

Verohallinnon varmennepalvelu – kuvaus PKI-järjestelmästä ja rajapinnoista

Verohallinto

Versiohistoria

Versio	Päivämäärä	Kuvaus
1.0	19.9.2024	Julkaistu uusi dokumentti, jossa kuvataan Verohallinnon varmennepalvelun osat, palvelun käyttö, rajapinnan palvelut ja niiden tietosisältö. Lisäksi dokumentissa on testipenkin kuvaus ja esimerkkejä käytön tueksi.



SISÄLLYS

1	Yleistä Verohallinnon varmennepalvelusta	5
1.1	Varmennepalvelun osat ja palvelun käyttö.....	5
1.2	Varmenteiden käyttötarkoitukset ja tyypit.....	5
1.3	Varmenteiden tilaaminen	6
1.4	Varmenteiden noutaminen.....	8
1.5	Varmenteiden sulkeminen	11
1.6	Varmenteiden elinkaari ja uusiminen	11
2	Sanasto ja lyhenteet	14
3	Rajapinnan nimiavaruudet, merkistö ja lukuohje	16
3.1	PKI-järjestelmän Web Service -rajapinta.....	16
3.2	Skeema.....	16
3.3	Merkistö	17
3.4	Kaavioiden lukuohje.....	17
4	Rajapinnan palvelut ja virheiden käsittely	19
4.1	Rajapinnan palvelut.....	19
4.2	Sanomien allekirjoitus.....	20
4.3	Virheiden käsittely	20
5	Rajapinnan palveluiden tietosisältö	21
5.1	Uuden varmenteen pyytäminen – pyyntösanoma (SignNewCertificateRequest)	21
5.2	Uuden varmenteen pyytäminen – vastausanoma (SignNewCertificateResponse)	22
5.3	Voimassa olevan varmenteen uusiminen – pyyntösanoma (RenewCertificateRequest)	23
5.4	Voimassa olevan varmenteen uusiminen – vastausanoma (RenewCertificateResponse)	24
5.5	Varmenteen noutaminen – pyyntösanoma (GetCertificateRequest)	26
5.6	Varmenteen noutaminen – vastausanoma (GetCertificateResponse).....	27
5.7	Sanoman käsittelyn lopputulos (Result).....	28
6	Virhekoodit ja virhekoodien selitteet.....	30
7	Testipenkin ohjeet.....	33
7.1	Testimateriaali.....	33
7.1.1	Testipenkin palveluissa käytettävät parametrit.....	33



7.2	Testipenkin yhteysosoite	35
7.3	Testipenkin palveluiden virhetilanteet	35
8	Esimerkkisanomia.....	37
8.1	Varmenteen nouto (getCertificate).....	37
8.2	Varmenteen uusiminen (renewCertificate)	38
9	Esimerkki varmenteen uusimisesta ja allekirjoituksen (CSR) luomisesta	42
10	Allekirjoituksen (CSR) luonti Windowsin MMC-työkalulla	48



1 YLEISTÄ VEROHALLINNON VARMENNEPALVELUSTA

1.1 Varmennepalvelun osat ja palvelun käyttö

Verohallinnon varmennepalvelu koostuu taustalla olevasta PKI-järjestelmästä ja asiointipalvelusta, joka on varmennepalvelun selaimessa käytettävä asiakkaan käyttöliittymä. Verohallinnon varmennepalvelun varmenteita hyödyntävät organisaatiot, jotka toimittavat tai noutavat aineistoja teknisten rajapintojen kautta tai kyselevät tietoja järjestelmistä rajapintapalveluiden avulla. Varmenne myönnetään organisaatiolle, joka vastaa tietojen toimittamisesta tai jolla on oikeus saada tietoja. Varmennepalvelusta saa varmenteita sekä testaukseen että tuotantokäyttöön.

Verohallinto myöntää asiakkaille varmenteita Verohallinnon, tulorekisterin ja positiivisen luottotietorekisterin rajapintoihin. Tässä dokumentissa kuvataan järjestelmän käyttö yleisesti ja vain tekniseltä kannalta. Kun käytät eri tahojen rajapintoja, tutustu aina myös kyseisen tahon omiin ohjeisiin. Esimerkiksi tulorekisterin tietojen käyttämiseen tai luottotietorekisterin tietojen hyödyntämiseen tarvitaan tietolupa, jota haetaan suoraan kyseiseltä taholta. Verohallinnon varmenteet perustuvat PKI-ratkaisuun (Public Key Infrastructure). Asiakkaalla on yksi tai useampi avainpari (yksityinen ja julkinen avain) ja avainpariin liittyvä varmenne, joka on X.509-standardin mukainen. Varmennetta käytetään asiakkaan tunnistamiseen ja asiakkaan lähettämän aineiston allekirjoittamiseen sähköisellä allekirjoituksella (XML Signature).

Asiakas hallinnoi organisaationsa rajapinto-oikeuksia ja varmenteita varmennepalvelun asiointipalvelussa. Palvelussa asiakas tekee rajapintahakemukset, tilaa varmenteet ja ylläpitää varmenteiden tietoja. Varmenteet luodaan ja säilytetään taustalla olevassa PKI-järjestelmässä. Varmenteen voi noutaa joko asiointipalvelussa tai PKI-järjestelmän rajapinnan kautta.

Asiointipalveluun kirjaudutaan sivulla [Verohallinnon varmennepalvelu](#). Samoilla sivuilla ohjeistetaan rajapintahakemusten ja varmennetilausten tekeminen testauksen ja tuotannon tilanteissa. Palveluun tunnistaudutaan pankkitunnuksilla, mobiilivarmenteella tai varmennekortilla.

1.2 Varmenteiden käyttötarkoitukset ja tyypit

Varmenteet myönnetään aina tiettyyn käyttötarkoitukseen tietylle asiakkaalle, eikä niitä voi käyttää alkuperäisestä poikkeavaan tarkoitukseen. Asiakkaan on tutustuttava [Verohallinnon ja tulorekisterin rajapintapalveluiden käyttöehtoihin](#) ja noudatettava niitä.

Jos asiakas hyödyntää Verohallinnon teknisiä rajapintoja eri käyttötarkoituksiin (esimerkiksi palkka- tai etuustiedon tuottajana ja tulorekisterin tiedon käyttäjänä), pitää eri käyttötarkoituksiin tilata omat varmenteet. Samoin eri rajapintoihin pitää tilata erilliset varmenteet. Yhdellä toimijalla voi siis olla useita varmenteita. Jos asiakas käyttää useita varmenteita samassa ohjelmistossa, varmenteiden hallintaan pitää kiinnittää erityistä huomiota.

Rajapinnat	Kanava	Varmenteen julkaisija
Palkkatiedon tuottaja (Web Service)	Web Service (SOAP)	Data Providers Issuing CA
Palkkatiedon tuottaja SFTP)	SFTP	Data Providers SFTP Issuing CA
Etuustiedon tuottaja (WS)	Web Service (SOAP)	IR Benefit Data Providers Issuing CA
Etuustiedon tuottaja (SFTP)	SFTP	IR Benefit Data Providers SFTP Issuing CA
Tiedon käyttäjä (WS)	Web Service (SOAP)	IR Income Data Users Issuing CA
Tiedon käyttäjä (SFTP)	SFTP	IR Income Data Users SFTP Issuing CA
Tulorekisterin ulkopuoliset tukipalvelut	Web Service (SOAP)	IR External Data Providers Issuing CA
	SFTP	IR External Data Providers SFTP Issuing CA
Vero API	Web Service (REST)	Data Providers Issuing CA
APItamoPKI	Web Service (SOAP)	Data Providers Issuing CA
Luoton tietojen ilmoittaja	Web Service (REST)	Data Providers Issuing CA
Luottotiedon hyödyntäjä	Web Service (REST)	PCR Credit Data Users Issuing CA v1

Taulukko 1: Varmenteen tyypit ja julkaisijat.

