Versio 1.04

Varmennepalvelu – Yleiskuvaus

Tulorekisteriyksikkö

Versiohistoria

Versio	Päivämäärä	Kuvaus
1.0	30.10.2017	Dokumentti julkaistu.
1.01	15.12.2017	Dokumenttia päivitetty kohdista: 2. Sanasto ja lyhenteet, 3.1 Uuden varmenteen pyytäminen, 3.3. Varmenteiden elinkaari ja uusiminen, 3.4. Virhetilanteet, 4. Varmenteiden käyttö tulorekisterin SFTP-kanavassa, 5 Palvelun testaus. Aikaisempi kappale 3 Palvelun käyttöoikeus ja käytöstä sopiminen on poistettu.
1.02	16.10.2018	Dokumenttia päivitetty kohdista: 1. Johdanto, 3. Varmennepalvelu, 3.4 Varmenteiden elinkaari ja uusiminen, 4. Varmenteiden käyttö tulorekisterin teknisissä rajapinnoissa, 4.1 Web Service -kanava, 4.2 SFTP-kanava Lisätty: 3.1 Varmennetyypit
1.03	10.4.2019	Dokumenttia päivitetty kohdista: 3. Varmennepalvelu, 3.1 Varmenteen tyypit, 3.2 Uuden varmenteen pyytäminen, 3.4 Varmenteiden elinkaari ja uusiminen, 3.5 Virhetilanteet, 4. Varmenteiden käyttötulorekisterin teknisissä rajapinnoissa, 5. Palvelun testaus.
1.04	20.1.2020	Dokumenttia päivitetty kohdasta: 3.4 Varmenteiden elinkaari ja uusiminen

SISÄLLYS

1 JOHDANTO

Varmennepalvelua hyödyntävät organisaatiot, jotka toimittavat aineistoja tulorekisteriin tai noutavat aineistoja tulorekisteristä teknisten rajapintojen kautta. Tulorekisterin teknisen rajapinnan kanavat ovat SFTP-kanava ja Web Service -kanava. Varmenne myönnetään organisaatiolle, joka vastaa tietojen toimittamisesta tulorekisteriin tai jolla on oikeus saada tietoja tulorekisteristä. Tulorekisterin varmennepalvelu myöntää varmenteet.

Dokumentin tarkoituksena on kuvata tulorekisterin varmennepalvelu yleisellä tasolla. Varmenteen pyytämiseen, hakuun ja uusimiseen käytettävät tekniset toiminnallisuudet ja skeemat on kuvattu erillisessä dokumentissa Varmennepalvelu – Rajapintakuvaus.

2 SANASTO JA LYHENTEET

Palvelukuvauksessa käytetyt lyhenteet ja tärkeimmät termit on esitetty taulukossa 1.

