# Suomi.fi-tunnistus

Asiakasinfo 25.11.2020

DIGI- JA VÄESTÖTIETO-VIRASTO

# Agenda

- Asiakastestiympäristöön toteutetut muutokset
- SAML2 -varmenteen vaihto tuotantoympäristöön
- Algoritmit (mm. AES128-GCM) ja vastaussanomien salauksen pakotus
- Kertakirjautuminen (SSO) ja kertauloskirjautuminen (SLO) siirtymäaikana
- Tekninen dokumentaatio

- Kysymyksiä

# Asiakastestiympäristöön toteutetut muutokset

# 14.9.2020 Asiakastestiympäristön hyväksymät allekirjoitusalgoritmit muuttuivat

- Jos tunnistuksen asiakastestiympäristön (testi.apro.tunnistus.fi) käyttö estyi kyseisen päivämäärän jälkeen, todennäköisesti syy on, että tunnistukselle kohdistetussa pyyntösanomassa käytetään sha1:ta tai rsa-sha1:stä algoritmia.

- Vuonna 2021 näitä algoritmeja ei tulla hyväksymään tuotannossa AuthnRequest eikä LogoutRequest + LogoutResponse käyttötilanteissa.

# 15.10.2020 Tunnistusvastaus salataan aina

Salausalgoritmiksi vaihtui http://www.w3.org/2009/xmlenc11#aes128-gcm

Jos palvelu rikkoontui, toimimattomuuteen voi vaikuttaa:

- **Asiointipalvelun SAML2 SP metadatan rekisteröinnissä ei ole julkaistu varmennetta, jota voidaan käyttää vastaussanoman salaukseen**
  - Kirjaudu palveluhallinta.suomi.fi ja lataa asiointipalvelun XML metadata.
  - Jos löytyy use="signing" muttei use="encryption" Key element, niin kyse on tästä.
  - Huom! Jos tarkentavaa use -määritettä ei ole, niin Suomi.fi-tunnistus ymmärtää tämän niin, että samaa varmennetta tullaan käyttämään sanomien allekirjoituksien varmistamiseen, sekä paluuvastauksen suojaukseen/salaukseen.
  - Toimimattomuus näkyy yleensä ennen kuin tunnistusprosessia käynnistetään, selain ohjataan ’Jokin meni pieleen’ -virhesivulle.

- **Onnistuneen tunnistamisen jälkeen turvallisempaa allekirjoitusalgoritmia ei ole tuettu**
  - Tästä ei tule virheilmoitusta Suomi.fi-tunnistuksen puolesta, vaan kontrolli siirtyy asiointipalvelun puolelle henkilötietojen välistyssivun jälkeen.
  - Tarkista tukeeko käytetty SAML2 kirjasto AES128-gcm algoritmia, jos ei, niin ota yhteys tunnistuksen käyttöönottoihin.