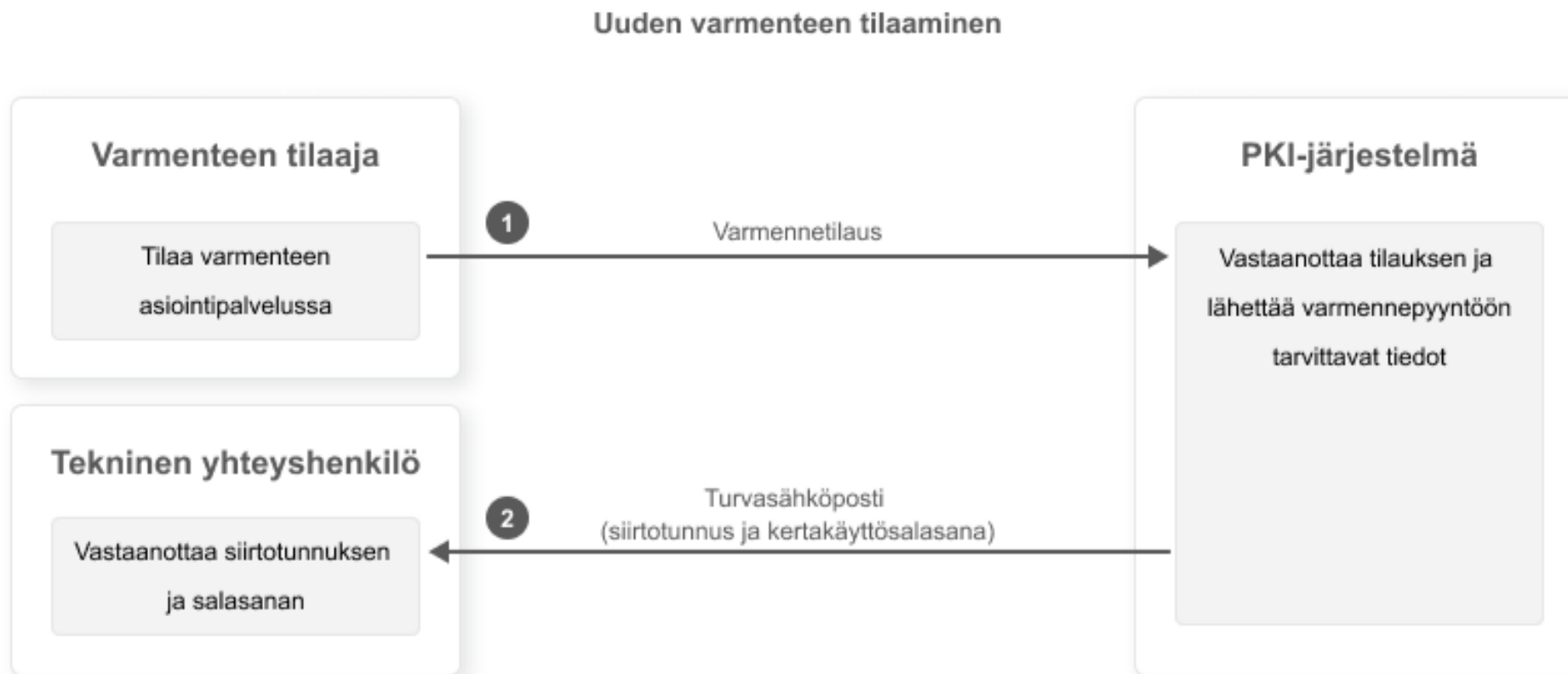
Varmenteet luodaan yllä mainittujen julkaisijoiden (Certificate Authority, CA) mukaisesti ja niitä vastaavat julkaisupaketit voi ladata varmennepalvelun sivuilta kohdasta [Dokumentaatio](#).

1.3 Varmenteiden tilaaminen

Varmenteet tilataan aina varmennepalvelun asiointipalvelussa. Asiakas nimeää tilauksessa varmenteen teknisen yhteyshenkilön, ja varmennepalvelu lähettää henkilölle tiedot, jotka tarvitaan varmenteen noutamiseen: siirtotunnus (TransferId) ja kertakäyttösalausana (TransferPassword). Nämä lähetetään tekniselle

yhteyshenkilölle turvasähköpostiviestissä, jonka avaamista varten henkilö saa tekstiviestillä PIN-koodin. Kertakäyttösalasana on voimassa 14 vuorokautta. Jos varmennetta ei noudeta tämän ajan kuluessa, kertakäyttösalasana vanhenee, ja asiakkaan pitää tehdä uusi varmennetilaus.

Uuden varmenteen tilaaminen on esitetty kuvassa 1. Tarkemmat ohjeet tilaamiseen asiointipalvelussa ovat sivulla [Verohallinnon varmennepalvelu](#).



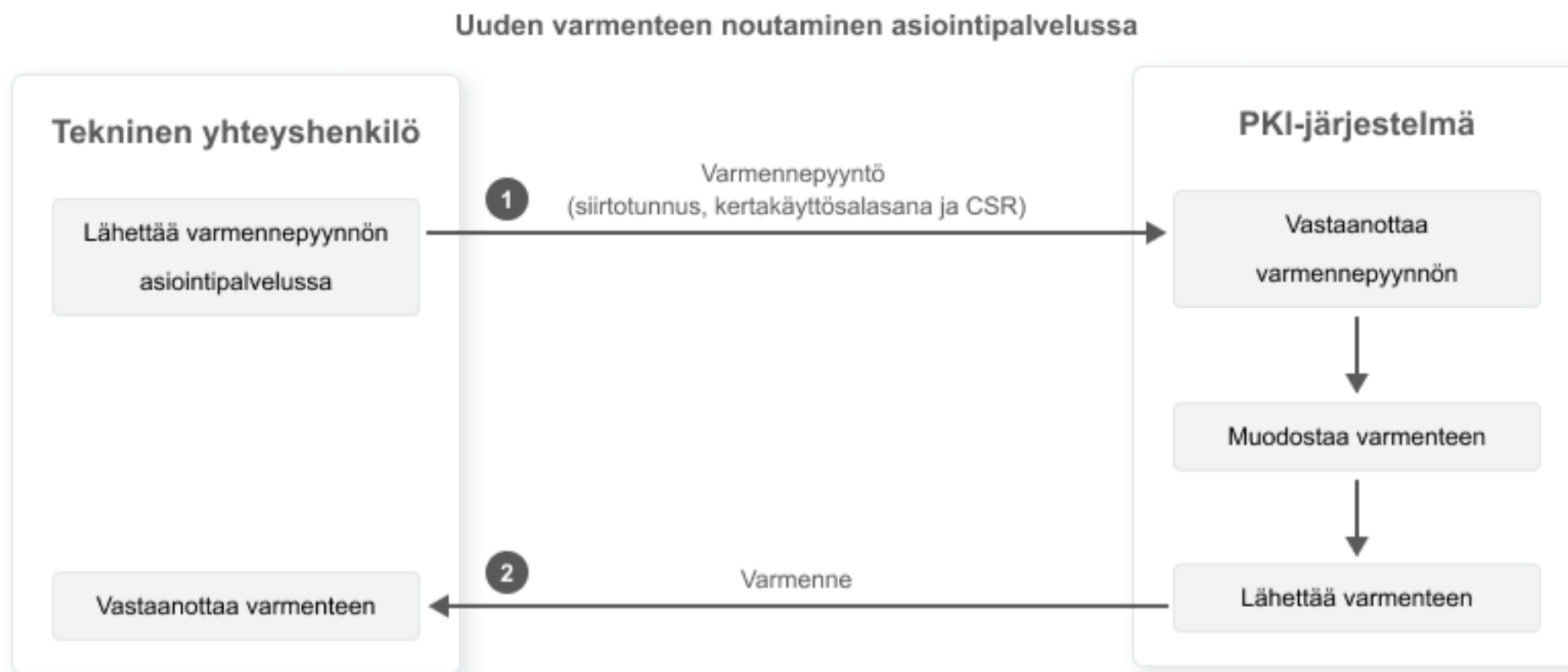
Kuva 1: Varmenteen tilaaminen.



1.4 Varmenteiden noutaminen

Varmenteen voi noutaa joko rajapinnassa tai asiointipalvelussa. Molemmilla tavoilla noutoon tarvitaan siirtotunnus, kertakäyttösalasana ja varmenteen allekirjoituspyyntö (CSR). 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.

Kun varmenne noudetaan asiointipalvelussa (kuva 2), asiakas syöttää käyttöliittymään siirtotunnuksen, salasanan ja muodostamansa allekirjoituspyynnön. Varmenne latautuu tietokoneelle.



Kuva 2: Varmenteen noutaminen asiointipalvelussa.

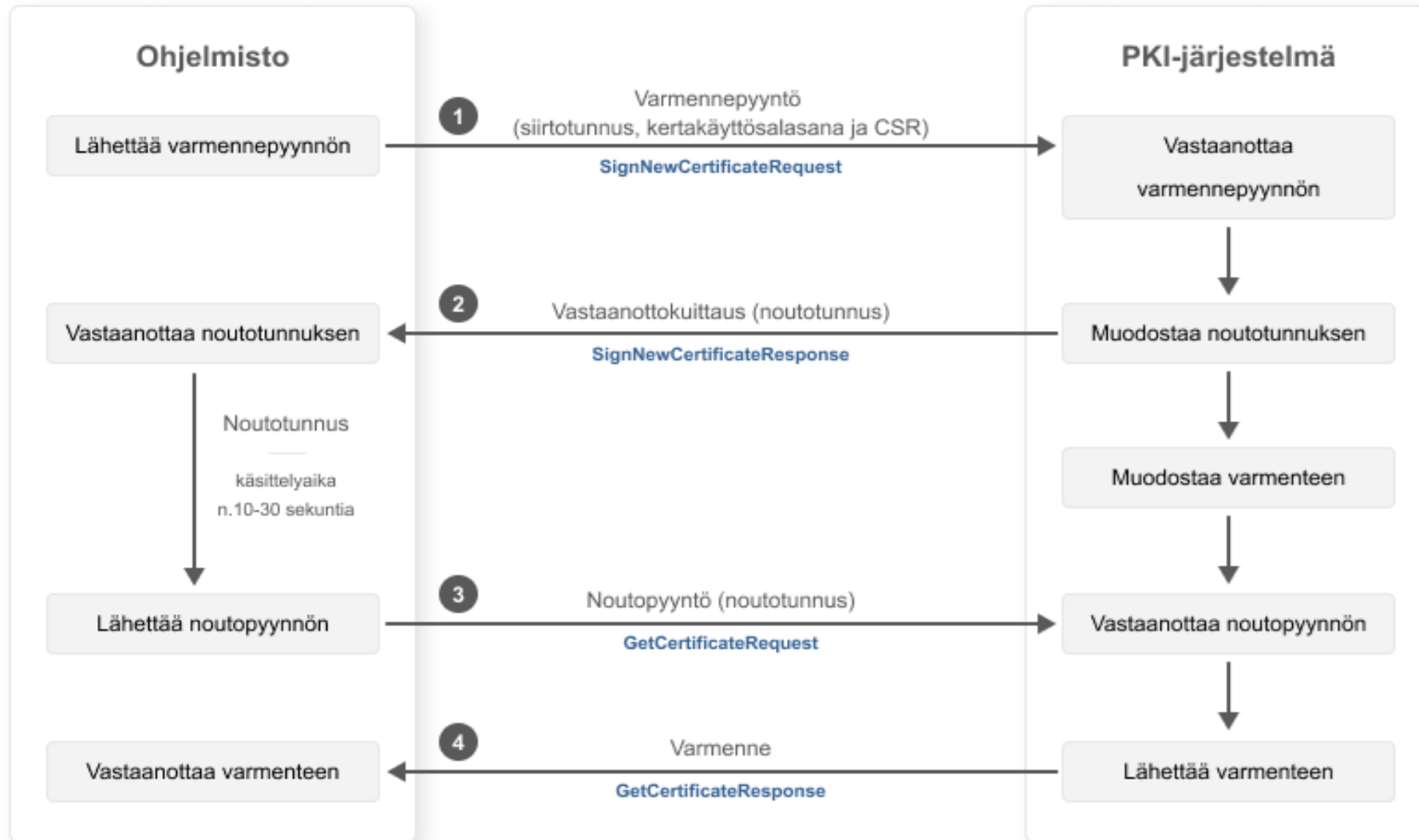
Kun varmenne noudetaan rajapinnan kautta (kuva 3), asiakas liittää siirtotunnuksen, salasanan ja allekirjoituspyynnön uuden varmenteen pyynnön palvelukutsuun (SignNewCertificateRequest). Palvelukutsu palauttaa asiakkaalle vastaanottokuittauksessa noutotunnuksen (RetrievalID). Noutotunnuksen saamisen jälkeen asiakkaan pitää odottaa noin 10–30 sekuntia. Tämän jälkeen asiakas luo varmenteen noutamisen palvelukutsun (GetCertificateRequest) ja liittää siihen noutotunnuksen. Vastauksena palvelukutsuun asiakas saa varmenteen. Jos varmennetta ei voida muodostaa virhetilanteen vuoksi, palauttaa noutamisen palvelukutsu varmenteen sijaan virheilmoituksen.

