Tieto Oyj
Tietokarhu Oy

v. 2.1

31.10.2019

Ilmoitin.fi – tunnelipalvelun tekninen kuvaus

1 Yleistä

Tässä dokumentissa on kuvattu Ilmoitin.fi-palveluun kuuluvan tunnelipalvelun tekninen toteutus. Dokumentin tarkoitus on auttaa tunnelipalvelua hyödyntäviä tahoja toteuttamaan lähettävässä päässä vaadittavat toiminnallisuudet.

Tunnelipalvelu on Ilmoitin.fi-palvelun Web Services -rajapintoja täydentävä kokonaisuus henkilöasiakkaiden ja henkilöyritysten ilmoitusten lähettämiseen. Lähettävällä verkkopalvelulla tarkoitetaan tässä yhteydessä Verohallinnon ulkopuolisen tahon verkkopalvelua, joka kytketään sovellus-sovellusrajapinnoilla Ilmoitin.fi-palveluun.

Tunnelipalvelun toiminnallisuutta ja käyttökelpoisuutta ei ole rajattu minkään tietyn toimijan tarpeisiin, vaan tunnelipalvelua voivat käyttää kaikki Verohallinnon hyväksymät toimijat. Tunnelipalvelun kautta voi lähettää tunnus:tieto-parimuotoisia tulovero-, vuosi- ja oma-aloitteisten verojen veroilmoituksia. Kiinteämittaisia tai XML-muotoisia ilmoituksia tunnelipalvelun kautta ei voi lähettää.

Tunnelipalvelun toimintaprosessi on kuvattu dokumentissa ”Ilmoitin.fi - Tunnelipalvelun toimintoprosessikuvaus”.

Tunnelipalveluun liittymisen helpottamiseksi on laadittu ns. referenssiclient Java-ohjelmointikielellä. Sitä voi käyttää sellaisenaan tai antamaan mallia omalle toteutukselle. Se löytyy osoitteesta www.ilmoitin.fi/kehittajat/Komponentit.

Jos on tarve lähettää ilmoituksia, jossa taho, josta ilmoitetaan, on yksilöity y-tunnuksella ja käytetään Katso-tunnisteita, siihen on tarjolla ApiTamo-rajapinta. ApiTamo-rajapinnasta löytyy lisätietoja osoitteesta www.ilmoitin.fi/kehittajat.

