä yhteydessä ei ole tarpeen muuttaa muita palvelusta metadataan syötettyjä tietoja ja esim. palvelun entityId pysyy entisellään. EntityId:n säilyttäminen varmistaa, että opaakit nimitunnisteet säilyvät ja käyttäjät pääsevät omiin käyttäjäprofiileihinsa omilla tunnisteillaan. Samasta syystä entityId:n ei pitäisi perustua palvelualustan hostnimeen.

ACS-URL:n muutos tehdään seuraavalla prosessilla

1. Testataan palvelu uudessa osoitteessa / uudella alustalla
2. Lisätään uusi ACS-URL Resurssirekisteriin palvelun tietoihin
3. Odotetaan metadatan päivittymistä
4. Aikaisintaan 24 tunnin kuluttua metadatan päivittymisestä ohjataan käyttäjät palvelun uuteen osoitteeseen
5. Kun palvelun toiminta uudessa osoitteessa on varmistettu, poistetaan vanha ACS-URL resurssirekisteristä