Tuotantovarmenteiden rajapinnan osoite: <https://pkiws.vero.fi/2017/10/CertificateServices>

Testivarmenteiden rajapinnan osoite: <https://pkiws-testi.vero.fi/2017/10/CertificateServices>



Uuden varmenteen noutaminen PKI-järjestelmän rajapinnan kautta



Kuva 3: Varmenteen noutaminen rajapinnan kautta.

1.5 Varmenteiden sulkeminen

Asiakkaan pitää pyytää tuotantovarmenteen sulkemista, jos tiedetään tai epäillään, että varmenteen haltijan yksityinen avain on kadonnut tai päätynyt väärin käsiin. Varmenne on suljettava myös silloin, jos se on tarpeeton. Varmenteen myöntäjä eli Verohallinto voi sulkea varmenteen esimerkiksi silloin, kun palvelun käyttöön oikeuttava sopimus päättyy tai on ilmeistä, että myönnettyä varmennetta on käytetty väärin.

Asiakas sulkee tuotantovarmenteen ottamalla yhteyttä tulorekisterin asiakaspalveluun. Tarkat ohjeet ovat sivulla [Varmenteen sulkeminen](#). Tulorekisterin asiakaspalvelu vastaa Verohallinnon, tulorekisterin ja positiivisen luottotietorekisterin tuotantovarmenteiden sulkemisesta.

Tuotantovarmenteen 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 sulkemisen, varmenne suljetaan lopullisesti. Asiakkaan pitää vahvistaa sulkeminen tai aktivoida varmenne uudelleen 14 vuorokauden kuluessa siitä, kun varmenne on asetettu väliaikaiseen käyttökieltoon. Jos asiakas ei tänä aikana vahvista uudelleen aktivointia, Verohallinto 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 rajapintahakemus varmennepalvelun asiointipalvelussa ja noutaa varmenne samalla tavalla kuin tilattaessa varmenne ensimmäisen kerran.

Testivarmenteen voi sulkea täyttämällä [varmennepalvelun havaintolomakkeen](#).

1.6 Varmenteiden elinkaari ja uusiminen

Asiakkaan tuotanto- tai testivarmenne on voimassa kaksi vuotta. Jos varmenteen haluaa uusia, se pitää tehdä ennen sen vanhenemista. Varmenteen haltijan pitää tarkistaa varmenteiden voimassaolo säännöllisesti. Viimeisen voimassaolopäivän voi tarkistaa varmennepalvelun asiointipalvelusta tai varmenteesta.

Varmenne uusitaan PKI-järjestelmän rajapinnan kautta. Varmenteen voi uusia aikaisintaan kuusikymmentä (60) vuorokautta ennen sen voimassaolon päättymistä. Vanha varmenne säilyy voimassa alkuperäisen voimassaolon loppuun asti. Jos varmenteen uusii ajoissa, ei tarvitse tilata uutta varmennetta eikä asiakas tarvitse uutta siirtotunnusta ja kertakäyttösalasanaa.

Varmenteen uusiminen rajapinnan kautta on esitetty kuvassa 4.

Voimassaolevan varmenteen uusiminen



Kuva 4: Varmenteen uusiminen rajapinnan kautta.

Rajapinnassa on uusimiseen oma palvelu (RenewCertificate). Uusimista varten asiakas luo uuden avainparin, muodostaa varmenteen allekirjoituspyynnön ja allekirjoittaa palvelukutsun voimassa olevaan varmenteeseen liittyvällä yksityisellä avaimella.

Varmenteen allekirjoituksessa käytetään samaa muotoa kuin silloin, kun asiakas lähettää aineistoja rajapintojen kautta voimassa olevalla varmenteella. Varmenteen uusimisen pyyntö palauttaa vastaanottokuittauksessa asiakkaalle varmenteen noutotunnuksen. Asiakas noutaa varmenteen samalla tavalla kuin uuden varmenteen noudossa. Asiakkaan pitää siis odottaa noin 10–30 sekuntia. Tämän jälkeen asiakas luo varmenteen noutamisen palvelukutsun (GetCertificateRequest) ja liittää siihen noutotunnuksen. Vastauksena palvelukutsuun asiakas saa varmenteen.

Huom! Aikaisempi varmenne pitää korvata uudella varmenteella viipymättä, kuitenkin viimeistään ennen kuin aiemman varmenteen voimassaolo päättyy. Jos samaa varmennetta on käytetty useammassa kuin yhdessä paikassa, pitää kaikki vanhan varmenteen kopiot korvata uudella, jotta vältetään vanhentuneen varmenteen aiheuttamilta virhetilanteilta.

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



2 SANASTO JA LYHENTEET

Varmennepalvelun yhteydessä käytetyt lyhenteet ja tärkeimmät termit.

Lyhenne tai termi	Selite
CSR (Certificate Signing Request) varmenteen allekirjoituspyyntö	Varmennepalvelun käyttäjän tekemä varmenteen allekirjoituspyyntö. Se on PKCS#10-muotoinen Base64-koodattu merkkijono.
Julkisen avaimen menetelmä	Epäsymmetrinen salaus, jossa toinen salausavaimista on julkinen avain ja toinen on yksityinen avain.
Noutotunnus (RetrievalID)	Tunnus, jolla varmenteen voi myöhemmin noutaa.
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 suoritettujen allekirjoitusten 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.
Siirtotunnus (TransferID)	Asiakkaalle varmenteen pyytämistä varten toimitettu tunnus.
Varmennetilaus	Verohallinnon varmennepalvelun asiointipalvelussa tehtävä varmenteen tilaus.
Varmennepyyntö	Rajapinnan SignNewCertificate-palvelun pyyntösanoma, jolla asiakas aloittaa aiemmin tilatun varmenteen noutamisen.
Varmenteen noutopyyntö	Rajapinnan GetCertificate-palvelun pyyntösanoma, jolla asiakas noutaa aiemmin pyydetyn varmenteen.
Varmenteen uusimispyyntö	Rajapinnan RenewCertificate-palvelun pyyntösanoma, jolla asiakas uusii voimassa olevan varmenteen.
WS (Web Service)	Verkkopalvelimessa toimiva ohjelmisto, joka tarjoaa standardoitujen internetyhteyksikäytäntöjen 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 voimassa olevalla varmenteella muodostama XML-allekirjoitus.



X.509	Varmenteen rakenteen määrittelevä standardi.
-------	--

Taulukko 2: Termit ja lyhenteet.

3 RAJAPINNAN NIMIAVARUUDET, MERKISTÖ JA LUKUOHJE

Seuraavassa kuvataan Verohallinnon varmennepalvelun PKI-järjestelmän Web Service -rajapinnan toteutus järjestelmäintegraation toteuttajan näkökulmasta. Dokumentissa kuvataan rajapinnan palvelut sekä palveluiden tietosisältö (XML-skeemat).

PKI-järjestelmän rajapinnan tekninen toteutus esitellään sillä tarkkuudella, että osapuolet voivat sen pohjalta määritellä ja toteuttaa oman järjestelmänsä integraation PKI-järjestelmän kanssa.

3.1 PKI-järjestelmän Web Service -rajapinta

Rajapinnan palvelut on määritelty kuvauksessa **CertificateServices.wsdl**.

Kuvauksessa käytetyt nimiavaruudet ovat seuraavat:

Tiedoston nimi	Prefix	Namespace
XMLSchema	xmlns:xs	http://www.w3.org/2001/XMLSchema
WSDL	xmlns:wsdl	http://schemas.xmlsoap.org/wsdl/
WSDL SOAP binding	xmlns:soap	http://schemas.xmlsoap.org/wsdl/soap/
CertificateServices.wsdl	xmlns:tns	http://certificates.vero.fi/2017/10/certificateservices

3.2 Skeema

PKI-järjestelmän myöntämien varmenteiden elinkaaren hallintaan käytetään XML-skeeman **CertificateServices.xsd** mukaisia elementtejä.