Lyhenne tai termi	Selite
CSR (Certificate Signing Request) varmenteen allekirjoituspyyntö	Varmennepalvelun käyttäjän tekemä varmennepyyntö. Varmennepyyntö on PKCS#10-muotoinen Base64-koodattu merkkijono.
Julkisen avaimen menetelmä	Epäsymmetrinen salaus, jossa toinen salausavaimista on julkinen avain ja toinen on yksityinen avain.
PKCS#10 (Public Key Cryptography Standards # 10)	Standardi, joka määrittää varmenteen allekirjoituspyynnön muodon ja sisällön.
PKI (Public Key Infrastructure)	Julkisen avaimen menetelmää hyödyntävä järjestelmä, jolla varmentaja tarjoaa ja ylläpitää varmenteita.
Private key (Yksityinen avain)	Salassa pidettävä osa epäsymmetrisestä avainparista, jota käytetään julkisen avaimen salauksessa. Yksityistä avainta käytetään tyypillisesti sähköiseen allekirjoittamiseen tai julkisella avaimella salatun viestin avaamiseen.
Public Key (Julkinen avain)	Julkinen osa epäsymmetrisestä avainparista. Julkista avainta käytetään tyypillisesti viestin salaamiseen ja yksityisellä avaimella suoritetun allekirjoituksen todentamiseen.
Rajapinta	Standardin mukainen käytäntö tai yhtymäkohta, joka mahdollistaa tietojen siirron laitteiden, ohjelmien tai käyttäjän välillä.
RSA-salaus	Rivestin, Shamirin ja Adlemanin kehittämään salausalgoritmiin perustuva julkisen avaimen menetelmä
SFTP (Secure File Transfer Protocol)	Tiedonsiirtoprotokolla, joka mahdollistaa salatun tiedonsiirtoyhteyden kahden järjestelmän välillä.
SGML (Standard Generalized Markup Language)	Merkintäkieli, jota käytetään aineiston eri osien ja niiden välisten suhteiden merkitsemiseen.
Tiedon käyttäjät	Sellaiset toimijat, joilla on lainsäädäntöön perustuva oikeus saada tulorekisteristä tulo- tai muita tietoja oman tehtävänsä hoitamiseen. Ensimmäisessä vaiheessa 1.1.2019 lähtien tiedon käyttäjiä ovat Verohallinto, Kela, Työllisyysrahasto sekä työeläkelaitokset ja ETK. Toisessa vaiheessa 1.1.2020 lähtien tiedon käyttäjiä ovat lisäksi mm. Tilastokeskus, Työllisyysrahasto (aikuiskoulutusetuudet), vahinkovakuuttajat, työttömyyskassat, TEMin hallinnonala, kunnat ja työsuojeluviranomainen.
Tiedon tuottajat	Kaikki yritykset ja muut toimijat, joilla on palkka-, eläke- tai etuustietojen ilmoitusvelvollisuuksia Suomeen jollekin tulorekisterin tiedon käyttäjälle.
WS (Web Service)	Verkkopalvelimessa toimiva ohjelmisto, joka tarjoaa standardoitujen internetyhteyskäytäntöjen avulla palveluja sovellusten käytettäväksi. Varmennepalvelun tarjoamia palveluja ovat varmenteen pyyntö, haku ja uusiminen.
XML (Extensible Markup Language)	SGML-kielestä erityisesti internetkäyttöä varten rajattu merkintäkieli, joka on helposti laajennettavissa.
XML Signature (allekirjoitus)	Asiakkaan voimassaolevalla varmenteella muodostama XML-allekirjoitus.
X.509	Varmenteen rakenteen määrittelevä standardi.

Taulukko 1. Käytetyt lyhenteet ja tärkeimmät termit.

3 VARMENNEPALVELU

Tulorekisterin varmennepalvelu perustuu PKI-ratkaisuun (Public Key Infrastructure). Varmennepalvelussa asiakkaalla on yksi tai useampi avainpari (yksityinen ja julkinen avain) ja avainpariin liittyvä varmenne, joka on X.509-standardin mukainen.

Asiakas tilaa varmenteen tulorekisterin varmennepalvelusta, ja varmennepalvelu myöntää sen. Varmennetta käytetään asiakkaan tunnistamiseen ja tulorekisteriin toimitettavan aineiston allekirjoittamiseen sähköisellä allekirjoituksella (XML Signature) tulorekisterin teknisissä rajapinnoissa. Varmenteet myönnetään tiettyyn käyttötarkoitukseen tietylle asiakkaalle, eikä niitä voi käyttää alkuperäisestä poikkeavaan tarkoitukseen. Varmenteen käyttäjän on hyväksyttävä ja noudatettava Verohallinnon ja tulorekisterin rajapintapalveluiden käyttöehtoja (pdf).