2 Tunnelipalvelun tekninen kuvaus

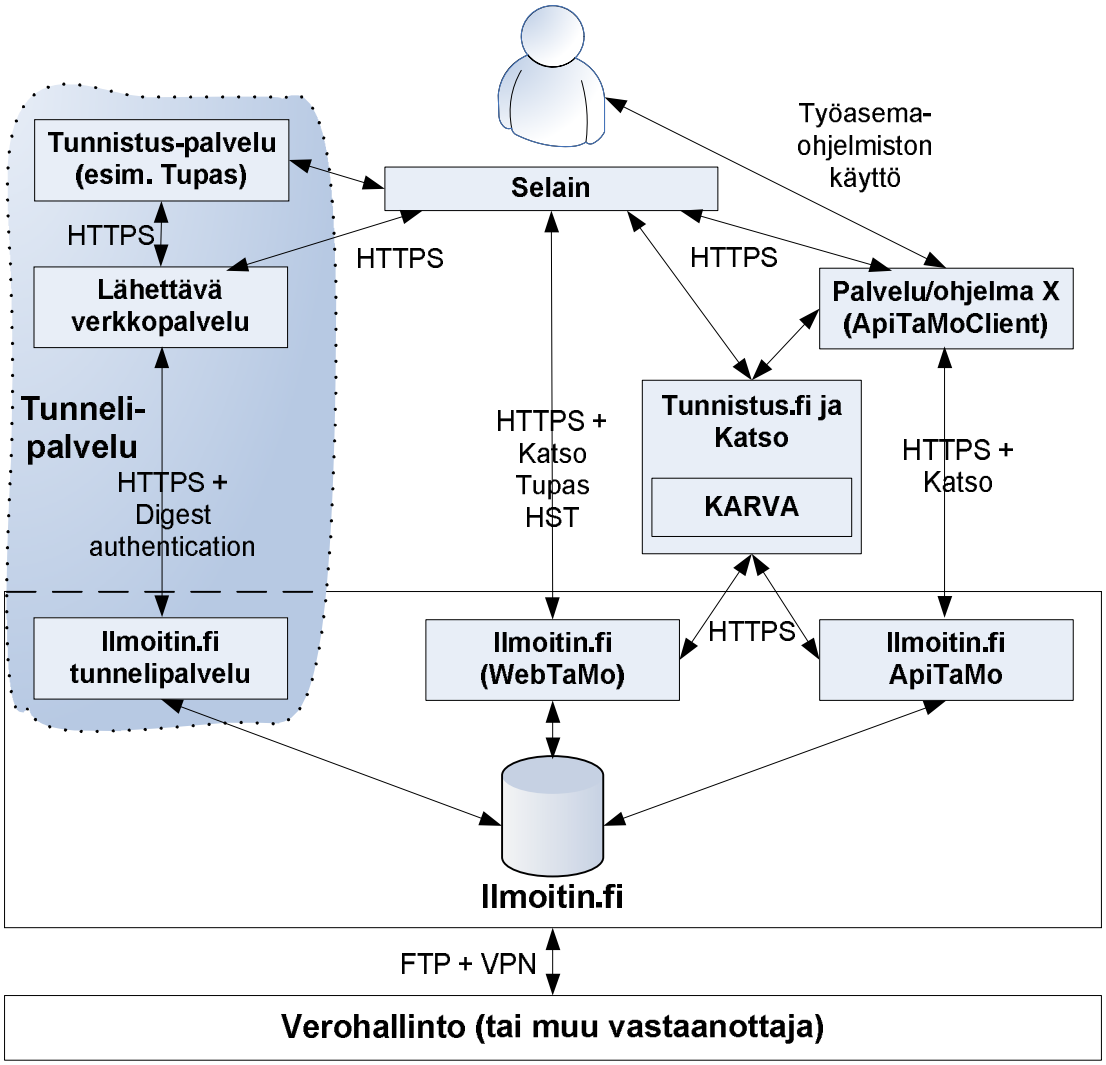
2.1 Yleiskuvaus

Tunnelipalvelu on tarkoitettu sellaisten verkkopalveluiden käyttöön, jossa kysymyksessä on henkilöasiakkaiden sähköinen ilmoittaminen.

Tunnelipalvelun suurin ero Ilmoitin.fi:n ApiTamo-rajapinnan kautta tapahtuvaan lähettämiseen on se, että loppukäyttäjä tunnistetaan lähettävän verkkopalvelun päässä eikä tunnistamisessa käytetä Katso-tunnisteita.

Seuraavassa kuvassa on Ilmoitin.fi:n palvelukokonaisuus, joka koostuu selainkäyttöisestä osuudesta (WebTaMo), Web Services -rajapinnasta (ApiTaMo) ja sinertävällä pohjalla olevasta tunnelipalvelusta.

Tunnelipalvelun tietoturvaa on käsitelty tarkemmin liitteessä 1.



Kuva 1. Ilmoitin.fi-palvelukokonaisuus ja tunnelipalvelu

Tunnelipalvelun toteutus perustuu siihen, että Verohallinto on hyväksynyt lähettävän verkkopalvelun ja luottaa siihen, että lähettävässä verkkopalvelussa loppukäyttäjä tunnistetaan riittävän vahvasti ja vaaditut tunnistautumistiedot välitetään Ilmoitin.fi-palveluun. Kysymyksessä on siis luottamukseen perustuva liittymä.

2.2 Tekninen ratkaisu

Tunnelipalvelu perustuu request-response -malliin, jossa käytetään SOAP-rakennetta (Simple Object Access Protocol). Lähettävä verkkopalvelu lähettää pyynnön (request) ja tunnelipalvelu vastaa siihen (response). Muuta ilmoitusliikennettä ei tarvita.