Skeemassa käytetyt nimiavaruudet ovat seuraavat:

Tiedoston nimi	Prefix	Namespace
XMLSchema	xmlns:xs	http://www.w3.org/2001/XMLSchema
CertificateServices.xsd	xmlns:ser	http://certificates.vero.fi/2017/10/certificateservices

Sanomissa ei sallita tyhjiä elementtejä. Jos elementtiin ei tule arvoa, se jää sanomalta kokonaan pois. Myöskään tyhjiä merkkijonoja ei sallita, eli kaikkien arvojen pituus on vähintään 1.



3.3 Merkistö

Skeemoissa on käytössä XML:n oletusmerkistö UTF-8. Tiedostossa ei saa olla Byte Order Mark (BOM) -merkkiä.

Seuraavassa taulukossa on esitetty sanomissa esiintyvien erikoismerkkien muunnoksiin liittyvät vaatimukset.

Merkki	Kuvaus	Esitysmuoto entiteettinä
&	et-merkki	& muunnos on pakollinen
<	pienempi kuin	< muunnos on pakollinen
>	suurempi kuin	> muunnos ei ole pakollinen, mutta on hyvien käytäntöjen mukaista
'	heittomerkki	' muunnos ei ole pakollinen, mutta on hyvien käytäntöjen mukaista
"	lainausmerkki	" muunnos ei ole pakollinen, mutta on hyvien käytäntöjen mukaista
--	tuplaviiva	Merkki ei saa esiintyä xml-tiedostossa
/*	kauttaviiva asterisk	Merkki ei saa esiintyä xml-tiedostossa
&#	et-merkki risuaitamerkki	Merkki ei saa esiintyä xml-tiedostossa

3.4 Kaavioiden lukuohje

Dokumentin kaavioissa olevien elementtien oikeassa alakulmassa oleva merkintä $0 \dots \infty$ tarkoittaa, että elementti voi toistua useita kertoja ja se voi myös puuttua kokonaan. Merkintä $1 \dots \infty$ tarkoittaa, että elementti voi toistua useita kertoja, mutta aina vähintään kerran. Pakolliset elementit on merkitty yhtenäisellä reunaviivalla ja vapaaehtoiset elementit katkonaisella reunaviivalla.

Dokumentin taulukoissa elementin pakollisuus ja myös ilmentymien määrä ilmaistaan sarakkeessa 'Elementin pakollisuus'. Elementin määrät ilmaistaan muodossa A:B, missä A kertoo, montako kyseistä elementtiä sanomalla tulee vähintään olla (minOccurs), ja B kertoo, montako kyseistä elementtiä sanomalla enintään saa olla (maxOccurs). Arvoina käytetään seuraavia arvoja:

0 = elementti voi puuttua

1 = elementti esiintyy kerran

N = N on numeerinen arvo ja elementti esiintyy N kertaa



unbounded = elementti esiintyy ennalta määrittelemättömän määrän kertoja

4 RAJAPINNAN PALVELUT JA VIRHEIDEN KÄSITTELY

4.1 Rajapinnan palvelut

Alla olevassa taulukossa on kuvattu rajapinnan palvelut:

Operaatio	Pyyntösanoma	Vastaussanoma	Kuvaus
Uuden varmenteen pyytäminen (SignNewCertificate)	SignNewCertificateRequestMessage	SignNewCertificateResponseMessage	Varmennepyyntö, jolla asiakas aloittaa uuden varmenteen noutamisen. Ennen varmennepyyntöä asiakkaan pitää tilata uusi varmenne Verohallinnon varmennepalvelun asiointipalvelussa. Varmennepyyntöä käytetään, kun - asiakas on noutamassa organisaation ensimmäistä varmennetta - asiakkaalla on jo voimassa oleva varmenne tai varmenteita, mutta organisaatio tarvitsee lisää varmenteita - asiakkaan aiempi varmenne on vanhentunut tai se on revokoitu eli poistettu käytöstä.
Voimassa olevan varmenteen uusiminen (RenewCertificate)	RenewCertificateRequestMessage	RenewCertificateResponseMessage	Varmenteen uusimispyyntö, kun käyttäjän hallussa oleva varmenne on vanhenemassa ja uusiminen tehdään ennen voimassa olevan varmenteen vanhenemista.
Varmenteen noutaminen (GetCertificate)	GetCertificateRequestMessage	GetCertificateResponseMessage	Aiemmin pyydetyn uuden tai uusitun varmenteen noutaminen. Varmennepyyntö tai voimassa olevan varmenteen uusimisen vastaussanomien välillä on oltava vähintään 10 sekunnin viive.

Rajapinnan palveluiden ja sanomien tietosisältö kuvataan luvussa 5.



4.2 Sanomien allekirjoitus

Web Service -rajapinnan palveluissa käytetään sähköistä allekirjoitusta (XML Signature). Sillä todennetaan viestin tietosisällön muodostaja luvussa 5 määriteltävissä sanomissa. Allekirjoitus takaa myös viestin muuttumattomuuden. Allekirjoitus toteutetaan XML Enveloped Signature -mekanismilla, jonka käsittelysäännöt ja rakenne kuvataan dokumentissa XML Signature Syntax and Processing (<http://www.w3.org/TR/xmlsig-core/>). Sähköisen allekirjoituksen esimerkki on tässä dokumentissa kappaleessa 9.

4.3 Virheiden käsittely

Palvelut palauttavat virhetilanteissa niihin liittyvät virheilmoitukset vastaussanomana mukana, tietosisällössä kuvatun rakenteen mukaisesti. Virheen tiedot -elementti sisältää virheen koodin ja virhekoodin selitteen. Jos virhe havaitaan ennen varsinaisen palvelupyynnön käsittelyä (SOAP-viestin käsittely), palvelu palauttaa pelkän HTTP-virheen. HTTP-virhe voi olla esimerkiksi HTTP 404 Not found. Palvelu voi palauttaa myös SOAP 1.1 Fault -rakenteen mukaisen virheilmoituksen HTTP 500 -virhekoodilla (Internal Server Error). SOAP Fault voidaan palauttaa muun muassa tilanteissa, joissa SOAP-kehys ei ole validi, vastaanotettua sanomaa ei voida jäsentää XML-dokumentiksi tai dokumentti ei läpäise skeemavalidointia.

Pääsääntöisesti tiedot virheistä palautetaan välittömästi palvelun vastauksen yhteydessä. Osa virheistä havaitaan kuitenkin vasta varmennepyyntöä käsitellessä, jolloin varmenteen haun palvelukutsu palauttaa varmenteen sijaan virheilmoituksen.

Välittömästi palvelukutsun vastaanottokuittauksessa palautetaan tieto virheestä silloin, kun

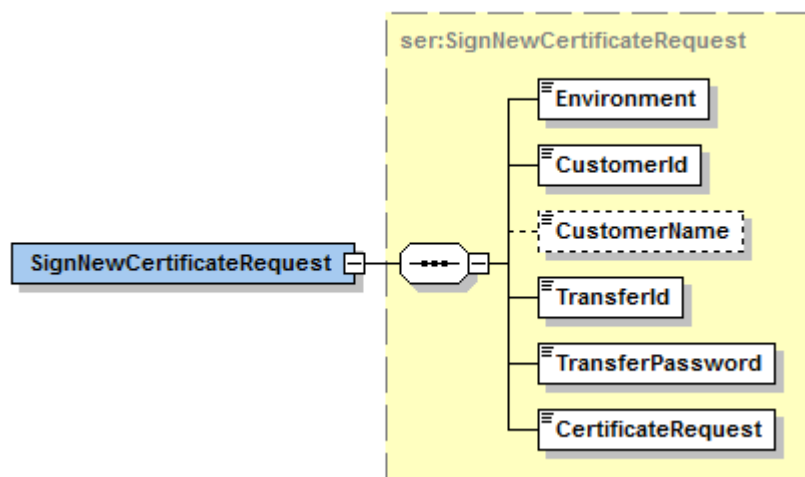
- palvelukutsu ei ole palvelun skeeman mukainen
- siirtotunnus on virheellinen
- pyyntöön mahdollisesti liitetty varmenteen allekirjoituspyyntö on virheellisesti muodostettu
- varmenteen uusimisessa käytettävän sähköisen allekirjoituksen tarkistus epäonnistuu
- ilmenee jokin muu poikkeustilanteen aiheuttama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

Jos varmenteen luonti epäonnistuu, pitää mahdollinen virhetilanne, kuten virheelliset tunnisteet, korjata. Sen jälkeen virheeseen päättynyt varmennepyyntöä 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.