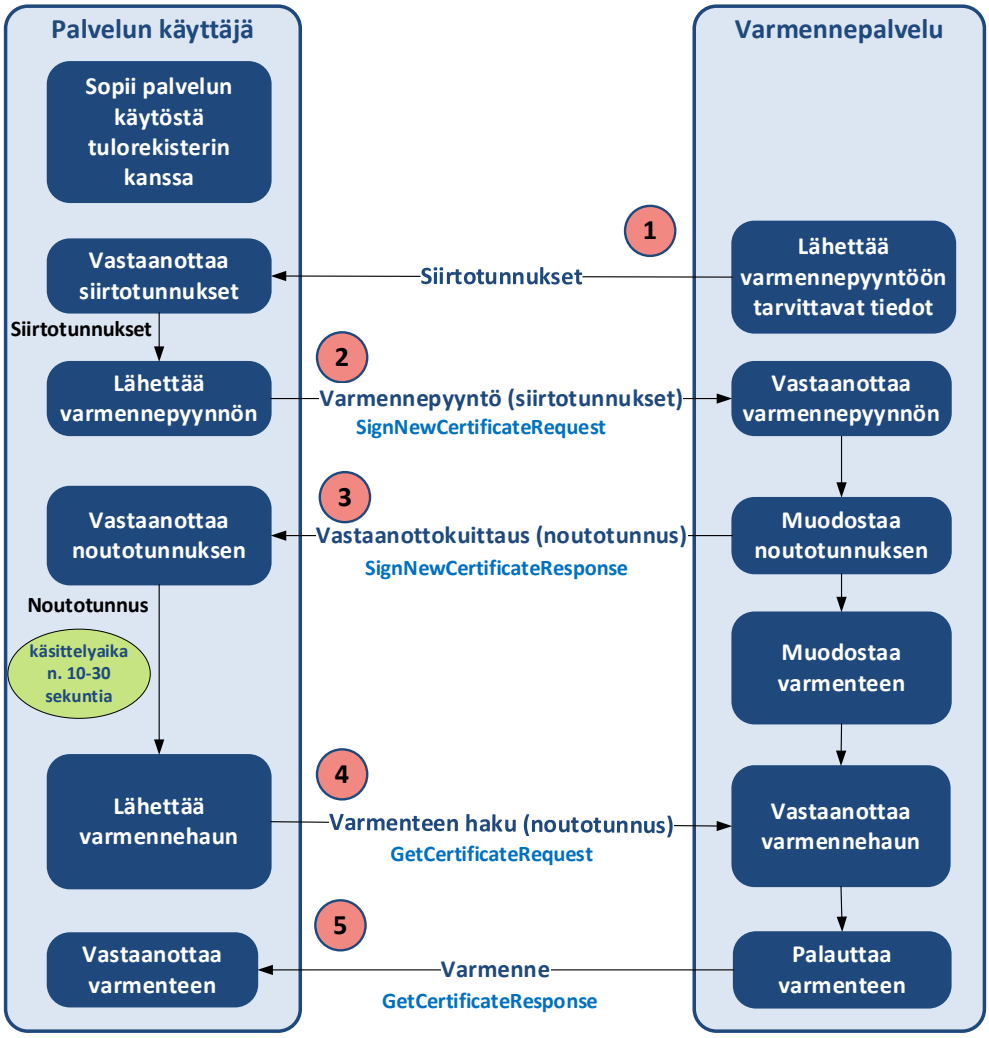
Jos tulorekisterin palveluiden käyttäjä toimii sekä palkka- tai etuustiedon tuottajana, että tiedon käyttäjänä, pitää eri käyttötarkoituksiin tilata eri varmenteet. Jos asiakas käyttää sekä teknisen rajapinnan SFTP- että Web Service -kanavaa, pitää myös silloin tilata varmenteet eri kanaviin. Varmenteita voi siis olla useampia yhdellä toimijalla. Jos asiakas käyttää useampia eri käyttötarkoituksiin ja kanaviin tarkoitettuja varmenteita esimerkiksi samassa ohjelmistossa, varmenteiden hallintaan pitää kiinnittää erityistä huomiota.