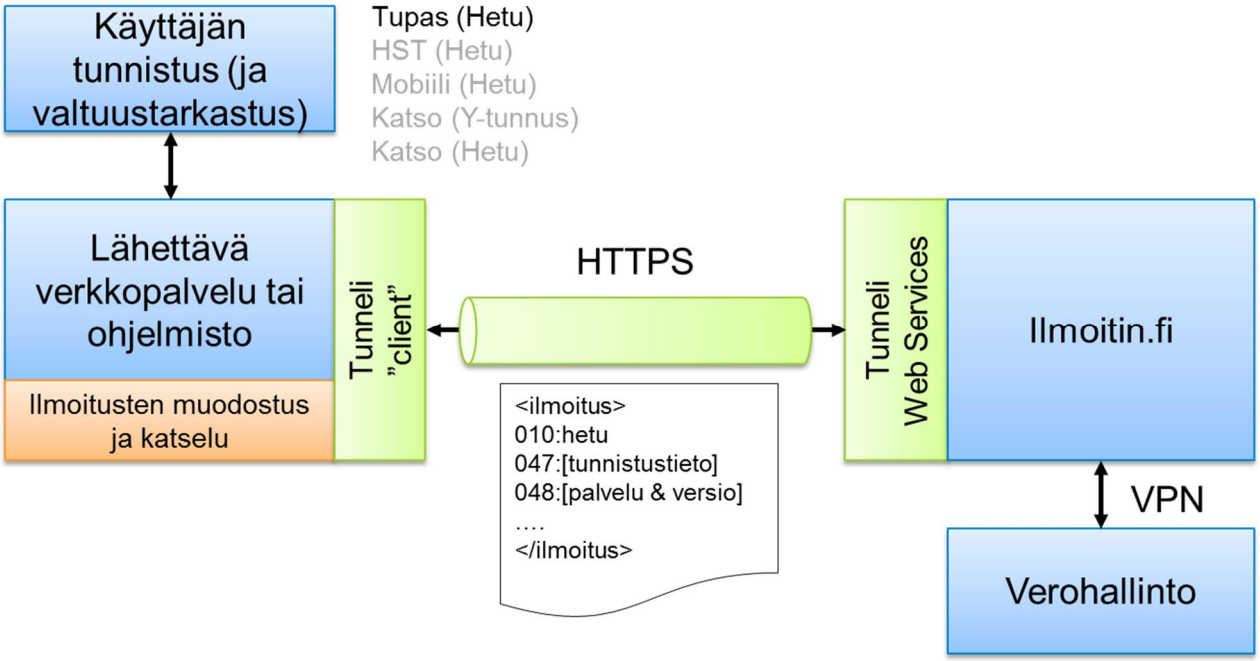
Ratkaisun ominaisuuksia:

- Kaikki tietoliikenne on https:ää lähettävän verkkopalvelun ja Ilmoitin.fi:n välillä
- Tunnelipalvelu näkyy julkisessa internetissä eikä Ilmoitin.fi:n päässä ei tarvita lähettäjäkohtaisia palomuuriavauksia

- Pyyntö ja vastaus ovat XML-muotoisia sanomia (SOAP)
- Lähettävä verkkopalvelu tunnistetaan käyttäjätunnuksen ja salasanan perusteella käyttäen http digest authentication:a RFC 2617:n mukaisesti
- Loppukäyttäjän tunnistus välitetään tunnelipalvelulle
- Lähettävän verkkopalvelun käyttäjätunnukset ja salasanat tallennetaan Ilmoitin.fi:ssä ei-selväkielisessä muodossa

Seuraavassa kuvassa on kuvattu tunnelipalvelun rakenne yleistasolla. Tunnelipalvelukokonaisuudessa on kolme osapuolta, jotka ovat:

- Ulkoinen tunnistuspalvelu, kuten verkkopankin tunnistuspalvelu
- Lähettävä verkkopalvelu, jossa ilmoitukset muodostuvat
- Varsinainen Ilmoitin.fi:n tunnelipalvelu



Kuva 2. Tunnelipalvelun periaatekuva

2.3 Lähettävän ohjelmiston/palvelun tunnistaminen

Jokaiselle tunnelipalvelua käyttävälle ohjelmistolle/palvelulle annetaan oma käyttäjätunnus, salasana ja kolminumeroinen koodi.

2.4 Loppukäyttäjän tunnistaminen

Tunnelipalvelun käyttö vaatii, että lähettävä verkkopalvelu lähettää tiedon loppukäyttäjän tunnistautumisesta. Tämä tieto on ilmoituksessa tunnuksessa 047 (Valtuutustieto). Valtuustieto on tieto loppukäyttäjän tunnistamisessa käytetystä tunnistusmenetelmästä.

