Aleksi Yrttiaho 8.6.2010

AvoHILMO 2011, versio 2.0

Sähköisen tiedonsiirron ohje

Periaatteet

- Kaikki arkaluonteinen ja henkilötunnuksellista tietoa sisältävä aineisto toimitetaan aina vahvasti salakirjoitettuna.
- Aineiston on oltava salakirjoitettuna koko toimitusprosessin ajan
- THL ottaa vastaan ainoastaan allekirjoitettuja aineistoja.
- Tiedonsiirtoratkaisuissa pyritään käyttämään standardeja, joiden avulla asiakasohjelmien ja reitityksen muodostus olisi mahdollisimman helppoa.
- Aineistojen toimitus ei ole kriittistä toimintaa: riittää, että aineisto saadaan jossain vaiheessa toimitetuksi
- Aineistoissa suositaan tiivistä päivitystahtia esimerkiksi kerran päivässä. Reaaliaikaisuutta ei vaadita.

Poimintatiedoston muodostus

Poimintatiedoston muodostuksessa noudatetaan AvoHILMO-oppaassa esitettyä määrittelyä.

Poimintatiedoston salakirjoitus

Poimintatiedostot sisältävät arkaluonteisia ja salassa pidettäviä tietoja. Tästä johtuen poimintatiedostot tulee salakirjoittaa aina ennen kuin ne toimitetaan THL:n.

AvoHILMOn salakirjoitustavaksi on valittu OpenPGP-standardi RFC 4880. Salaus perustuu julkiseen avaimeen, jonka avulla salattu tiedosto voidaan avata vain ja ainoastaan julkista avainta vastaavan salaisen avaimen avulla. Kullekin toimijalle muodostetaan OpenPGP-standardin mukaiset julkinen ja salainen avain. Toimijat jakavat keskenään julkiset avaimensa. Erityisesti poimintatiedoston salaava taho noutaa THL:n julkisen avaimen ja rekisteröi oman julkisen avaimensa THL:n.

Poimintatiedostojen salaukseen käytetään AES-256 salausalgoritmia. Avaimet ovat muodostettu 2048-bittisinä RSA-avaimina.

Salausprosessi:

1. Potilastietojärjestelmästä muodostetaan AvoHILMO-poimintatiedosto
2. Poimintatiedosto syötetään salausohjelmalle tai –komponentille
3. Salausohjelma tai -komponentti luo salakirjoitetun version poimintatiedostossa siten, että salausavaimena käytetään THL:n *julkista avainta*
4. Salausohjelma tai -komponentti luo allekirjoituksen poimintatiedostosta siten, että salausavaimena käytetään salaajan *salaista avainta*
5. Salakirjoitettu poimintatiedosto ja poimintatiedoston allekirjoitus toimitetaan THL:lle
6. THL:n vastaanottopalvelin purkaa salakirjoituksen oman salatun avaimensa avulla
7. THL:n vastaanottopalvelin tarkistaa poimintatiedoston allekirjoituksen salaajaan *julkisen avaimen* avulla

Huom. poimintatiedosto salakirjoitetaan kokonaisuudessaan; henkilötunnuksia tai muita kenttiä ei salakirjoiteta erikseen.

Salakirjoitetun poimintatiedoston toimitus

Poimintatiedostot voidaan toimittaa THL:lle automatisoidusti web-palvelun avulla. Web-palvelu on julkaistu WSDL-kuvauksena ja kommunikointi tapahtuu SOAP-protokollan mukaisesti. Palvelu ei ota kantaa siihen, mitä toimitettava aineisto sisältää.

Viestien reititykseen käytetään versiosta 1.0 lähtien WS-Addressing -spesifikaatiota. Tämän avulla voidaan määritellä viestin yksilöintitunnus, lähettäjä, kohde sekä reitityksen seuraava välietappi. WS-Addressing korvaa pilottivaiheessa käytössä olleen ad-hoc -ratkaisun.

Salakirjoitettu aineisto toimitetaan MTOM (Message Transmission Optimization Mechanism) -liitteenä. MTOM:n käyttö pienentää lähetettävien viestien kokoa, sillä ilman MTOM:a lähettävän aineiston koko kasvaa 33 %. Lisäksi MTOMin avulla aineisto voidaan toimittaa binäärivirtana (application/octet-stream), joka mahdollistaa viestien tehokkaamman käsittelyn.