3.1 Varmenteen tyypit

Rooli	Kanava	Varmenteen julkaisija
Palkkatiedon tuottaja	Web Service	Data Providers Issuing CA
	SFTP	Data Providers SFTP Issuing CA
Etuustiedon tuottaja	Web Service	IR Benefit Data Providers Issuing CA
	SFTP	IR Benefit Data Providers SFTP Issuing CA
Tiedon käyttäjä	Web Service	IR Income Data Users Issuing CA
	SFTP	IR Income Data Users SFTP Issuing CA
Tulorekisterin ulkopuoliset tukipalvelut	Web Service	IR External Data Providers Issuing CA
	SFTP	IR External Data Providers SFTP Issuing CA

3.2 Uuden varmenteen pyytäminen

Uuden varmenteen pyytäminen ja varmenteen noutaminen on esitetty kuvassa 1.



Kuva 1. Uuden varmenteen pyytäminen ja noutaminen.

Tiedon tuottamiseen tarvittavien teknisten rajapintojen käyttöoikeudet haetaan tulorekisterin sähköisessä asiointipalvelussa. Kun organisaatio tekee hakemuksen teknisen rajapinnan käyttöönottamiseksi, se hyväksyy Verohallinnon ja tulorekisterin rajapintapalveluiden käyttöehdot. Hakemus käynnistää varmennetilauksen. Tiedon käyttämiseen tarvittavat teknisen rajapinnan käyttöoikeudet haetaan täyttämällä tulorekisterin tiedon käyttäjän ilmoitus tietolupaa varten.

Varmennepalvelu lähettää asiakkaalle varmennepyynnön tekoa varten tarvittavat tiedot: siirtotunnuksen (TransferId) ja kertakäyttösalasanan (TransferPassword). Asiakas voi tehdä varmennepyynnön sen jälkeen, kun on vastaanottanut varmennepyyntöä varten lähetetyn siirtotunnuksen ja kertakäyttösalasanan. Kertakäyttösalasana on voimassa 14 vuorokautta.

- Jos varmennepyyntöä ei tehdä tämän ajan kuluessa, kertakäyttösalasana vanhenee, ja asiakkaan on tehtävä uusi hakemus rajapinnan käyttöönottamiseksi.

- Siirtotunnus ja kertakäyttösalasana toimitetaan varmenteen tekniselle yhteyshenkilölle turvasähköpostiviestillä, jonka avaamista varten asiakas saa tekstiviestillä koodin.

Asiakas muodostaa varmennepyyntöä varten RSA-algoritmilla muodostetun 2048-bittisen avainparin. Lisäksi asiakas muodostaa PKCS#10-määrityksen mukaisen varmenteen allekirjoituspyynnön (Certificate Signing Request, CSR), joka sisältää asiakkaan julkisen avaimen.

Varmennepyynnön palvelukutsuun liitetään muodostettu allekirjoituspyyntö. Lisäksi pyynnön yksilöimiseksi ja suojaamiseksi palvelukutsuun liitetään asiakkaalle erikseen toimitettu siirtotunnus ja kertakäyttösalasana. Varmennepyynnön palvelukutsu palauttaa vastaanottokuittauksessa noutotunnuksen, jolla yksilöidään varmennepyynnön palaute ja onnistuneen pyynnön yhteydessä luotava varmenne hakua varten. Varmenteen noudon yhteydessä on huomioitava varmennepyynnön käsittelyaika, eikä varmennetta saa noutaa välittömästi onnistuneen varmennepyynnön jälkeen. Varmenne saadaan palautteena varmenteen haun palvelukutsulle, johon liitetään noutotunnus. Onnistuneen varmenteen haun jälkeen asiakkaalla on tulorekisterin palveluiden käyttöön tarvittava varmenne. Jos varmennetta ei voida muodostaa virhetilanteen vuoksi, palauttaa varmenteen haun palvelukutsu varmenteen sijaan virheilmoituksen.