Kentän arvoksi asetetaan lähettävässä verkkopalvelussa tunnistuspalvelusta saatu tunnistusmenetelmä, aikaleima, puolipiste (;) ja henkilötunnus tai y-tunnus. Tunnistuspalvelusta saatu

tieto käytetystä tunnistusmenetelmästä muutetaan kolminumeroiseksi Tupas-määrityksessä kuvatuksi koodiksi. Koodit on listattu Tupas 2.4 –määrityksen sivulla 10, luku 4.5 (http://www.finanssiala.fi/maksujenvalitys/dokumentit/Tupas_varmennepalvelu_V_2.4.pdf). Jos tunnistusmenetelmä on mobiilivarmenne tai sähköinen henkilökortti, asettakaa arvoksi 997. Jos tunnistuspalvelu ei välitä tietoa tunnistusmenetelmästä, käyttäkää arvoa 998.

Tunnelipalvelu tarkastaa, ettei aikaleima ole liian vanha. Aikaleiman voimassaoloaika on tietovirtasidonnainen ja se vaihtelee 8 tunnista 13 kuukauteen. Kysy asiasta lisää osoitteesta tamo.tk@vero.fi. Puolipisteen jälkeinen henkilötunnus on sama kuin varsinaisessa ilmoituksessa oleva henkilötunnus (tunnuksen 010 arvo esim. tulovero- ja kausiveroilmoituksissa).

Muut 047-tiedossa vaaditut tietoelementit saadaan OpenID Connect - ja SAML2-protokollista seuraavasti:

Tupas 2.4	**FTN/OpenID Connect**	**FTN/SAML2**
B02K_TIMESTMP	ID Token:n auth_time	NotOnOrAfter
B02K_CUSTID	urn:oid: 1.2.246.21	urn:oid: 1.2.246.21

Muuttakaa aikaleima Tupas-määrittelyn muotoon vvvvkkpphhmmssxxxxx.

Esimerkki, kun tunnistusmenetelmää ei voida yksilöidä: 9982019092408292675943 4;030680-XXXX
Esimerkki, kun tunnistusmenetelmä on 800 (Danske Bank): 8002019092408292675943 4;030680-XXXX

Lisätietoja tietoelementeistä:
Finnish Trust Network - OpenID Connect 1.0 Protocol Profile - version 1.0:
https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ftn_oidc_profile_v1.0_ficora_rec_213_2018_s.pdf

- välitettävät attribuutit: luku 4.1.1.1 Required attributes

Finnish Trust Network - SAML 2.0 Protocol Profile - version 1.0:
https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ftn_saml2_profile_v1.0_ficora_rec_212_2018_s.pdf

- välitettävät attribuutit: luku 3.4.1.1 Required attributes

2.5 Ohjelmistotiedon välittäminen (tunnus 048)

Tiedon 047 lisäksi tunnelipalvelu vaatii, että lähettävä verkkopalvelu välittää tunnelipalvelulle tiedon 048 eli aineiston muodostaneen ohjelmiston tai palvelun nimen ja version. Tätä tietoa tarvitaan mm. virheselvittelyä ja tilastointia varten.

Tieto muodostuu Verohallinnon lähettävälle palvelulle antamasta kolminumeroisesta koodista, puolipisteestä (;) ja ohjelmiston/palvelun nimestä ja versionumerosta. Kolminumeroinen koodi annetaan samassa yhteydessä kun lähettävä verkkopalvelu saa tunnelipalvelun käyttämisessä tarvittavan käyttäjätunnuksen ja salasanan.

Esimerkki 048-tunnuksen arvosta: `101;OhjelmistoX v. 1.51`

3 Tunnelipalvelun sanomat

3.1 Palvelun WSDL-kuvaus

Palvelun WSDL-kuvaukset löytyvät seuraavista osoitteista:

- testiympäristö: https://testi.ilmoitin.fi/ws/Tunneli?wsdl
- tuotantoympäristö: https://www.ilmoitin.fi/ws/Tunneli?wsdl