Jotta MTOM toimisi mahdollisimman tehokkaasti, sen on oltava tuettuna kaikissa reitityksen osallistuvissa pisteissä. Lisäksi viestin toimitusta tulisi ohjeistaa siten, että SOAP viesti toimitetaan HTTP/1.1 -protokollan mukaisesti siten, että lähetys toimitetaan osissa (Chunked Transfer Coding, RFC 2616 3.6.1).

AvoHILMO-asiakasohjelma

THL on kehittänyt asiakasohjelman, joka sisältää salaus-, allekirjoitus- ja viestinvälitys-toiminnallisuuden. Aineistojen lähetys ei edellytä asiakasohjelman käyttöä. Ohjelma on julkaistu avoimen MIT-lisenssin mukaisesti; ohjelmaa voi käyttää ja laajentaa vapaasti. Sitä voi hyödyntää myös osittain esimerkiksi pelkkänä salausohjelmana.

Asiakasohjelma edellyttää

- Java 5 ympäristön tai uudemman
- Java Cryptographic Extensionin salausvahvuusrajausten poiston (JCE Unlimited Strength Jurisdiction Policy tiedostot ovat saatavilla Javan kotisivuilta)
- HTTP, HTTPS portin auki siten, että viesti voidaan lähettää THL:n tai johonkin välittävään palveluun
- Asiakasohjelmassa on lisäksi riippuvuus JAX-WS:n standarditoteutukseen. Tarvittaessa asiakasohjelmasta voidaan muodostaa versio, jossa tätä riippuvuutta ei ole vaan SOAP-viestit käsitellään Apache Axis 2 -kirjaston avulla.

Jos asiakasohjelmaa käytetään, kunkin toimittajan kohdalla on luotava asiakasohjelman asetustiedosto, jossa määritellään käytettävän OpenPGP-avaimen identiteetti ja salasana sekä minne aineisto lähetetään. Esimerkkiasetustiedosto ja sen muokkausohjeet toimitetaan asiakasohjelman yhteydessä. Käytettävä asetustiedosto on parametrisoitavissa, mikäli samasta asennuksesta lähetetään useita eri tyyppisiä tiedostoja.

Asiakasohjelma toimii komentorivillä. Ohjelman käyttöä varten on luotu komentosarjatiedostot client.bat ja client.sh, joiden avulla ohjelma voidaan ajaa kutsulla `client <lähetttävän aineiston nimi>`.

Asiakasohjelman kutsu johtaa seuraaviin askeleisiin

- Asiakasohjelma lukee viestinvälitysasetukset asetustiedostosta
- Jos määritellylle identiteetille ei ole avainnippua, asiakasohjelma luo identiteetille julkisen ja salaisen avaimen
- Jos THL:n julkista avainta ei ole julkisten avainten nipussa, asiakasohjelma rekisteröi lähettäjän julkisen avaimen THL:n ja noutaa THL:n julkisen avaimen
- Asiakasohjelma salakirjoittaa ja luo erillisen allekirjoituksen syötteeksi annetusta tiedostosta
- Jos ei ole erikseen kielletty, asiakasohjelma kutsuu SOAP-viestillä vastaanottopalvelua, joka on määritelty asetustiedostossa.

Asiakasohjelman ensimmäinen ajo kannattanee suorittaa siten, että SOAP-viestiä ei reititetä kolmannen osapuolen kautta. Avainten jakoa ei ole testattu reititetyn yhteyden ylitse eikä sen toimintaa voida tällaisessa tilanteessa taata.

Vastaanottorajapinta 1.0

Vastaanottorajapinnan versio 1.0 julkaistaan kesällä 2010. Vastaanottorajapinta ottaa vastaan lähetettyjä aineistoja sekä rekisteröi ja jakelee julkisia avaimia. Aineistot käsitellään asynkronisesti.