5 RAJAPINNAN PALVELUIDEN TIETOSISÄLTÖ

5.1 Uuden varmenteen pyytäminen – pyyntösanoma (SignNewCertificateRequest)



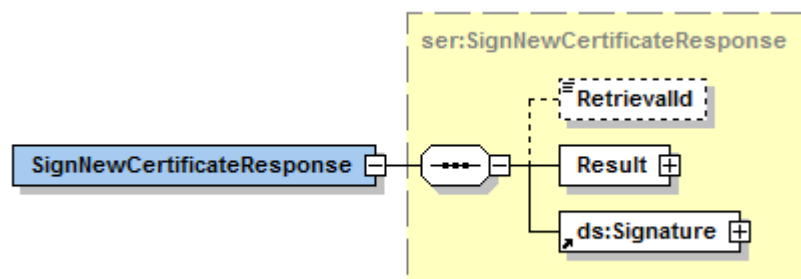
Tietoryhmän *SignNewCertificateRequest* tiedot:

Tiedon nimi	Tyyppi	Sallitut arvot	Elementin pakollisuus (minOccurs: maxOccurs)	Tiedon selite
Ympäristö (Environment)	ser:EnvironmentTypes	PRODUCTION, TEST	1:1	Tuotantoympäristössä arvon on oltava PRODUCTION ja testiympäristössä arvon on oltava TEST.
Asiakkaan tunnistetunnus (CustomerId)	ser:String30		1:1	Asiakkaan tunnistetunnus. Tunnistetunnusena käytetään organisaation virallista, Verohallinnon kanssa asiointiin käytettyä tunnistetunnusta. Tunnistetunnus voi olla esimerkiksi Y-tunnus. Jos käytetään Y-tunnusta, tunnistetunnus on oltava Yritys- ja



Tiedon nimi	Tyyppi	Sallitut arvot	Elementin pakollisuus (minOccurs: maxOccurs)	Tiedon selite
				yhteisötietojärjestelmässä (YTJ) ja tunnisteessa on oltava väliviiva.
Asiakkaan nimi (CustomerName)	ser:String100		0:1	Asiakkaan nimi. Tietoa ei sellaisenaan käytetä varmenteella, mutta se auttaa mahdollisessa virheselvittelyssä.
Siirtotunnus (TransferId)	ser:String32		1:1	Asiakkaalle varmenteen pyytämistä varten toimitettu tunnus.
Kertakäyttösalausana (TransferPassword)	ser:String16		1:1	Asiakkaalle varmenteen pyytämistä varten toimitettu kertakäyttöinen salasana.
Varmenteen allekirjoituspyyntö (CertificateRequest)	ser:CertificateRequestType		1:1	Asiakkaan tekemä varmenteen allekirjoituspyyntö, joka on PKCS#10-muotoinen Base64-koodattu merkkijono.

5.2 Uuden varmenteen pyytäminen – vastaussanoma (SignNewCertificateResponse)

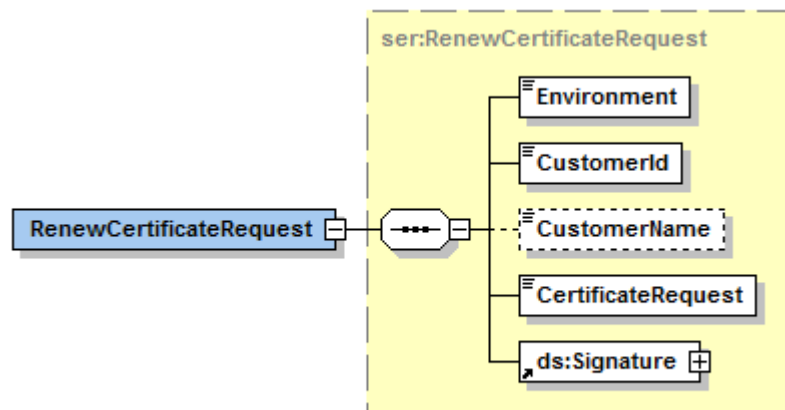


Tietoryhmän *SignNewCertificateResponse* tiedot:



Tiedon nimi	Tyyppi	Sallitut arvot	Elementin pakollisuus (minOccurs: maxOccurs)	Tiedon selite
Varmenteen noutotunnus (RetrievalId)	ser:String32		0:1	Tunnus, jolla varmenteen voi myöhemmin noutaa.
Käsittelyn lopputulos (Result)	ser:Result		1:1	Käsittelyn lopputulos, ks. tarkempi sisältö elementin Sanoman käsittelyn lopputulos kuvauksesta.
XML-allekirjoitus (Signature)	ds:Signature		1:1	XML-allekirjoitus, jonka PKI-järjestelmä muodostaa omalla varmenteellaan.

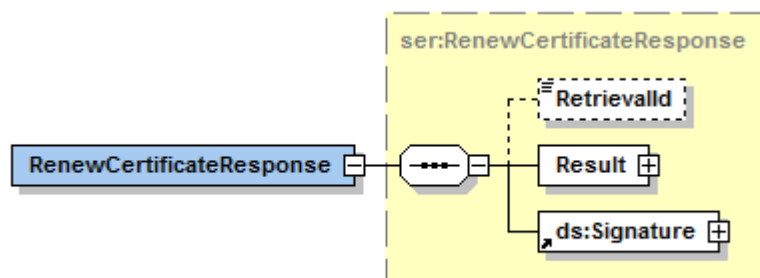
5.3 Voimassa olevan varmenteen uusiminen – pyyntösanoma (RenewCertificateRequest)



Tietoryhmän *RenewCertificateRequest* tiedot:

Tiedon nimi	Tyyppi	Sallitut arvot	Elementin pakollisuus (minOccurs: maxOccurs)	Tiedon selite
Ympäristö (Environment)	ser:EnvironmentTypes	PRODUCTI ON, TEST	1:1	Tuotantoympäristössä arvon on oltava PRODUCTION ja testiympäristössä arvon on oltava TEST.
Asiakkaan tunniste (CustomerId)	ser:String30		1:1	Asiakkaan tunniste. Tunnisteena käytetään organisaation virallista, Verohallinnon kanssa asiointiin käytettyä tunnistetta. Tunniste voi olla esimerkiksi Y-tunnus. Jos käytetään Y-tunnusta, tunniste on oltava Yritys- ja yhteisötietojärjestelmässä (YTJ) ja tunnisteessa on oltava väliviiva.
Asiakkaan nimi (CustomerName)	ser:String100		0:1	Asiakkaan nimi. Tietoa ei sellaisenaan käytetä varmenteella, mutta se auttaa mahdollisessa virheselvittelyssä.
Varmennepyyntö (CertificateRequest)	ser:CertificateRequestT ype		1:1	Asiakkaan tekemä varmenteen allekirjoituspyyntö, joka on PKCS#10-muotoinen Base64-koodattu merkkijono.
XML-allekirjoitus (Signature)	ds:Signature		1:1	XML-allekirjoitus, jonka asiakas muodostaa voimassa olevalla varmenteellaan.

5.4 Voimassa olevan varmenteen uusiminen – vastaussanoma (RenewCertificateResponse)



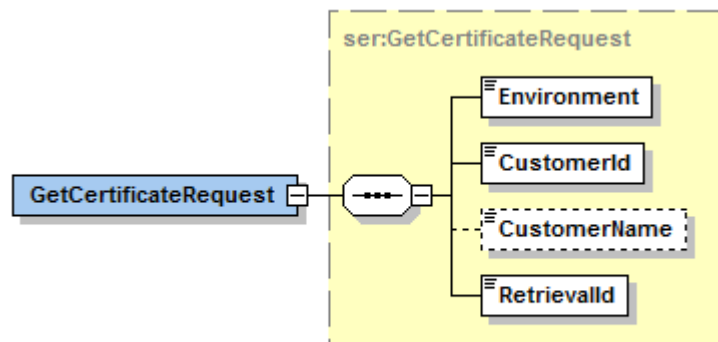
Tietoryhmän *RenewCertificateResponse* tiedot:



Tiedon nimi	Tyyppi	Sallitut arvot	Elementin pakollisuus (minOccurs: maxOccurs)	Tiedon selite
Varmenteen noutotunnus (RetrievalId)	ser:String32		0:1	Tunnus, jolla varmenteen voi myöhemmin noutaa.
Käsittelyn lopputulos (Result)	ser:Result		1:1	Käsittelyn lopputulos, ks. tarkempi sisältö elementin Sanoman käsittelyn lopputulos kuvauksesta.
XML-allekirjoitus (Signature)	ds:Signature		1:1	XML-allekirjoitus, jonka PKI-järjestelmä muodostaa omalla varmenteellaan.



5.5 Varmenteen noutaminen – pyyntösanoma (GetCertificateRequest)

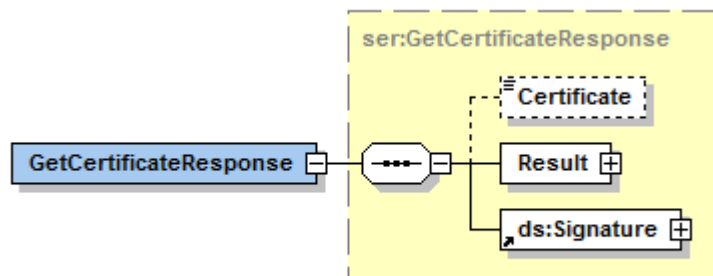


Tietoryhmän *GetCertificateRequest* tiedot:

Tiedon nimi	Tyyppi	Sallitut arvot	Elementin pakollisuus (minOccurs: maxOccurs)	Tiedon selite
Ympäristö (Environment)	ser:EnvironmentTypes	PRODUCTION, TEST	1:1	Tuotantoympäristössä arvon on oltava PRODUCTION ja testiympäristössä arvon on oltava TEST.
Asiakkaan tunniste (CustomerId)	ser:String30		1:1	Asiakkaan tunniste. Tunnisteena käytetään organisaation virallista, Verohallinnon kanssa asiointiin käytettyä tunnistetta. Tunniste voi olla esimerkiksi Y-tunnus. Jos käytetään Y-tunnusta, tunniste on oltava Yritys- ja yhteisötietojärjestelmässä (YTJ) ja tunnisteessa on oltava väliviiva.
Asiakkaan nimi (CustomerName)	ser:String100		0:1	Asiakkaan nimi. Tietoa ei sellaisenaan käytetä varmenteella, mutta se auttaa mahdollisessa virheselvittelyssä.
Varmenteen noutotunnus (RetrievalId)	ser:String32		1:1	Noutotunnus, jonka PKI-järjestelmä palauttaa varmenteen pyyntösanomalle tai varmenteen uusimissanomalle.