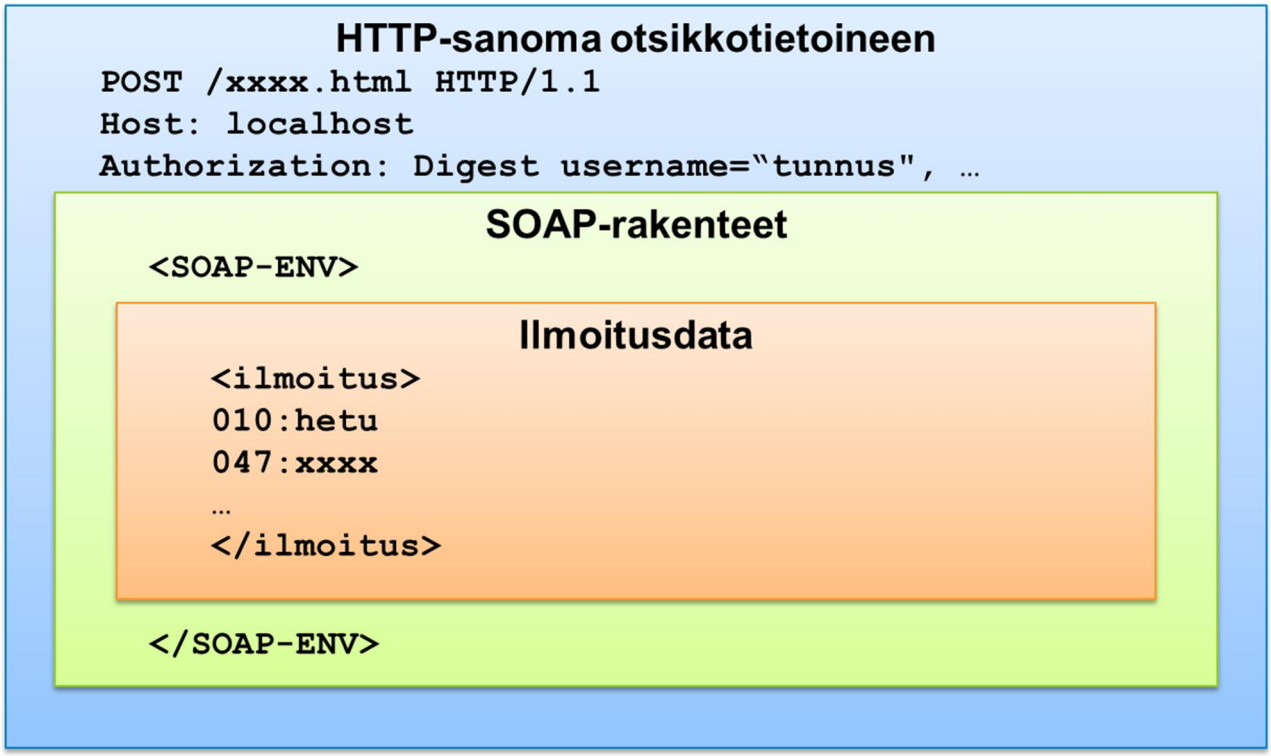
Huom! Kuormantasaajasta johtuen WSDL-tiedoston lopussa olevan address-elementin location-attribuutin arvo palautuu virheellisesti http-alkuisena vaikka sen pitäisi olla https-alkuinen. Samasta syystä myös WSDL-tiedoston tarkastustuloksen skeeman import-lause epäonnistuu. Nämä on muutettava käsin, jotta WSDL vastaa todellisuutta.

Tarkastustuloksen skeemat löytyvät seuraavista osoitteista:

- testiympäristö: https://testi.ilmoitin.fi/ws/Tunneli?xsd=../xsd/TamoTulos.xsd
- tuotantoympäristö: https://www.ilmoitin.fi/ws/Tunneli?xsd=../xsd/TamoTulos.xsd

3.2 Sanomaliikenne

Tunnelipalvelun sanomaliikenteessä protokollapino on esitelty kuvassa 3.



Kuva 3. Sanomaliikenteen protokollapino

Alimmalla tasolla on https ja siinä tarvittavat header-tiedot, joista keskeisimpänä http digest authentication:n käyttämä authorization-tieto. Https:n yläpuolella on SOAP-rakenteet. Varsinainen ilmoitus on yhtenä elementtinä SOAP-rakenteessa (ilmoitus-elementti).

Seuraavassa on yleisluontoiset esimerkit XML-sanomista (pyyntö ja vastaus). Tarkemmin sanomista voi lukea tunnelipalvelun toimintaprosessin kuvauksesta.