# 3.11.2020 vaihdettiin SAML2-sanomien allekirjoitusvarmenne

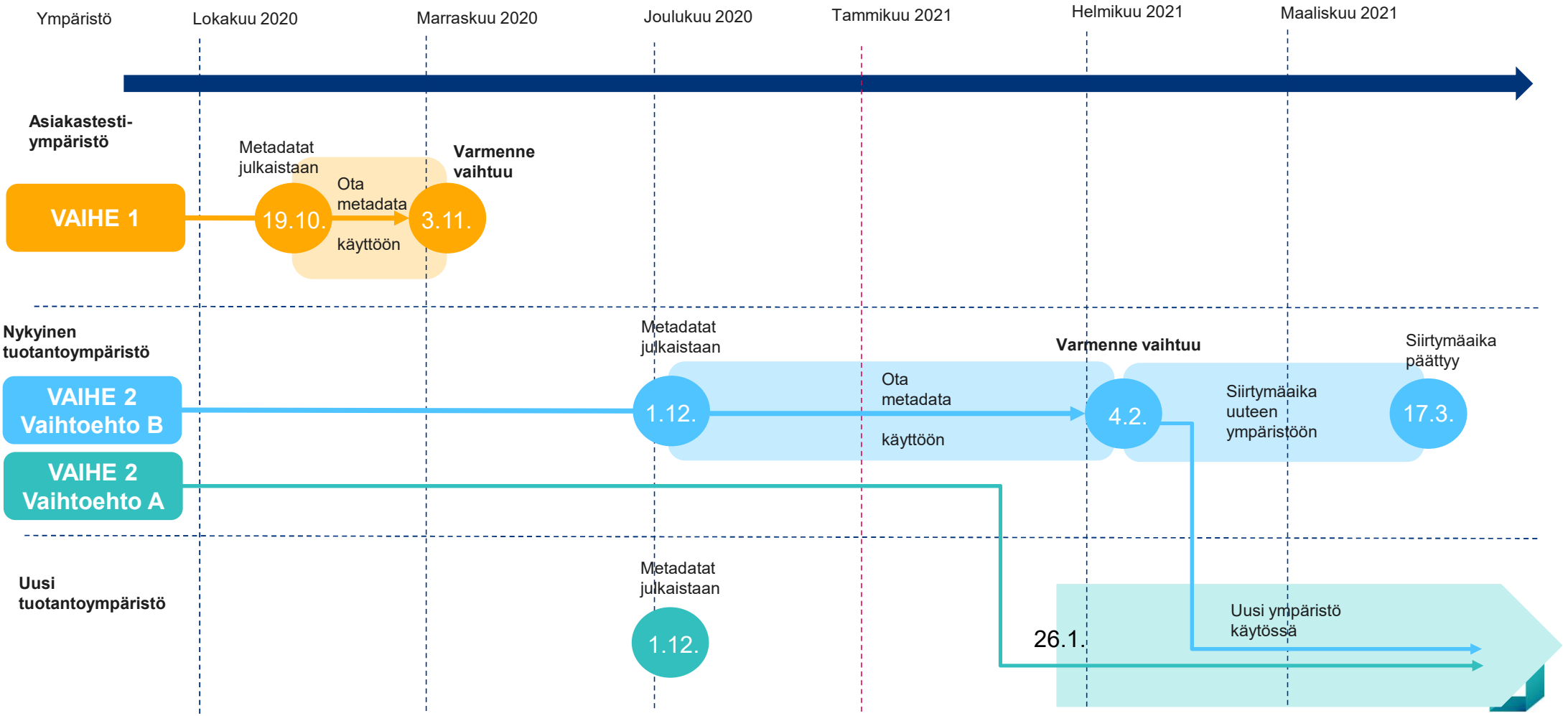
- Jos palvelu rikkoontui, vikana voi olla kyvyttömyys lukea dynaamisesti Suomi.fi-tunnistuksen idp-metadata.xml

  - Tarkista kyvykkyys lukea Suomi.fi-tunnistuksen idp-metadata.xml dynaamisesti etukäteen ilmoitetuista URLeista. Varmista kuitenkin, että kyseinen idp-metadata.xml -tiedosto on peräisin DVV:ltä.
  - Huomioi SAML2 IDP metadatojen allekirjoitusvarmenteen tunnistetiedot (SHA1 Fingeprint)

- Jos konfiguraatiota ja/tai vastaussanomien oikeellisuuden toteamiseen käytettyä varmennetta piti muuttaa asiointipalvelun puolella, varaa kalenterista torstai 4.2.2021 testaamiseen, toimiiko asiointipalvelusi tuotannossa klo 12 jälkeen.

# SAML2 -varmenteen vaihto tuotantoympäristössä

# Aikataulu


Ympäristö
Lokakuu 2020
Marraskuu 2020
Joulukuu 2020
Tammikuu 2021
Helmikuu 2021
Maaliskuu 2021
Asiakastesti-ympäristö
VAIHE 1
Metadatat julkaistaan
19.10.
Ota metadata käyttöön
Varmenne vaihtuu
3.11.
Nykyinen tuotantoympäristö
VAIHE 2 Vaihtoehto B
Metadatat julkaistaan
1.12.
Ota metadata käyttöön
Varmenne vaihtuu
4.2.
Siirtymäaika uuteen ympäristöön
Siirtymäaika päättyy
17.3.
VAIHE 2 Vaihtoehto A
Uusi tuotantoympäristö
Metadatat julkaistaan
1.12.
26.1.
Uusi ympäristö käytössä

# 1.12. julkaistavat idp-metadata.xml ja miten luen niitä?

Q: "--Onko Suomi.fi:n metadata sama vai eri vaihtoehdoissa A ja B?"