5.6 Varmenteen noutaminen – vastaussanoma (GetCertificateResponse)



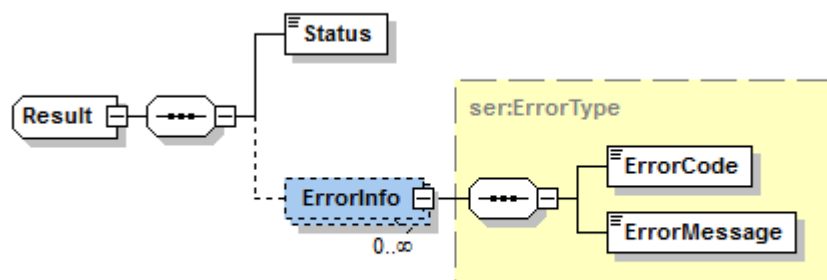
Tietoryhmän *GetCertificateResponse* tiedot:

Tiedon nimi	Tyyppi	Sallitut arvot	Elementin pakollisuus (minOccurs: maxOccurs)	Tiedon selite
Asiakkaan varmenne (Certificate)	ser:CertificateType		0:1	PKI-järjestelmän allekirjoittama asiakkaan varmenne. Varmenne toimitetaan Base64-koodattuna.
Käsittelyn lopputulos (Result)	ser:Result		1:1	Käsittelyn lopputulos, ks. tarkempi sisältö elementin Sanoman käsittelyn lopputulos kuvauksesta.
XML-allekirjoitus (Signature)	ds:Signature		1:1	XML-allekirjoitus, jonka PKI-järjestelmä muodostaa omalla varmenteellaan.



5.7 Sanoman käsittelyn lopputulos (Result)

Tämä tietorakenne kuvaa Result-elementin tietosisällön. Elementti kuvaa käsittelyn lopputuloksen varmenteen pyytämiseen, uusimiseen tai noutamiseen liittyvillä vastaussanomilla. Virhetilanteessa elementti sisältää käsittelyn lopputuloksen lisäksi virheen tiedot.



Tietoryhmän *Result* tiedot:

Tiedon nimi	Tyyppi	Sallitut arvot	Elementin pakollisuus (minOccurs: maxOccurs)	Tiedon selite
Sanoman käsittelyn lopputulos (Status)	ser:ResultTypes	FAIL, OK	1:1	Sanoman käsittelyn lopputulos. Virhetilanteessa palautetaan arvo FAIL, ja tarkemmat tiedot virheestä toimitetaan elementissä Virheen tiedot. Käsittelyn onnistuessa palautetaan arvo OK, ja elementtiä Virheen tiedot ei palauteta.
Virheen tiedot (ErrorInfo)	ser:ErrorType		0:unbounded	Elementissä palautetaan virheilmoitukset.



Tiedon nimi	Tyyppi	Sallitut arvot	Elementin pakollisuus (minOccurs: maxOccurs)	Tiedon selite
Virhekoodi (ErrorCode)	ser:String10		1:1	Elementissä palautetaan virheen koodi.
Virhekoodin selite (ErrorMessage)	ser:String255		1:1	Elementissä palautetaan virhekoodin selite.

Virhetilanteiden virhekoodit ja virhekoodien selitteet on kuvattu luvussa 6.



6 VIRHEKODIT JA VIRHEKODIEN SELITTEET

Uuden varmenteen pyytäminen – vastaussanomien mahdollisesti palauttavat virhetilanteet:

Virhekoodi	Virhekoodin selite	Virheen kuvaus
PKI005	Wrong environment type specified	Pyyntösanoman parametrin ympäristö (Environment) arvo ei vastaa kohdejärjestelmään määritettyä arvoa. Parametrin arvon korjauksen jälkeen toimintoa voi yrittää uudelleen.
PKI020	Invalid credentials	Jokin annetuista tunnistuksista, asiakkaan tunniste (CustomerID), siirtotunnus (TransferId) tai kertakäyttösalasana (TransferPassword) on virheellinen. Syötettyjen parametrien tarkistuksen ja korjaamisen jälkeen on tehtävä uusi varmennepyyntö.
PKI030	Attached CSR is not valid	Pyyntösanomaan liitetty varmenteen allekirjoituspyyntö (CSR) on virheellinen. Uuden allekirjoituspyynnön luomisen jälkeen toimintoa voi yrittää uudelleen.
PKI040	The certificate signing request (CSR) is invalid or has been used already.	Varmenteen allekirjoituspyyntö (CSR) on virheellinen tai jo aiemmin käytetty. Luo uusi allekirjoituspyyntö ja yritä uudelleen. Jos ongelma jatkuu, ota yhteyttä varmennepalvelun havaintolomakkeella.
PKI099	Generic Technical Error	Virhetilanne, jolle ei ole erikseen määritettyä virhekoodia. Virheellisen kutsun muoto ja tiedot tulee tarkistaa. Jos virhe toistuu usein, tulee ottaa yhteyttä Verohallinnon varmennepalvelun havaintolomakkeella.

Voimassa olevan varmenteen uusiminen – vastaussanomien mahdollisesti palauttavat virhetilanteet:

Virhekoodi	Virhekoodin selite	Virheen kuvaus
PKI005	Wrong environment type specified	Pyyntösanoman parametrin ympäristö (Environment) arvo ei vastaa kohdejärjestelmään määritettyä arvoa. Parametrin arvon korjauksen jälkeen toimintoa voi yrittää uudelleen.
PKI010	Signature verification failed	Varmenteen uusiminen -pyyntösanoman sisällön allekirjoituksen tarkistus epäonnistui. Sanoma tulee



Virhekoodi	Virhekoodin selite	Virheen kuvaus
		allekirjoittaa sillä varmenteella, joka halutaan uusia. Mahdollisen virheellisen allekirjoituksen korjaamisen jälkeen kutsun voi uusia.
PKI015	Invalid certificate to be renewed received	Varmenne, jolla pyyntösanoma on allekirjoitettu, on virheellinen tai ei sisällä vaadittuja tietoja. Varmennepyyntö voidaan uusia, kun sanoma on allekirjoitettu oikealla varmenteella.
PKI030	Attached CSR is not valid	Varmenteen allekirjoituspyyntö (CSR) on virheellinen. Uuden allekirjoituspyynnön luomisen jälkeen toimintoa voi yrittää uudelleen.
PKI040	The certificate signing request (CSR) is invalid or has been used already.	Varmenteen allekirjoituspyyntö (CSR) on virheellinen tai jo aiemmin käytetty. Luo uusi allekirjoituspyyntö ja yritä uudelleen. Jos ongelma jatkuu, ota yhteyttä varmennepalvelun havaintolomakkeella.
PKI080	Certificate renewal not yet allowed	Varmenne voidaan uusia vasta, kun sen vanhenemiseen on aikaa enintään 60 vuorokautta.
PKI099	Generic Technical Error	Virhetilanne, jolle ei ole erikseen määritettyä virhekoodia. Virheellisen kutsun muoto ja tiedot tulee tarkistaa. Jos virhe toistuu usein, tulee ottaa yhteyttä Verohallinnon varmennepalvelun havaintolomakkeella.

Varmenteen noutaminen – vastaussanomien mahdollisesti palauttavat virhetilanteet:

Virhekoodi	Virhekoodin selite	Virheen kuvaus
PKI005	Wrong environment type specified	Pyyntösanoman parametrin ympäristö (Environment) arvo ei vastaa kohdejärjestelmään määritettyä arvoa. Parametrin arvon korjauksen jälkeen toimintoa voi yrittää uudelleen.
PKI020	Invalid credentials	Jokin annetuista tunnistuksista, asiakkaan tunniste (CustomerID), siirtotunnus (TransferId) tai kertakäyttösalasana (TransferPassword) on virheellinen uutta varmennetta pyydettyäessä tai varmennetta uusiessa. Tunnistetietojen



Virhekoodi	Virhekoodin selite	Virheen kuvaus
		tarkistuksen jälkeen alkuperäinen varmennepyyntö tai voimassa olevan varmenteen uusiminen ja varmenteen nouto pitää suorittaa uudelleen. Pelkkä varmenteen noudon uusiminen palauttaa alkuperäisen PKI020-virheen.
PKI099	Generic Technical Error	Virhetilanne, jolle ei ole erikseen määriteltyä virhekoodia. Virheellisen kutsun muoto ja tiedot tulee tarkistaa. Virhetilanne syntyy esimerkiksi silloin, kun varmenne noudetaan liian nopeasti varmenteen pyytämisen tai uusimisen pyyntösanoman jälkeen, jolloin PKI-järjestelmä ei ole vielä ehtinyt käsitellä pyyntösanomaa. Jos virhe toistuu usein, tulee ottaa yhteyttä Verohallinnon varmennepalvelun havaintolomakkeella. Koska palvelu on luonteeltaan asynkroninen, virhe on voinut syntyä jo aikaisemmin. Esimerkiksi varmennetta pyydettäessä tai uusittaessa on voitu antaa virheellisiä tietoja ja varmenteen luominen on epäonnistunut.



7 TESTIPENKIN OHJEET

Varmennepalvelun testipenkin tarkoitus on helpottaa varmennepalvelun rajapintaa käyttävän sovelluksen kehittämistä. Testipenkissä on mahdollista testata varmenteen allekirjoituspyynnön lähetystä, varmenteen uusimispyynnön lähetystä ja varmenteen noutoa.

Testipenkissä käytetään ennakoon määriteltyjä kertakäyttöisiä tunnisteita, PKI-avaimia ja varmenteita. Tästä johtuen Web Service -pyyntöjä voi toistaa useita kertoja käyttäen samoja parametreja. Esimerkiksi ”Uuden varmenteen allekirjoituspyynnön” siirtotunnusta (TransferId) ja ”kertakäyttösalasanaa” (TransferPassword) voi käyttää monta kertaa.

Testipenkistä saatavia varmenteita ei voi käyttää Verohallinnon, tulorekisterin tai positiivisen luottotietorekisterin rajapinnoissa.