3.3 Varmenteiden sulkeminen

Varmenne on suljettava, jos tiedetään tai epäillään, että varmenteen haltijan yksityinen avain on kadonnut tai päätynyt vääriin käsiin. Varmenne on suljettava myös silloin, jos se on tarpeeton. Tulorekisteriyksikkö voi sulkea varmenteen esimerkiksi silloin, kun palvelun käyttöön oikeuttava sopimus päättyy tai on ilmeistä, että myönnettyä varmennetta on käytetty väärin.

Varmenne suljetaan ottamalla yhteyttä Tulorekisteriyksikköön. Varmenteen sulkeminen ohjeistetaan tarkemmin varmennepalvelun sivuilla. Varmenteen sulkemista voi pyytää milloin tahansa. Kun asiakas pyytää varmenteen sulkemista virka-ajan ulkopuolella, varmenne suljetaan ensin tilapäisesti (asetetaan väliaikaiseen käyttökieltoon). Tällöin varmenteen käyttö on estetty, mutta varmenne on mahdollista aktivoida uudelleen. Jos asiakas vahvistaa sulkemispyynnön, varmenne suljetaan lopullisesti. Asiakkaan pitää vahvistaa väliaikaisesti suljetun varmenteen sulkeminen tai uudelleen aktivointi 14 vuorokauden kuluessa väliaikaiseen käyttökieltoon asettamisesta. Jos asiakas ei tänä aikana vahvista uudelleen aktivointia, Varmennepalvelu sulkee varmenteen lopullisesti.

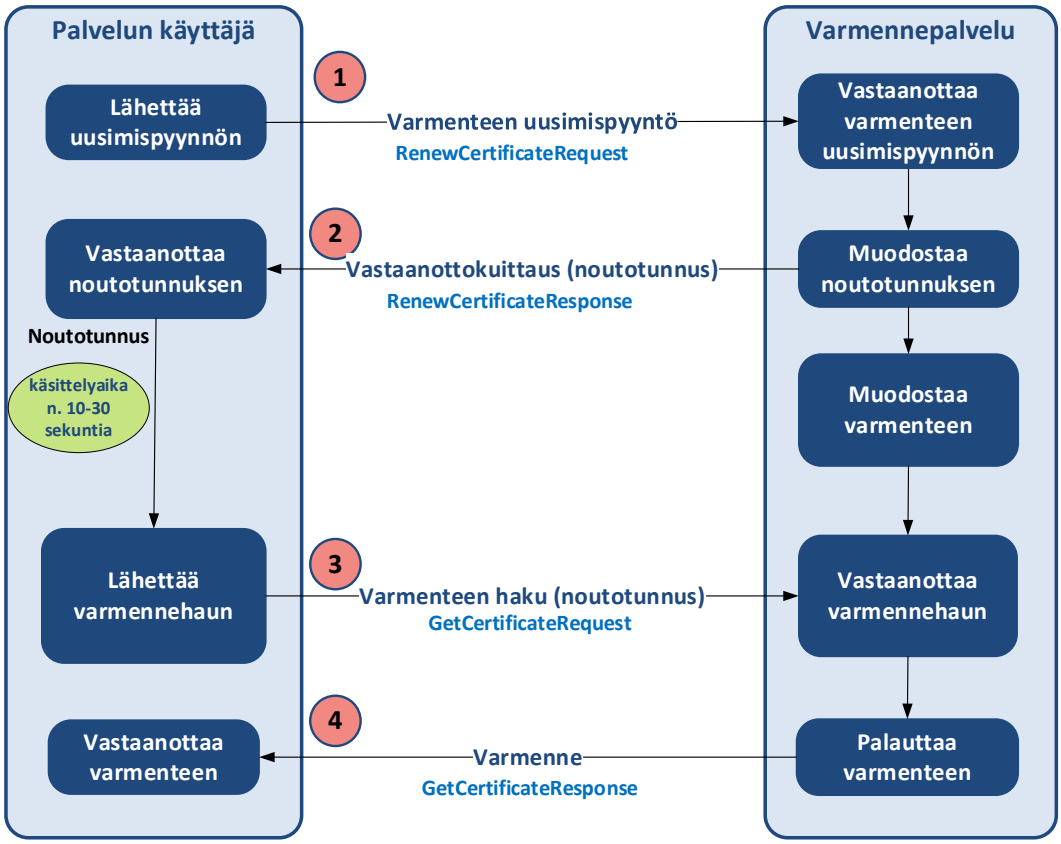
Lopullisesti suljettua varmennetta ei voi palauttaa käyttöön, eikä sitä voi uusia, vaan asiakkaan on tilattava uusi varmenne. Tällöin asiakkaan pitää tehdä uusi hakemus rajapinnan käyttöönottamiseksi tulorekisterin sähköisessä asiointipalvelussa ja noutaa se samalla tavalla kuin tilattaessa varmenne ensimmäisen kerran.

