

Finnish Trust Network SAML 2.0 Protocol Profile version 2.1 ohjeistuksen päivitykseen liittyvän lausuntopyynnön yhteenveto

1 212/2023 S Lausuntopyyntö

Oli lausuttavana 12.1.2023 - 26.2.2023 välisenä aikana lausuntopalvelu.fi:ssa,

<https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=da653d4f-9eae-4843-acee-ac3a2a350864> .

Lausuntopyyntö sisälsi liitteenä ohjeistuksen päivityksen siten, että muutokset edelliseen versioon olivat helposti havaittavissa.

Lausuntopyynnössä kysyttiin seuraavat kysymykset:

- 1) Onko SAML metadatojen vaihtamisen ja luottamuksen perustamisen periaatteen kuvaus riittävän selkeä?
- 2) Tuodaanko hyväksytyn sähköisen allekirjoituksen ja hyväksytyn sähköisen leiman hyöty SAML metadatan allekirjoituksessa selkeästi esille?
- 3) Mikä on arvionne mukaan sopiva SAML viestinnässä käytettäväksi avainten vaihtoväliksi?
- 4) Onko ehdotetut toimitavat sopivia luottamusverkoston välityspalvelun tarjoajalle (Policy 1, 2 ja 3)?
- 5) Onko ehdotetut toimitavat sopivia tunnistusvälineen tarjoajalle (Policy 1, 4, 5 ja 6)?
- 6) Anna tässä vapaamuotoinen palaute luonnoksesta (SAML).

2 Saadut vastaukset

Annettuun määräaikaan mennessä saatiin yksi vastaus Liikenne- ja viestintävirasto Traficomien kirjaamon kautta, jossa mukana oli tarkentavia kysymyksiä liittyen lausunnolla olevaan ohjeistukseen. Lausuntopalvelun kautta ei tullut lausuntoja.

Lisäksi yhdeltä SAMLia käyttävältä tunnistuspalvelun tarjoajalta varmistettiin, että lausuntopyyntö oli huomattu, eikä siihen ollut kommentoitavaa.

Saadusta yhdestä lausunnosta ilmeni, että luottamuksen perustamisen periaatteen kuvaus ja SAML metadatojen vaihtaminen ei ollut riittävän selkeä ja että hyväksytyn sähköisen allekirjoituksen sekä hyväksytyn sähköisen leiman hyöty SAML metadatan allekirjoituksessa eivät tulleet selkeästi esille.

3 Johtopäätökset annettujen vastauksen perusteella

Tekninen kyvykkyys SAML tietoliikenteen avainten vaihtamiseen katkotta on rajallinen. Osapuolet joutuvat sopimaan keskenään ajanhetken, jolloin vaihto tapahtuu kummallekin osapuolelle sopivana ajanhetkenä.

Traficom katsoo tämän vähäiseksi haitaksi ja kannustaa teknisen tuen lisäämistä tunnistusvälityspalveluiden ja tunnistusvälineen tarjoajien toteutuksiin siten, että SAML metadatatassa voidaan julkaista useampi SAML sanomien allekirjoitusvarmenne, joilla voidaan tarkistaa sanomien eheys ja alkuperä.

Muilta osin saatu vastaus ei antanut aihetta muuttaa ohjeistusta.