7.1 Testimateriaali

Testipenkissä on pysyvästi voimassa oleva varmennetilauksella sekä kaksi esivalmistettua varmennetta ”Varmennepyyntö” ja ”Varmenteen uusimista” varten. Tässä luvussa on ohjeet testipenkin käyttöä varten. Lisäksi käyttäjä tarvitsee testausta varten julkaistut testiavaimet (PKI yksityinen avain).

Nämä testiavaimet on julkaistu zip-pakettina: <https://vero.fi/globalassets/tietoa-verohallinnosta/ohjelmistokehittäjille/varmennepalvelu/varmennepalvelu-testipenkki.zip>

Zip-paketti sisältää seuraavat tiedostot:

- SignNewCertificate_Private.key
 - o Tämä yksityinen avain on tarkoitettu uuden varmenteen allekirjoituspyynnön (CSR) luontiin (signNewCertificate-operaatio) ja varmenteen uusimisen (renewCertificate-operaatio) SOAP-sanoman XML-allekirjoituksen muodostamiseen.
- RenewCertificate_Private.key
 - o Tämä yksityinen avain on tarkoitettu varmenteen uusimisen yhteydessä varmenteen allekirjoituspyynnön (CSR) luontiin (renewCertificate-operaatio).

Testiavaimiin liittyvät testivarmenteet on uusittu heinäkuussa 2020 ja ne ovat voimassa heinäkuuhun 2030 saakka. Samassa yhteydessä vaihtuivat testivarmenteiden noutamiseen tarvittavat RetrievalId-tunnisteet. Uudet tunnisteet on listattu tässä dokumentissa.

7.1.1 Testipenkin palveluissa käytettävät parametrit

Testipenkin Web Service -palveluissa on **käytettävä** alla lueteltuja ennalta määriteltyjä tietoja.

1. Uuden varmenteen allekirjoituspyynnön lähetys (signNewCertificate)

- Environment: TEST
- CustomerId: 0123456-7
- CustomerName: Ab PKI Developer Company Oy
- TransferId: 12345678903
- TransferPassword: Pw8a1d4u3HhOqhlo
- CertificateRequest: <PKCS#10-muotoinen Base64-koodattu merkkijono>

CertificateRequest (CSR) -tiedon muodostus on tehtävä 'SignNewCertificate_Private.key' -avainta käyttäen. Tällöin on mahdollista yhdistää palvelun palauttama varmenne tähän samaan yksityiseen avaimeen. On mahdollista toteuttaa CSR myös itse muodostamallaan avaimella, mutta tällöin palautettua varmennetta ei voida yhdistää käyttäjän avaimeen.

2. Voimassa olevan varmenteen uusimisen allekirjoituspyynnön lähetys (renewCertificate)

- Environment: TEST
- CustomerId: 0123456-7
- CustomerName: Ab PKI Developer Company Oy
- CertificateRequest: <PKCS#10-muotoinen Base64-koodattu merkkijono>
- Signature: <XML Signature mukainen elementti>

CertificateRequest (CSR) -tiedon muodostus on tehtävä 'RenewCertificate_Private.key' -avainta käyttäen. Tällöin palvelun palauttama varmenne voidaan yhdistää tässä yhteydessä käytettyyn yksityiseen avaimeen. Myös tässä yhteydessä on mahdollista toteuttaa CSR itse muodostamallaan avaimella, mutta sitä ei voida yhdistää käyttäjän avaimeen.

Signature-elementti on muodostettava 'SignNewCertificate_Private.key' -avainta käyttäen. Signature-elementin X509Certificate-tietoon on liitettävä varmennepalvelun testipenkistä noutoavaimella (RetrievalId) 990639930742461205 saatu varmenne (katso kohta 3. Varmenteen noutaminen).

3. Varmenteen noutaminen (getCertificate)

- Environment: TEST
- CustomerId: 0123456-7
- CustomerName: Ab PKI Developer Company Oy



- RetrievalId: <Uuden varmenteen pyyntöön saatu vastaus>

Varmenteen nouto-operaatiolla voi hakea kaksi esivalmisteltua varmennetta. Noudettaessa varmennetta, joka on "muodostettu" testipenkin signNewCertificate-operaatiossa käytetyllä yksityisellä avaimella, on käytettävä noutotunnusta (RetrievalId) 990639930742461205. Mikäli haluaa noutaa varmenteen, joka liittyy renewCertificate-operaatiossa käytettyyn yksityiseen avaimeen, käytetään noutotunnusta 11885819811430372306.

Testipenkissä ei ole varmennetta uusitun varmenteen (renewCertificate-operaatiosta saatu varmenne) uusimiseen, vaan testipenkki palauttaa "Voimassa olevan varmenteen uusimiseen" aina saman esivalmistetun varmenteen.

7.2 Testipenkin yhteysosoite

Varmennepalvelun testipenkki sijaitsee varmennepalvelun testiympäristön yhteydessä. Sen osoite poikkeaa varsinaisen testiympäristön osoitteesta palvelun kontekstissa olevan /DEV-kohdan osalta. Osoite kokonaisuudessaan on: <https://pkiws-testi.vero.fi/DEV/2017/10/CertificateServices>

Huom! osoite ei aukea selaimeen, vaan sitä käytetään rajapintojen testiohjelmista kuten SoapUI tai Curl.

7.3 Testipenkin palveluiden virhetilanteet

Testipenkin virhekäsittely ei ole siinä käytettyjen rajallisten varmenteiden ja niiden elinkaaren takia täysin tuotantoa vastaava. Tyypillisimmät virhetilanteet on esitelty tässä kappaleessa. Kattava listaus palvelun virhekoodeista on luvussa 6.

Uuden varmenteen pyynnössä CSR on virheellinen: palautuu virhekoodi PKI030, Attached CSR is not valid.

SOAP-ENV:Body	
ns4:SignNewCertificateRe...	
Result	
Status	FAIL
ErrorInfo	
ErrorCode	PKI030
ErrorMessage	Attached CSR is not valid

Uuden varmenteen pyynnössä TransferId on virheellinen: palautuu virhekoodi PKI020, Invalid Credentials.

SOAP-ENV:Body	
ns4:SignNewCertificateResponse	
Result	
Status	FAIL
ErrorInfo	
ErrorCode	PKI020
ErrorMessage	Invalid Credentials

Varmenteen noudossa RetrievalId on virheellinen: palautuu virhekoodi PKI099, Generic Technical Error.

SOAP-ENV:Body	
ns4:GetCertificateResponse	
Result	
Status	FAIL
ErrorInfo	
ErrorCode	PKI099
ErrorMessage	Generic Technical Error

Varmenteen uusimisen allekirjoitus on virheellinen: palautuu virhekoodi PKI010, Signature verification failed.

SOAP-ENV:Body	
ns3:RenewCertificateResponse	
Result	
Status	FAIL
ErrorInfo	
ErrorCode	PKI010
ErrorMessage	Signature verification failed



8 ESIMERKKISANOMIA

Seuraaviin esimerkkeihin on käytetty SmartBear Software ReadyAPI -ohjelmaa.

8.1 Varmenteen nouto (getCertificate)

Request Generate Values

XML Raw Outline **Form**

✓ View Type: All ⓘ

☒ **GetCertificateRequest** GetCertificateRequest

Environment *: TEST (EnvironmentTypes)

CustomerId *: 0123456-7 (String30)

CustomerName: Ab PKI Developer Company Oy (String100)

RetrievalId *: 990639930742461205 (String32)



Response Smart Assertion

XML Raw Outline Overview

Transfer to Assert

XML Node	Value	
SOAP-ENV:Envelope		(Envelope)
SOAP-ENV:Header		(Header)
SOAP-ENV:Body		(Body)
ns4:GetCertificateResponse		(GetCertifica...
Certificate	MIIFqzCCA5OgAwIBAgIIIGZoeTGyXo3lwDQYJKoZlh...	(CertificateT...
Result		(Result)
Status	OK	(ResultTypes)
ds:Signature		(SignatureT...

Jos asiakas tallettaa vastauksena saadun varmenteen tiedostoon, siihen voi joutua lisäämään varmenteen alku- ja lopputunnisteet (BEGIN ja END):

-----BEGIN CERTIFICATE-----

.... base64-koodattu varmenne...

-----END CERTIFICATE-----

Jotkin ohjelmat ja käyttöjärjestelmät vaativat tunnisteet, jotta osaavat avata varmenteen.

