S212 SAML ja S213 OIDC rajapintasuositusten lausunnot

1 Taustaa

Virasto julkaisi rajapintasuositukset tunnistuspalveluiden SAML ja OpenID Connect yhteyskäytännöille (protokollille) vuonna 2018. Vuonna 2019 TUPAS yhteyskäytännön alasajossa huomattiin että rajapintasuositusta olisi syytä tarkentaa.

Vuoden 2020 aikana virasto loi vahvan sähköisen tunnistamisen ja luottamuspalveluiden teknisiin asioihin keskittyvän avoimen sähköpostilistan. Tekninen ryhmä, joka koostui pääasiassa luottamusverkoston toimijoista ja heidän asiantuntijoistaan, kokoontui vuonna 2020 useamman kerran pohtimaan rajapintasuosituksen uudistamista. Teknisen ryhmän palautteiden ja ehdotusten perusteella virasto pyysi lausuntoja S212 (SAML) ja S213 (OIDC) yhteyskäytäntöihin liittyvistä muutoksista lausuntopalvelussa ajalla 5.3. - 6.4.2021.

Lausuntopyyntöön vastasivat DVV, OP Ryhmä, Danske Bank, Ubisecure ja Aktia Pankki. Seuraavissa kappaleissa käsitellään annetut lausunnot.

1.1 Kappale 2.2.2 Onko taulukko ajantasainen?

Kyllä: 5

Ei: -

Kommentit:

- Määrityksessä olisi hyvä välttää kiinteitä viittauksia algoritmeihin. Niiden sijasta olisi hyvä osoittaa viittaus vakiintuneen standardoijan määrittelemään ja aktiivisesti ylläpitämään algoritmiluetteloon.
- Emme näe päivitystarvetta.

Liikenne- ja viestintäviraston arvio: Lausuntojen perusteella ei ole nähtävissä tarvetta muuttaa suosituksia. Päätös: Ei muutoksia

1.2 Kappale 2.2.3/4.2.2 Olisiko tunnistuspyyntöjen allekirjoitus määriteltävä pakolliseksi (nyt tämä on valinnainen)?

Kyllä: 5

Ei: -

Kommentit/Miksi :

- Erilaisissa käyttötapauksissa ei olisi ns. tulkinnanvaraa onko allekirjoitusta tarpeellista käyttää ja tunnistuspyyntöjen osalta toimittaisiin aina mahdollisimman turvallisella tavalla. Pystyttäisiin aina varmistumaan, keneltä pyyntö on tullut.
- Reason: It is important to have the auth request as signed so that we know the source of the request. Also, signed has a expiry time, therefore it cannot be fraudulently invoked any number of times.

- Broker ja IdP välinen tunnistuspyyntö pitäisi olla allekirjoitettu. Tunnistuspyyntö sisältää tiettyjä parametreja kuten acr_values ja ftn_spname joiden eheys pitäisi olla varmistettu.
- Allekirjoituksen määrittäminen kategorisesti pakolliseksi vähentäisi yksittäistä konfiguraatiotarvetta ja tekisi toteutuksesta siten yksinkertaisemman.
- Pakollisuus olisi hyvä, koska se estäisi tunnistuspyyntöjen väärentämisen tai kaappaamisen.

Liikenne- ja viestintäviraston arvio:

Lausuntojen perusteella on perusteltua muuttaa luottavan osapuolen tunnistuspyyntöjen allekirjoitus valinnaisesta pakolliseksi.

Tunnistuspyyntöjen allekirjoitus luottamusverkoston sisällä voidaan säilyttää edelleen valinnaisena.

Määräyksen M72 uudistuksessa tämä sama asia on ollut esillä ja käsittely jatkuu myös itse määräyksen valmistelutyössä.

Päätös: Muutetaan pakolliseksi

1.3 Kappale 3.1.1.2/3.1.2.2 Onko lista valinnaisista attribuuteista riittävä?

Kyllä: 4

Ei: -

Kommentit/Mitä tulisi lisätä:

- Kommenttina AuthCachingDisabled on näkemyksemme mukaan uusi. Tärkeää on, että nämä pysyvät valinnaisina atribuutteina jatkossakin.

Liikenne ja viestiäviraston arvio:

Lausuntojen perusteella ei ole nähtävissä tarvetta muuttaa suosituksia. AutoCachingDisabled on ollut suosituksessa alusta lähtien.

Päätös: Ei muutoksia

1.4 Kappale 4.2 Onko tunnistuspyynnön parametreissä pakolliseksi muutetun ftn_spname kommentti tarpeeksi selkeä?

Kyllä: 3

Ei: 2

Kommentit/Miten muuttaisit tekstiä:

- Reason: According to the description, they expect the Service Provider name to be displayed in the language selected by the user. Does it mean the Service provider has to send the SP name in all three languages? Please clarify.
- Loppukäyttäjän käyttökokemuksen kannalta parametrin käsittelyä olisi hyvä tarkentaa.