3.4 Varmenteiden elinkaari ja uusiminen

Asiakkaan varmenne on voimassa kaksi vuotta, jonka jälkeen se pitää uusia. Varmenteen haltijan pitää tarkistaa varmenteiden voimassaolo säännöllisesti. Viimeisen voimassaolopäivän voi tarkistaa sähköisestä asiointipalvelusta tai varmenteesta.

Varmenteen voi uusia varmennepalvelun rajapinnan kautta. Rajapinnassa on tätä varten oma palvelu (RenewCertificate). Uusimista varten luodaan uusi avainpari, muodostetaan varmenteen allekirjoituspyyntö ja allekirjoitetaan palvelupyyntö voimassaolevaan varmenteeseen liittyvällä avaimella. Varmenteen voi uusia aikaisintaan kuusikymmentä (60) vuorokautta ennen voimassaolon päättymistä. Vanha varmenne säilyy voimassa alkuperäisen voimassaolon loppuun asti. Jos varmenteen uusii ajoissa, ei tarvitse tilata uutta varmennetta eikä tulorekisteri toimita siirtotunnuksia (siirtotunnus ja kertakäyttösalasana).

Varmenteen uusiminen on esitetty kuvassa 2.



Kuva 2. Varmenteen uusiminen.

Varmenteen uusimista varten asiakkaan pitää luoda uusi avainpari sekä varmenteen allekirjoituspyyntö (CSR) samalla tavalla kuin pyydettäessä uusi varmenne.

Palvelun käyttäjä liittää muodostamansa allekirjoituspyynnön varmenteen uusimisen palvelukutsuun. Palvelukutsu allekirjoitetaan sähköisesti käyttäen aikaisempaan, edelleen voimassaolevaan varmenteeseen liittyvää yksityistä avainta.

Varmenteen allekirjoituksessa käytetään samaa muotoa kuin silloin, kun tulorekisteriin toimitetaan aineistoja voimassaolevalla varmenteella. Varmenteen uusiminen -toiminto palauttaa varmenteen noutotunnuksen, jota käyttämällä uusi varmenne haetaan varmenteen haun palvelukutsulla samalla tavalla kuin haettaessa varmennetta ensimmäistä kertaa. Varmenteen noudon yhteydessä on huomioitava varmennepyynnön käsittelyaika, eikä varmennetta saa noutaa välittömästi onnistuneen varmennepyynnön jälkeen.

Huom! Aikaisempi varmenne pitää korvata uudella varmenteella viipymättä, kuitenkin viimeistään sen voimassaolon päättymiseen mennessä. Jos samaa varmennetta on käytetty useammassa kuin yhdessä paikassa, pitää kaikki vanhan varmenteen kopiot korvata uudella, jotta vältytään vanhentuneen varmenteen aiheuttamilta virhetilanteilta.