Karkea malli lähettävän verkkopalvelun pyyntösanomasta:

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:SOAP-ENC=http://schemas.xmlsoap.org/soap/encoding/
xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <SOAP-ENV:Body>
    <m:parseData xmlns:m="http://www.vero.fi/xmlschema/ApiTaMo">
      <Ilmoitus>[varsinainen ilmoitus tunnus:tieto-pari tai kiinteämittaisessa muodossa]</Ilmoitus>
      <Kieli>[vastauksen kielisyys: arvo FI,SV tai EN)]</Kieli>
      <Vastaanotto>TRUE</Vastaanotto>
    </m:parseData>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Karkea malli tunnelipalvelun vastaussanomasta:

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
    <Vastaus>
      <TamoTulos>
        <TarkistuksenTulos korjaamo="0" oikeellisia="1" tietuekpl="1" virheellisia="0">Ok</TarkistuksenTulos>
          <Lomake
            asiakas="[hetu tai y-tunnus]"
            nimi="[lomaketunnus esim. VSY02C16]"
            selite="[lomakkeen selväkielinen nimi, esim. Metsätalouden veroilmoitus]"
            tila="[kyseisen lomakkeen tarkastuksen tila, joko Ok tai False]"
            vuosi="[mitä vuotta ilmoitus koski, esim. 2016. Tyhjä jos vuosiriippumaton ilmoituslaji]"/>
      </TamoTulos>
      <Vastaanotto>TRUE</Vastaanotto>
      <Info/>
      <Aika>[vastaanottoaika, esim. 23.09.2016 10:41:39.180]</Aika>
      <Tarkistussumma>[esim. B85577DACC4BC2305DFFFB4EDA52327EAE8D2734]</Tarkistussumma>
    </Vastaus>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Sanoma, jossa tunnelipalvelu vaatii autentikointia:

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Header />
  <SOAP-ENV:Body>
    <SOAP-ENV:Fault>
      <faultcode>SOAP-ENV:client</faultcode>
      <faultstring>401 Unauthorized</faultstring>
    </SOAP-ENV:Fault>
```

```
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Ilmoituksen merkistönä käytetään Verohallinnon tietuekuvauksissa ilmoitettua merkistöä eli ISO-8859-1:stä.

Vastausviestin tietosisällön tarkempi kuvaus löytyy dokumentista ”Ilmoitin.fi - Tunnelipalvelun toimintoprosessikuvaus”.

4 Tunnelipalvelun käyttöönotto

Käyttöönoton tiimoilta ole yhteydessä osoitteeseen tamo.tk@vero.fi. Täältä saat tunnukset testiympäristöön.

Kun lähettävä palvelu on testattu testiympäristössä, Tietokarhu muodostaa Verohallinnon luvalla tunnukset tuotantoympäristöön. Tämän jälkeen tuotantokäyttö voi alkaa.

5 Linkkejä ja lisätietoja

Ilmoitin.fi - Tunnelipalvelun toimintoprosessikuvaus

Ilmoitin.fi-palvelu: www.ilmoitin.fi

Ilmoitin.fi-palvelun testipalvelu: https://testi.ilmoitin.fi

Ilmoitin.fi-palvelun kehittäjäsivusto: https://www.ilmoitin.fi/kehittajat

HTTP Digest access authentication: http://en.wikipedia.org/wiki/Digest_access_authentication

RFC 2617 - HTTP Authentication: Basic and Digest Access Authentication: http://www.ietf.org/rfc/rfc2617.txt

Tupas 2.4 -palvelukuvaus: http://www.finanssiala.fi/maksujenvalitys/dokumentit/Tupas_varmennepalvelu_V_2.4.pdf

Verohallinnon ilmoitusten tietuekuvaukset: http://www.vero.fi/fi-FI/Syventavat_veroohjeet/Sahkoinen_asiointi/Kehittajat/Tietuekuvaukset

Liite 1: Tunnelipalvelun tietoturvallisuus

Ilmoitin.fi:n tunnelipalvelun tietoturva perustuu useaan eri tekijään. Ensimmäisenä on rajapinnan luvanvaraisuus: rajapintaa ei voi käyttää ellei Verohallinto anna siihen lupaa ja toimita lähettävälle verkkopalvelulle käytössä tarvittavia tunnistetietoja. Toisena ovat normaalit, jo Ilmoitin.fi:ssä olevat laitteistoihin ja tietoliikenteeseen liittyvät tekijät. Kolmantena tätä rajapintaa koskevat tekijät. Tässä tärkeimpänä on lähettävän verkkopalvelun tunnistaminen.