Pitäisikö sovelluksen nimen lisäksi esim. välityspalvelun nimi näkyä tai olla näytettävissä käyttöliittymissä? Ja käyttöliittymä tarkoittaa tässä yhteydessä usein kahta asiaa: käyttäjän selaimessa ja tunnistusvälineessä näkyvät käyttöliittymät.

Tärkeää olisi että tunnistusvälineessä näytetään mahdollisimman tarkasti samat tiedot kuin selaimessa.

Esim. jos selaimessa näkyy "Olet kirjautumassa Esimerkkikauppa Oy palveluun" myös mobiilissa tunnistusvälineessä pitäisi näkyä sama sovelluksen nimi

Liikenne- ja viestintäviraston arvio:

Attribuutin ftn_spname kohdalla on nähtävissä tarvetta tarkentaa rajapintasuositusta. Asiointisovelluksen nimen näyttäminen kaikissa niissä tilanteissa ja käyttöliittymissä, joissa vaaditaan käyttäjän toimenpiteitä, on määräyksen M72 uudistustyössä esitetty pakolliseksi. Itse suosituksessa olisi hyvä tarkentaa miten toimitaan eri kielisten selainasetusten kanssa.

Päätös: Tarkennetaan kuvausta kieliversioihin liittyen perustuen teknisen työryhmän näkemykseen myöhemmässä vaiheessa tarpeen mukaan. Nykyisessä suosituksessa oleva teksti voisi olla riittävä "The name is RECOMMENDED to be in the same language as user's preferred user interface language (parameter ui_locales)." Suosituksen julkaistavasta versiosta kieliversiointi on poistettu, ja otetaan tarvittaessa uudelleen suositukseen, jos tekinen työryhmä päättää sen olevan tarpeellinen.

1.5 Kappale 4.2.1 Olisiko ensitunnistustapahtumissa (ketjutus) välitettäviä attribuutteja lisättävä?

Kyllä: -

Ei: 4

Kommentit/Mitä tulisi lisätä:

- Reason: A sufficient parameter “ftn_chain_level” already exists.
- Tunnistuspyynnön yhteyteen ei ole tarvetta lisätä attribuutteja. Sen sijaan voisi tarkentaa nykyisiä FTN LOA -tasoja ensitunnistamisen vahvuutta kuvaavalla vektorilla, joka voitaisiin ilmaista tunnistusvastauksessa luovutettavina attribuutteina ketjutetun tunnistustapahtuman yhteydessä.

Liikenne- ja viestintäviraston arvio:

Lausuntojen perusteella ei ole nähtävissä tarvetta lisätä ensitunnistuksen attribuutteja.

Päätös: Ei muutoksia

1.6 Kappale 4.3.1/4.5.1 Onko uusi virhetilanteita koskeva määrittely riittävällä tasolla?

Kyllä:

Ei: 4

Kommentit:

- Error-tasolla olisi hyvä olla useampiakin määritelmiä kuin kaksi. Päättelyä ei pitäisi siirtää error_decscription osuuden tietosisältöön, vaan vastaanottajan pitäisi saada suoraan oikea error=[arvo] jolla on yksiselitteinen merkitys. Esimerkiksi juuri 'user cancel' olisi hyvä tuoda error-tasolle, jotta se erottuu varsinaisesta access_denied -tilanteesta.
- Reason: More error response are needed. For example, "invalid_grant", "invalid_grant_type", "invalid_state" which tells that the auth code is expired or the invalid code is sent.
- Kappaleesta on jäänyt puuttumaan työryhmissä keskusteltu ehto, että virhevastaus palautetaan vain tunnistetulle asiakastoteutukselle.
- Cancelille pitäisi lisätä oma virhekoodi. Error = "cancel" jolla voi olla sitten error_description lisäkenttä tai sitten ei ole lisäkenttää.

Liikenne- ja viestintäviraston arvio:

Virheidenkäsittelyä käsiteltiin teknisen ryhmän työpajoissa vuonna 2020. Virasto pyysi luottamusverkoston jäseniltä muutosehdotusta suositukseen. Muutosehdotus saatiin ja se käytiin läpi teknisen ryhmän työpajassa. Lausuntojen perusteella on tulkittavissa, että suosituksen teksti ei vielä vastaa toivottua. Mainінta virhevastauksen palauttamisesta voidaan viraston tulkinnan mukaan lisätä suositukseen välittömästi. Virheidenkäsittelyn kohdalla olisi suotavaa, että luottamusverkoston toimijat pääsevät yhteisymmärrykseen vakiotavasta käsitellä virheitä tai virhetilanteita. Viraston näkemyksen mukaan paras keino tähän olisi järjestää virheidenkäsittelyn yhtenäistämistä varten oma työpajansa, jossa toimivat voisivat sopia käytänteistä ja vakioiduista virheviesteistä.

Päätös: Lisätään maininta virhevastauksen palautuksesta tunnistetulle asiointisovellukselle. Järjestetään virheidenkäsittelyyn oma työpajatapaaminen, jonka perusteella muodostetaan yhteneväinen näkemys suositukseen tarvittavista muutoksista.