- idp-metadata.xml sisältää kummatkin ympäristöt SAML2 Metadata standardin mukaisesti ilmaistuna.


Vuonna 2021 poistuva ympäristö
Vaihtoehto B

Vaihtoehto A
Rinnalle tuleva uusi ympäristö v2021->

**Huom! <ds:Signature> -elementti piilotettu esimerkistä**

Q: Mitä tuotantoympäristön osalta tarkoittaa vaihtoehdon A toteamus: "SAML-varmennetta ei tarvitse vaihtaa"? Vaihtoehto B otsikko puolestaan mainitsee "SAML2-varmenteen" vaihdon. Mitä varmennetta tai metadataa SAML-varmenteella tarkkaan ottaen tarkoitetaan?

Jos valitset vaihtoehdon A, niin konfiguroit uuden Suomi.fi-tunnistus ympäristön ja otat sen käyttöön ennen 4.2.2021, niin tuotanto jatkuu ilman varmenteen vaihtoa.

Jos et ole saavuttanut esimerkiksi yhteensopivuutta asiakastestiympäristössä tai olet yrittänyt siirtyä käyttämään https://tunnistautuminen.suomi.fi/idp1 ympäristöä, mutta syystä tai toisesta yliheitto epäonnistui. Varaudu vaihtamaan Suomi.fi-tunnistuksen käyttämä SAML2 sanomien allekirjoitusvarmenne 4.2.2021, niin tuotanto käyttö voi jatkua siirtymäajan verran https://uusi.tunnistus.fi/idp1 -ympäristössä kunnes olet siirtynyt uuteen ympäristöön.

# IDP Metadatan allekirjoitusvarmenteiden tiedot

**Tuotanto (7.2.2021 saakka)**

**SUBJECT:**

CN = metadata-signing.tunnistus.suomi.fi,
serialNumber = 0245437-2,
O=Vaestorekisterikeskus,
L=Helsinki,
ST=Finland,
C=FI

**FINGERPRINT (SHA-1)**

F6:ED:3A:BE:1C:D5:54:55:80:DD:
C0:6A:FD:FC:AB:0C:B6:39:C1:43

**Asiakastesti (Voimassa 8.10.2022)**

**SUBJECT:**

CN = metadata-signing.apro.tunnistus.fi,
serialNumber = 0245437-2,
O=Digi- ja vaestotietovirasto,
L=Helsinki,
ST=FINLAND,
C=FI

**FINGERPRINT (SHA-1)**

FD:ED:55:48:FE:31:C3:0D:AF:9F:
13:37:C1:0A:40:A8:C7:86:AB:35

# Algoritmit ja vastaussanomien salauksen pakotus

# Algoritmit (mm. AES-GCM) ja vastaussanomien salauksen pakotus

Taustalla Traficomin linjaukset vuodelta 2018. Ohjeistus halutaan ottaa käyttöön Suomi.fi-tunnistuksessa ja huolehtia kansalaisten ajantasaisesta tietoturvallisuudesta.

- Kansalaisten selaimiin ja pelkästään TLS / HTTPS tietoliikenteen suojattuna pysymiseen ei voida luottaa.
- Yrityksien työasemille asennettu oma CA, jonka nimissä voidaan tekeytyä Suomi.fi-tunnistukseksi ja mahdollistaa täten HTTPS/TLS tietoliikennettä kuuntelevat järjestely
- Työasemille ja selaimiin asentuvat salakuuntelu- ja MITM hyökkäysvälineet.
- Eri asiointipalveluiden tietoliikenteen TLS asetuksissa vaihtelevuutta

→ SAML2 -vastaussanoman salaus pakotettu Suomi.fi-tunnistuksen toimesta

# Asiakaspalautteen perusteella kerätyt kokemukset, sanomien allekirjoitusalgoritmit

- Hyvin usein valmis SAML2 SP toteutus käyttää oletusarvoisesti http://www.w3.org/2000/09/xmldsig#rsa-sha1 allekirjoitusalgoritmia.