Käyttäjätunnus ja salasana on yksinkertainen ratkaisu, joka kuitenkin tarjoaa riittävän turvatason kun käytetään tietoliikenteen suojaamiseen https:ää ja riittävän pitkiä salasanoja (esim. yli 10 merkkiä sisältäen numeroita ja erikoismerkkejä). Lähettävän verkkopalvelun tunnistamisessa käytettävä käyttäjätunnus ja salasana ovat voimassa määräajan ja salasana uusitaan esim. kerran vuodessa.

Teknisen ratkaisun osalta lähettävän verkkopalvelun tunnistaminen perustuu tekniikan osalta HTTP Digest access authentication:iin (RFC 2617), joka on laajemmin käytettyä HTTP Basic authentication:a turvallisempi johtuen siitä, että salasanan sijaan tunnelipalvelulle välitetään salasanan tiiviste.

Tieto (tunnus 047) loppukäyttäjän tunnistautumisesta ja siinä käytetystä tunnistusmenetelmästä (vrt. KatsoID:n lisääminen aineistoon) välitetään lähettävästä verkkopalvelusta Ilmoitin.fi:lle ja tieto säilytetään mm. virhetilanteiden selvittelyä varten.

Rajapinnan käytöstä kirjoitetaan lokia, josta selviää mm. mistä verkkopalvelusta ilmoituksia on lähetetty, kuka on lähettänyt ja mihin aikaan.

http digest authentication tarkemmin

Tunnelipalvelun http digest authentication on toteutettu noudattaen RFC 2617:ää, josta kannattaa katsoa tarkka kuvaus toiminnasta ja käytettävistä attribuuteista.

Kun client pyytää palvelua, tunnelipalvelu lähettää seuraavan vastauksen:

```
WWW-Authenticate: Digest realm="www.ilmoitin.fi/ws/Tunneli",
qop="auth",
nonce="1326976543429:daf5a365c3e4240cdf447b116b5d117f",
opaque="D510EB0E955DEC60B736981D727D4181"
```

Client vastaa seuraavasti:

```
Authorization: Digest username="tunnus", realm="www.ilmoitin.fi/ws/Tunneli",
nonce="1326976543429:daf5a365c3e4240cdf447b116b5d117f",
uri="/ws/Tunneli",
response="6f994e0f69f510042323d386f7e1bbe5",
opaque="D510EB0E955DEC60B736981D727D4181",
qop=auth,
nc=00000001,
cnonce="5dcb2ca7401522e6"
```

qop = ”Quality of protection” kertoo tunnistuksen tason. qop:n arvo on aina ”auth”.

nonce = client-sovellus palauttaa nonce-attribuutin sellaisenaan takaisin palvelimelle.

Response-attribuutin arvo muodostuu seuraavasti:

```
a1Md5 = md5Hex(username + ":" + realm + ":" + password)
a2Md5 = md5Hex(httpMethod + ":" + uri)
response = md5Hex(a1Md5 + ":" + nonce + ":" + nc + ":" + cnonce + ":"
+ qop + ":" + a2Md5)
```

opaque = client-sovellus palauttaa opaque-attribuutin sellaisenaan takaisin palvelimelle.

nc = laskurin arvo siitä kuinka monta pyyntöä client on lähettänyt samalla nonce-attribuutin arvolla.

Jos nonce ei ole enää voimassa (voimassaoloaika on 5 minuuttia), tunnelipalvelu asettaa stale-attribuutin arvoksi true ja serveri vastaa ”401 Unauthorized”. http header on tässä tapauksessa seuraavanlainen:

```
Digest realm="www.ilmoitin.fi/ws/Tunneli",
qop="auth",
nonce="MTMyNTc1MjQyMDY5MDpmNDFlMmE0NzQ0NWVkODRjZDViMzBiM2JiNmZhOGM0Ng==",
stale="true"
```

Client-toteutukseen mallia saa esim. tunnelipalvelun referenssiclient:sta tai Apachen HttpClient-toteutuksesta (http://hc.apache.org/httpcomponents-client-ga/index.html), joka toteuttaa Javalla RFC 2617 mukaisen http digest authentication:n.