1.7 Vapaa palaute OIDC-suosituksesta Anna tässä vapaamuotoinen palaute luonnoksesta (OIDC).

- Free OIDC feedback

  Mandate some basic requirements for the UI screen such as cancel button, display Service provider name, language selection, etc.

  It would be good to display the log/error ID so it can be used for investigation.
- Kappaleessa 2.2.1 kehotetaan käyttämään etukäteen kiinnitettyjä avaimia, mutta avainten vaihdon prosessi jätetään kuvaamatta. Tämä on johtanut kirjavaan avaintenvaihtokäytäntöön verkostossa. Olisi parempi toimia avaintenvaihdossa OIDC Core -määrityksessä vakiintuneella tavalla.

Liikenne- ja viestintäviraston arvio:

Vuoden 2020 teknisissä työpajoissa yhtenä käsiteltävänä asiana oli käyttöliittymien yhtenäistäminen ja kirjaaminen suositukseen. Virasto pyysi luottamusverkoston toimijoilta ehdotusta, mutta tällaista ei toimitettu. Yhteneväisen graafisen ilmeen, tai elementtien lisääminen voidaan suositukseen sisällyttää, mutta tämä tarvitsee

luottamusverkoston toimijoiden hyväksynnän laajemmin. Lisäksi on oleellista että ehdotus suosituksen muuttamiseksi tulisi yhteneväisenä näkemyksenä verkoston toimijoilta. Määräyksen M72 uudistuksessa asiointisovelluksen nimen kuljettaminen ja näyttäminen läpi koko tunnistusprosessin on ollut esillä. Määräyksen valmistuttua muutetaan suositusten tekstejä heijastamaan uutta määräystä ja määräyksen perusteluja.

Kiinnitettyjen avainten (certificate/key pinning) ja avaintenvaihtoa sekä tietoliikenne- että sovellustasolla ollaan selkeyttämässä määräyksen M72 uudistuksen yhteydessä. Määräyksen valmistuttua, virasto muuttaa myös rajapintasuosituksia heijastamaan mahdollisia muutoksia määräyksessä tai määräyksen perusteluissa.

Aikataulu määräykseen liittyville muutoksille on vuoden 2022 alkupuoli.

Päätös: Ei muutoksia suositukseen. Otetaan käyttöliittymään/liittymiin esitetty toive uudestaan teknisen ryhmän pohdittavaksi.

1.8 Kommentit SAML-suosituksesta Anna tässä vapaamuotoinen palaute luonnoksesta (SAML).

- Free SAML feedback

  Standardize the auto key renewal in SAML flow.

Liikenne- ja viestintäviraston arvio:

Asiaa käsitellään edellisessä kohdassa (kiinnitetyt avaimet/avaintenvaihto)

1.9 Muut kommentit/Lausunnot

- Traficom on pyytänyt Digi- ja väestötietovirastolta lausuntoa Luottamusverkoston SAML- ja OIDC-rajapintasuosituksista. Digi- ja väestötietovirasto (DVV) kiittää mahdollisuudesta lausua asiassa ja esittää lausuntonaan seuraavaa.

  DVV pitää hyvänä, että rajapintasuositusta päivitetään ja että päivitystyötä on tehty yhteistyössä luottamusverkoston ja muiden markkinatoimijoiden kanssa. DVV näkee myös hyvänä, että rajapintakuvaukset julkaistaan vain englanniksi, jotta ne olisivat laajasti suoraan hyödynnettävissä ja tulkintaeroja eri kieliversioiden välillä ei pääsisi syntymään.

  Kappale 2.2.3 / 4.2.2

  DVV:n näkee hyvänä, että tunnistuspyynnön allekirjoittaminen olisi rajapintasuosituksessa määritelty pakolliseksi. Tunnistuspyynnön allekirjoittaminen on tälläkin hetkellä melko yleinen käytäntö, mutta jos se olisi määritelty pakolliseksi, erilaisissa käyttötapauksissa ei olisi ns. tulkinnanvaraa allekirjoituksen tarpeellisuuden osalta ja toimittaisiin aina mahdollisimman turvallisella tavalla. Pystyttäisiin aina varmistumaan, keneltä pyyntö on tullut.

  Kappale 4.3.1 / 4.5.1

  DVV esittää, että virhetilanteita koskevan määrittelyn sanasto voisi olla laajempikin kuin kaksi termiä. Päättelyä ei pitäisi siirtää error_decscription osuuden tietosisältöön, vaan vastaanottajan pitäisi saada suoraan oikea error=[arvo] jolla on yksiselitteinen merkitys. Esimerkiksi juuri ’user cancel’

olisi hyvä tuoda error-tasolle, jotta se erottuu varsinaisesta access_denied -tilanteesta.

Muilta osin DVV:lla ei ole lausuttavaa rajapintasuosituksista.