- Toisaalta voi käyttää http://www.w3.org/2000/09/xmldsig#sha1 DigestValuen tai SignatureValuen esittämiseen SAML2 sanomien allekirjoituksen yhteydessä.

- Nämä algoritmit ovat laitettu kiellettyjen listalle. Korvaavat vastineet ovat
  - #rsa-sha256 / #rsa-sha384 / #rsa-sha512
  - #sha256 / #sha384 / #sha512

# Asiakaspalautteen perusteella kerätyt kokemukset, AES128-GCM

**.Net**

- .Net 5.0 julkaistu, sisältää AES128-gcm tuen.
- .Net 4.x ja bountry castle kirjastolla saatu yhteensopiva AES128-GCM tuki räätälöityä

**Java**

- Java 7 ja Java 8, Ei vakiona tuettu AES128-GCM, mutta Bouncy Castlen kirjastolla yhteensopiva tuki.

**OpenSSL hyödyntävät SAML2 kirjastot**

- Tarkista, että käytät AES128-gcm tuellista kirjastoversiota

**SimpleSAMLphp**

- Tuki tulossa, https://github.com/simplesamlphp/saml2/issues/179

**Shibboleth SP, tuki olemassa**

# Mitä jos en ehdi saamaan AES128-GCM tukea valmiiksi 17.3. mennessä?

Q: voiko tunnistusvastauksen salausalgoritmin purkuun käyttää mitä tahansa tuetuista algoritmeista vai onko käytettävä nimenomaan aes128-gcm?

- Olemme tiedostaneet, että AES128-GCM tuen saaminen valmisratkaisuihin tai aikaisemmin julkaistuihin ohjelmistokirjastoihin on haasteellista.

- **Tämä takia tuemme AES128-GCM rinnalla nykyisin käytössä olevaa AES128-CBC:ta 2021/Q1 jälkeen.**
  - Jos asiointipalvelun omistaja ei reagoi, niin oletusarvoisesti uudessa ympäristössä asiointipalvelulle vastaussanomaan liittyvä Assertionin salaus tehdään AES128-GCM algoritmilla.
  - Muutosta CBC:hen voi koestaa jo nyt asiakastestiympäristössämme.

# Kertakirjautuminen (SSO) ja kertauloskirjautuminen (SLO) siirtymäaikana

# Kertakirjautuminen (SSO) ja Kertauloskirjautuminen (SLO) siirtymäajalla

- DVV tarjoaa asiointipalveluille siirtymäaikaa uuteen tuotantoympäristöön (26.1.-17.3.)
- Kertakirjautumis- sekä kertauloskirjautumistoiminnallisuus on molemmissa ympäristöissä
- Kertakirjautuminen tai kertauloskirjautuminen ei toimi ympäristöjen välillä
- Suosittelemme siirtymistä uuteen tuotantoympäristöön viivytyksettä sen avauduttua
- Teemme käyttöliittymään loppukäyttäjää ohjaavia päivityksiä siirtymäajalle

# Tekninen dokumentaatio

Q: Mistä löytyy, mitkä ovat relevantteja kohtia?

- suoralinkki: https://palveluhallinta.suomi.fi/fi/tuki/palvelut/tunnistus
- https://palveluhallinta.suomi.fi/ → Tuki ja asiakaspalvelu -> Tunnistus

- Ongelmissa tukee myös tunnistuksen käyttöönotot
  tunnistus-kayttoonotot@dvv.fi

# Kysymyksiä?

DIGI- JA VÄESTÖTIETOVIRASTO

dvv.fi