Jos varmenne ehtii vanheta, pitää asiakkaan tilata uusi varmenne tulorekisterin sähköisessä asiointipalvelussa. Tällöin uuden varmenteen pyytäminen ja noutaminen tehdään samalla tavalla kuin tilattaessa varmenne ensimmäisen kerran.

3.5 Virhetilanteet

Pääsääntöisesti varmennepalvelu palauttaa tiedot virheistä välittömästi palvelun vastauksen yhteydessä. Osa virheistä havaitaan kuitenkin vasta varmennepyynnön käsittelyssä, jolloin varmenteen haun palvelukutsu palauttaa varmenteen sijaan virheilmoituksen.

Välittömästi palvelukutsun vastaanottokuittauksessa palautetaan tieto virheestä silloin, kun

- palvelukutsu ei ole palvelun skeeman mukainen
- siirtotunnus on virheellinen
- pyyntöön mahdollisesti liitetty varmenteen allekirjoituspyyntö on virheellisesti muodostettu
- varmenteen uusimisessa käytettävän sähköisen allekirjoituksen tarkistus epäonnistuu
- ilmenee jokin muu poikkeustilanteen aiheuttama tekninen virhe.

Jos varmenteen luonti epäonnistuu, pitää mahdollinen virhetilanne, kuten virheelliset tunnisteet, korjata. Sen jälkeen virheeseen päättynyt varmennepyynnön palvelukutsu pitää suorittaa uudelleen. Poikkeuksena on kuitenkin tilanne, jossa järjestelmä ei ole ehtinyt käsitellä varmennepyyntöä, ennen kuin varmennetta yritetään noutaa. Tällöin hakua voi yrittää uudelleen 10–30 sekunnin käsittelyajan jälkeen.

Palautettavat virhekoodit ja selitteet on kuvattu varmennepalvelun rajapintakuvauksessa.

4 VARMENTEIDEN KÄYTTÖ TULOREKISTERIN TEKNISISSÄ RAJAPINNOISSA

Tulorekisterin tekniset rajapinnat tarkistavat yhteyden muodostuksen yhteydessä varmenteen voimassaolon ja käyttötarkoituksen. Jos varmenne on vanhentunut, se on suljettu tai varmenne on myönnetty eri kanavaa varten, yhteyden muodostus epäonnistuu. Lisätietoa tulorekisterin rajapintojen käytöstä, asiakkaan tunnistamisesta ja sähköisestä allekirjoituksesta löytyy dokumentista: Tekninen rajapinta – Soveltamisohje 2020.

4.1 Web Service -kanava

Tulorekisterin Web Service -kanavassa varmennetta käytetään asiakkaan tunnistamiseen. Varmennetta ja yksityistä avainta käytetään aineistojen sähköiseen allekirjoittamiseen.

4.2 SFTP-kanava

Tulorekisterin SFTP-kanavassa käytetään käyttäjätunnusta ja varmenteen avainparia asiakkaan tunnistamiseen. Tunnistaminen tapahtuu siten, että avainparin julkinen avain on tulorekisterin varmennepalvelun ja SFTP-palvelimen hallussa ja asiakas tunnistautuu käyttäen yksityistä avaintaan. Varmennetta ja yksityistä avainta käytetään aineistojen sähköiseen allekirjoittamiseen.

5 PALVELUN TESTAUS

Varmennepalvelua ja sen myöntämiä varmenteita voi testata ennen palvelun käyttöönottoa. Varmennepalvelun teknistä rajapintaa hyödyntäviä ohjelmistototeutuksia voi testata ennen varsinaisten testivarmenteiden käyttöä varmennepalvelun testipenkissä. Testipenkissä voi testata toistuvasti rajapintojen tärkeimpiä toimintoja ennalta määritellyillä testiavaimilla. Lisätietoa varmennepalvelun testauksesta ja testipenkistä löytyy sivulta Varmennepalvelun sidosryhmätestaus.