Tiedon toimitus

Palvelu tukee AvoHILMO -poimintatiedoston versioita 1.6, 1.7 ja 2.0.

https://www2.thl.fi/avohilmo/1.0/receive?wsdl

Pyyntö

Kenttä	Otsikko	Tyyppi	Selitys
submitter	kyllä	Merkkijono	Lähetettävän järjestelmän käyttötunnus, käytetään OpenPGP-identiteetin nimiä
content-type	kyllä	Merkkijono	Lähetettävän aineiston tyyppi, AvoHILMOssa käytettään "avohilmo/versio" esim "avohilmo/2.0"
signature	ei	64-kantainen lukuarvo	Aineiston OpenPGP:n mukainen allekirjoitus
attributes	ei	Merkkijono	Lista avain-arvo -pareja, joilla voidaan toimittaa sanomatason määreitä
content	ei	Binääriliite (application/octet-stream)	Varsinainen aineisto

Lisäksi WS-Addressing -spesifikaation mukaiset otsikkokentät ovat käytössä.

Content-type kentän tuetut arvot ovat

- http://thl.fi/avohilmo/1.6 - AvoHILMOn tietosisältöversio 1.6
- http://thl.fi/avohilmo/1.7 - AvoHILMOn tietosisältöversio 1.7
- http://thl.fi/avohilmo/2.0 - AvoHILMOn tietosisältöversio 2.0
- echo – Yhteyden tarkistusta varten

Vastaus

Vastausviestinä toimitetaan ServiceTicket-tyyppinen olio, jossa on seuraavat kentät

Kenttä	Otsikko	Tyyppi	Selitys
identifier	ei	Numero	Lähetetyn aineiston käsittelytunnus
state	ei	Enumeraatio	Lähetetyn aineiston tila (pending - otettu vastaan mutta ei käsitelty, completed - käsitelty, failed - epäonnistunut
message	ei	Merkkijono	Tilaa kuvaava viesti

Lisäksi WS-Addressing -spesifikaation mukaiset otsikkokentät ovat käytössä.

Virhetilanteet THL:n päässä

Virhetilanne	Syy	Toiminta
Palvelinta ei voida saavuttaa	THL:n vastaanottopalvelin tai edustapalvelin ei ole päällä tai verkkoliikenne ei pääse jostain muusta syystä perille.	Pidetään poimintatiedosto tallessa ja yritetään myöhemmin uudelleen esimerkiksi seuraavana päivänä
Proxy-virhe	Poimintatiedoston vastaanottoon on kulunut yli 20 minuuttia	Voidaan yrittää uudestaan. Pyritään pitämään lähetettävien viestien koot pienempinä
SOAP-virhe	Poikkeustilanne vastaanotossa johtuen joko virheellisestä viestistä tai jostain muusta tilasta	Tarkistetaan, että viesti on muodostettu oikein. Jos on, otetaan yhteyttä THL:n ja selvitetään, mistä on kyse
Failed-tila	Viestiä ei ole voitu ottaa vastaan syystä tai toisesta	Tarkistetaan tilaa kuvaava viesti, toimitaan viestin ohjeiden mukaisesti

Yhteyden tarkistus

Yhteyttä palvelimeen voi kokeilla echo-viestien avulla. Viesti, jonka content-type -kentän arvo on "echo", käsitellään siten, että lähetetty sisältö liitetään vastausviestin message-kentän arvoksi. Käsittely tehdään ajastetusti samalla tavalla kuin muiden viestien kanssa, joten vastaus ei ole välitön.

Yhteyden **tarkistusviesti ei saa sisältää arkaluonteista** sisältöä.

Käsittelytilan tarkistus

https://www2.thl.fi/avohilmo/1.0/receive?wsdl

Pyyntö

Kenttä	Otsikko	Tyyppi	Selitys
identifier	ei	Numero	Lähetetyn aineiston käsittelytunnus

Lisäksi WS-Addressing -spesifikaation mukaiset otsikkokentät ovat käytössä.

Vastaus

Vastausviestinä toimitetaan ServiceTicket-tyyppinen olio, jossa on seuraavat kentät

Kenttä	Otsikko	Tyyppi	Selitys
identifier	ei	Numero	Lähetetyn aineiston käsittelytunnus
state	ei	Enumeraatio	Lähetetyn aineiston tila (pending - otettu vastaan mutta ei käsitelty, completed - käsitelty, failed - epäonnistunut
message	ei	Merkkijono	Tilaa kuvaava viesti

