SAML-vastausviestien salaaminen muuttumassa pakolliseksi

Viimeaikainen keskustelu Shibboleth-konsortion postilistalla ja aiemmassa artikkelissa viitattu tietoturvasuositus ovat tuoneet uuteen valoon SAML-vastauksen salaamisen. Shibboleth IdP -ohjelmiston pääkehittäjä on esittänyt näkemyksen, että henkilötietojen suojaamiseksi ainoat riittävät vaihtoehdot ovat: tiedon siirtäminen taustakanavalla suoraan palvelimien välillä (artifact) tai autentikaatiovastauksen assertion salaaminen.

Tämä mielipide heijastelee jo saml2int-profiilin luonnoksessa, johon on kirjattu IdP-palvelimelle vaatimukseksi:

> *In the event the HTTP-POST binding [SAML2Bind] is used, assertions MUST be encrypted and transmitted via a <saml: EncryptedAssertion> element.*

Hakassa HTTP-POST on ainoa sallittu yhteystapa autentikaatiovastauksen välittämiseen. Nyt luonnoksena esitetty profiili edellyttäisi jatkossa Hakassa SAML-viestien salaamista. Jatkossa pelkkä HTTPS ei riittäisi viestien suojaamiseen.

Nykyisin Hakassa SP:n on tuettava salausta, eli pystyttävä avaamaan salattu SAML-viesti. Tästä syystä Hakassa SP:n on rekisteröitävä metadataan varmenne. IdP:lle SAML-viestien salaaminen on vapaaehtoista. Koska SP:lle kyky salauksen purkuun on pakollista, on ollut IdP:n valittavissa, salataanko viestit vai ei.

Vaikka Hakassa ei olisi palveluja, jotka eivät tue salausta, operoinnin tiedossa on, että käytössä on paljon tuotteita, joilla ei ole kykyä tukea salattuja SAML-viestejä. Hakaan liitetyillä IdP-palvelimilla voi olla kahdenvälisiä luottosuhteita tällaisille palveluille. Jos salaus Hakassa tulee pakolliseksi, IdP:n on luontevaa kytkeä salaus päälle kategorisesti kaikkien palvelujen osalta. IdP:n konfiguraatiossa on mahdollista tehdä poikkeussääntö ja jättää viestit salaamatta sellaisille palveluille, jotka salausta ei tue, jos se on organisaation toimintokäytänteiden mukaista.

Haka-operointi suosittaa jo etupainotteisesti kartoittamaan muutoksen vaikutuksia organisaation kertakirjautumiselle ja kytkemään SAML-viestien salauksen kategorisesti päälle IdP:palvelimella heti, kun mahdollista.

Lisätietoa:

- Shibboleth-postilistan keskustelu: https://marc.info/?t=151741666900001&r=1&w=2
- Saml2int-profiilin luonnos: https://kantarainitiative.github.io/SAMLprofiles/saml2int.html#_idp_requirements
- Aiempi tiedote SAML-viestien luottamuksellisuudesta: https://wiki.eduuni.fi/x/i4usAw

Briefly in english

Recent discussion implicates to encryption of SAML-assertions becoming mandatory in Haka. Please see relevant discussion in Shibboleth mailing list and the draft document for new version of saml2int-profile.

- Shibboleth mailing list: https://marc.info/?t=151741666900001&r=1&w=2
- Saml2int-profile draft: https://kantarainitiative.github.io/SAMLprofiles/saml2int.html#_idp_requirement