Virhetilanteet THL:n päässä

Virhetilanne	Syy	Toiminta
Palvelinta ei voida saavuttaa	THL:n vastaanottopalvelin tai edustapalvelin ei ole päällä tai verkkoliikenne ei pääse jostain muusta syystä perille.	Pidetään poimintatiedosto tallessa ja yritetään myöhemmin uudelleen esimerkiksi seuraavana päivänä
Proxy-virhe	Poimintatiedoston vastaanottoon on kulunut yli 20 minuuttia	Voidaan yrittää uudestaan. Pyritään pitämään lähetettävien viestien koot pienempinä
SOAP-virhe	Poikkeustilanne vastaanotossa johtuen joko virheellisestä viestistä tai jostain muusta tilasta	Tarkistetaan, että viesti on muodostettu oikein. Jos on, otetaan yhteyttä THL:n ja selvitetään, mistä on kyse
Failed-tila	Viestiä ei ole voitu ottaa vastaan syystä tai toisesta	Tarkistetaan tilaa kuvaava viesti, toimitaan viestin ohjeiden mukaisesti

Lisäksi WS-Addressing -spesifikaation mukaiset otsikkokentät ovat käytössä.

OpenPGP-avainten rekisteröintipalvelu

https://www2.thl.fi/avohilmo/register?wsdl

Palvelun avulla voidaan rekisteröidä uusi OpenPGP-identiteetti ja sitä vastaava julkinen avain. Tätä palvelua käytetään vain kerran.

Pyyntö

Kenttä	Otsikko	Tyyppi	Selitys
identity	ei	Merkkijono	Salaajan OpenPGP-identiteetti
publicKey	ei	Merkkijono	Salaajan OpenPGP-julkinen avain

Vastaus

- Jos onnistuu niin THL:n julkinen avain
- Jos ei onnistu niin tyhjä merkkijono.

Mikäli rekisteröinti epäonnistuu, vastausviesti ei sisällä julkista avainta. Rekisteröinti voi epäonnistua jos

- Viesti on muodostettu väärin, esimerkiksi toinen tai molemmat parametreista puuttuvat
- Rekisteröitävä julkinen avain ei ole OpenPGP:n mukainen julkinen avain
- Samalla identiteetille on jo rekisteröity toinen OpenPGP:n mukainen julkinen avain
- Muu ennakoimaton virhe osuu kohdalle

Virhetilanteet THL:n päässä

Virhetilanne	Syy	Toiminta
Palvelinta ei voida saavuttaa	THL:n vastaanottopalvelin tai edustapalvelin ei ole päällä tai verkkoliikenne ei pääse jostain muusta syystä perille.	Pidetään poimintatiedosto tallessa ja yritetään myöhemmin uudelleen esimerkiksi seuraavana päivänä
Proxy-virhe	Poimintatiedoston vastaanottoon on kulunut yli 20 minuuttia	Voidaan yrittää uudestaan. Pyritään pitämään lähetettävien viestien koot pienempinä
SOAP-virhe	Poikkeustilanne vastaanotossa johtuen joko virheellisestä viestistä tai jostain muusta tilasta	Tarkistetaan, että viesti on muodostettu oikein. Jos on, otetaan yhteyttä THL:n ja selvitetään, mistä on kyse

Pilottivaiheen vastaanottorajapinta

Pilottivaiheen vastaanottorajapinta pysyy käytettävissä niin kauan kuin sen kautta toimitetaan aineistoja.

Tiedon toimitus

https://www2.thl.fi/avohilmo/receive?wsdl

Palvelun kautta voi toimittaa ainoastaan AvoHILMO 1.6 ja 1.7 poimintatiedostoja. Muita tiedostomuotoja ei tulla tukemaan. Mikäli sähköistä tiedonsiirto ei ole toteutettu aiemmin THL:n suuntaan, tämän rajapinnan käyttöönottoa ei suositella.

Tiedostomuoto esitetään version-kentässä. Ainoa sallittu arvo kentälle on 1.6, jonka perusteella otetaan vastaan AvoHILMO 1.6 ja 1.7 tietosisältömäärittelyjä noudattavia poimintatiedostoja.

Rajapinta ei toimi tyydyttävällä tavalla, jos lähetettävät aineistot ovat suuria.

OpenPGP-avainten rekisteröintipalvelu

https://www2.thl.fi/avohilmo/register?wsdl

Käytössä sellaisenaan rajapinnan versiossa 1.0.