8.2 Varmenteen uusiminen (renewCertificate)

Jos varmenteen allekirjoituspyynnön (CertificateRequest) luonnissa käytetty ohjelma lisää CSR-tiedostoon alku- ja lopputunnisteet (BEGIN ja END), **käyttäjän pitää poistaa ne**. Vain base64-koodattu osa lähetetään:

-----BEGIN CERTIFICATE REQUEST-----

.... base64-koodattu varmenteen allekirjoituspyyntö

-----END CERTIFICATE REQUEST-----



Request

Generate Values

XML Raw Outline **Form**

✓ View Type: All ⓘ

☒ **RenewCertificateRequest** RenewCertificateRequest

Environment *: **TEST** (EnvironmentTypes)

CustomerId *: **0123456-7** (String30)

CustomerName: Ab PKI Developer Company Oy (String100)

CertificateRequest *: **aaq/m9qHUu/3qBRz/DDoEIU0dIINoT5JMM=** Browse... Clear (CertificateRequest)

☒ **Signature** SignatureType

Response

Smart Assertion

XML Raw **Outline** Overview

⌵ ⌵ ⌵ ⌵ ⌵ ⌵ ⌵ ⌵ xs: Transfer to ▼ Assert ▼ ⓘ

XML Node	Value	
[-] SOAP-ENV:Envelope		(Envelope)
[-] SOAP-ENV:Header		(Header)
[-] SOAP-ENV:Body		(Body)
[-] ns4:RenewCertificateResponse		(RenewCerti...
RetrieveId	11885819811430372306	(String32)
[-] Result		(Result)
Status	OK	(ResultTypes)
[-] ds:Signature		(SignatureT...
[-] ds:SignedInfo		(SignedInfo...



zKP8UUnJK8PmptJQo+E6jIEy+vzSsHouf0UMCgp9MutN9RIAtjqS6lyHtqp8BLn2hdEM1srIqCXB
RigkAH5w1mqbBSiVkgScaYJ+I5AY201ZTUlb138SY/bYk9gflS1aY1gEF+667Bmys0aJk4JRLHuj
MqfkEuHrfRWo1ps739H+8UPqkRmJfNybgFUPoJEwcfGIkXdYGPUCawEAAaOCAWswggFnMAwGA1Ud
EwEB/wQCAAAwHwYDVR0jBBgwFoAUZeehBs4guH858QDh/4DceYSqbCAwUwYIKwYBBQUHAQEERzBF
MEMGCCsGAQUFBzACHjdodHRwOi8vY3JsLXRlc3RpLnZlcm8uZmkvY2EvUetJU2VydmljZURldmVs
b3BlckNBdjEuY2VyMBMGA1UdJQMMMAoGCCsGAQUFBwMCMIGcBgNVHR8EgZQwgZEwgY6gPKA6hjho
dHRwOi8vY3JsLXRlc3RpLnZlcm8uZmkvY3JsL1BLSVNlcnZpY2VEZXZlbG9wZXJlDQXyXmNybkJO
pEwwSjEkMCIGA1UEAwWbUetJIFNlcnZpY2UgRGV2ZWxvcGVyIENBIHYxMRUwEwYDVQQKDAxWZXJv
aGFsbGludG8xCzAJBgNVBAYTAkZJMB0GA1UdDgQWBBQwtQwXI5AZJVyZf4DEemCYLnw+mzAOBgNV
HQ8BAf8EBAMCBaAwDQYJKoZIhvcNAQELBQADggIBAESy5Vom5gsk7YYAesYRCB3IMAR1VTGtbKH
s+oZxUJKHl8/K2bgGMLKyYbAySxDMD/SfnxO4TXU/1IOedBYp4D9oe8eKlyBmWwG1XdpJ8W2LCvx
+CMrolcwF/5D38pMnxW5sFebTFp7v7m2ZnI5nrdDLNG1XGdF/A4M3ZJ8RymJYG8jC/F3dTao1LWx
9wAevsRwzYm2Y4+CdW/J1wN28vHXJKG6qJsMLrpeBRC27MAqgN2h9NsJnimLKCKdXHPqrW4HKNEe
uXs2bxzHLN17A45RxBpTGnDY3Y6seu4Uw/4U/1ptFyeE8cdC8Gsu++3oOWRfJv5O4mVczGtX4iEk
hgmZTJNYRDEmKqtDN7aNXkoHZ66lgU31vK6M/aiu0FTWr7tugdKVydfNy65XBixM4GCYyGtWRuwu
89ojQnrSQ3h6a4N6jtweAaui0T04UCTr0aZFL6TiGBicjMez/8w1YzAmJ3+a0/ZGL6Q/WU5jPiJf
vNldJoNqyk+IKESr01loT5Cy+kg2Bzt5Pk+R4KdOERX8TedTxH5U/L/QfUXqGtyfl1768QxB7kaF
9T1CSuXAdR2O+JeYUkekV7WgtrbXA/Y8mZ04HZe7kgIH4WJRAkdZXIhPJqS4GudEx6YKZsrC6W0T
wQ9x/30aaIdulABePI3nVEUkGOYRetjoRBOQNckW</X509Certificate></X509Data></KeyInfo></Signature></cer:RenewCertificateRequest></soapenv:Body>



9 ESIMERKKI VARMENTEEN UUSIMISESTA JA ALLEKIRJOITUKSEN (CSR) LUOMISESTA

Tämä ohje kuvaa yhden tavan suorittaa Verohallinnon varmennepalvelun myöntämän varmenteen uusiminen ja allekirjoituksen luominen käyttäen Verohallinnon varmennepalvelun PKI-järjestelmän Web Service -rajapintaa. Esimerkin perusteella varmenteen uusimisen voi toteuttaa omaan ohjelmistoon.

Ohjeessa on kuvattu testivarmenteen uusiminen. Ohje on sovellettavissa myös tuotantovarmenteen uusimiseen. Silloin käytetään aitoja asiakastietoja ja varmennepalvelun tuotanto-osoitetta. Testiympäristössä ei saa käyttää tuotannon asiakastietoja.

Tarvittavat asiat:

- PKI-osaamista avainparin muodostamista ja allekirjoituspyynnön muodostamista varten
- Ohjelmointiosaamista, allekirjoitusohjelman kääntäminen ja suorittaminen
- Varmennepalvelun sanomarakenteet, WSDL-paketti: https://vero.fi/globalassets/tietoa-verohallinnosta/ohjelmistokehittajille/varmennepalvelu/varmennepalvelu-rajapinta_v1.01.zip
- Uusi avainpari varmenteen allekirjoituspyyntöä varten (CSR)
- Nykyinen varmenne ja siihen liittyvä yksityinen avain xml-sanoman allekirjoittamista varten
- Organisaatiosi käytössä oleva Web Service -varmenteen keinotekoinen Y-tunnus ja keinotekoinen yrityksen nimi
- Mahdollinen pfx-tiedosto, jossa nykyiseen varmenteeseen liittyvä yksityinen avain
- Nykyisen pfx-tiedoston salasana

Tarvittavat työvälineet:

- OpenSSL: <https://wiki.openssl.org/index.php/Binaries>
- .NET Core 3.1 tai uudempi: [.NET Downloads \(Linux, macOS, and Windows\) \(microsoft.com\)](https://dotnet.microsoft.com/download/linux-macos/windows)
- Visual Studio Code: <https://code.visualstudio.com/>
- Verohallinnon allekirjoitusohjelman esimerkkitoteutus, ladattavissa täältä (SignXmlNew.cs): https://www.vero.fi/globalassets/tietoa-verohallinnosta/ohjelmistokehittajille/swaggerui/verohallinto_program.zip
- SoapUI <https://www.soapui.org/downloads/soapui/> tai Curl <https://curl.se/download.html>

Lisätietoja:

- Ohjeet uusimiseen: [Varmenteen uusiminen](#)
- Dokumentaatio Verohallinnon varmennepalvelun sivuilla: [Dokumentaatio](#)
- Varmennepalvelun testipenkin ohje (tämän dokumentin luvussa 7)
- Vero API - ja ApitamoPKI-asiakkaille on olemassa Slack-kanava: <https://vero-api.slack.com>
 - Liity kanavalle API-havaintolomakkeen kautta.

■ Verohallinnon varmennepalvelun havaintolomake

Testivarmenteen uusiminen

1. Luo uutta varmennetta varten uusi yksityinen avain

Luo yksityinen avain OpenSSL-ohjelmalla komennolla:

```
openssl genrsa -out newprivate.key 2048
```

Uusi luotu yksityinen avain muodostuu tiedostoon newprivate.key

2. Luo uusi varmenteen allekirjoituspyyntö uusimista varten

Muodosta varmenteen allekirjoituspyyntö (CSR) käyttäen kohdassa 1 luotua yksityistä avainta esim. OpenSSL-ohjelmalla komennolla:

```
openssl req -new -key newprivate.key -out certificaterequest.csr
```

Syötä seuraavat tiedot OpenSSL:lle uusittavan varmenteen tietojen mukaisesti:

Country Name = *FI*

Organization Name = *Käytössänne olevan testiyrityksen nimi*

Common Name = *käytössänne oleva keinotekoinen y-tunnus*

Uusi varmenteen allekirjoituspyyntö muodostuu tiedostoon certificaterequest.csr

3. Muodosta xml-sanoma allekirjoittamista varten

Muodosta varmenteen uusimisen xml-sanoman sisältöosa uusimisrajapintaa varten. **Vain tämä osuus sanomasta allekirjoitetaan.** Käytä oheista templatea, huomaa että editorit saattavat lisätä rivinvaihtoja, eli **suositellaan** poistamaan rivinvaihdot templaatista ennen allekirjoituksen muodostamista:

```
<cer:RenewCertificateRequest xmlns:cer="http://certificates.vero.fi/2017/10/certificateservices" xmlns:xd="http://www.w3.org/2000/09/xmldsig#">
  <Environment>TEST</Environment>
  <CustomerId>Käytössänne oleva keinotekoinen y-tunnus</CustomerId>
  <CustomerName>Testiyrityksen nimi</CustomerName>
  <CertificateRequest>Kohdassa 2 muodostettu varmenteen allekirjoituspyyntö eli csr-tiedoston sisältämä base64 merkkijono ilman --- begin certificate request -- ja
  --- end certificate request --- otsikoita</CertificateRequest>
```



</cer:RenewCertificateRequest>

Täytä esimerkisanoman kenttiin testivarmenteesi Y-tunnus (keinotunnus), keinotekoinen yrityksen nimi sekä kohdassa 2 luomasi uusi varmenteen allekirjoituspyyntö (base 64 merkkijono, ilman "--- begin certificate request---" alku- ja loppuotsikoita). Tallenna xml-tiedosto levyille allekirjoittamista varten, ilman rivinvaihtoja.

4. Allekirjoita xml-sanoma

Muodosta allekirjoitus sanoman sisältöosalle eli osalle, joka on muodostettu kohdassa 3. Voit käyttää valmiita ratkaisuja esim. XML Signer -ohjelmaa tai toteuttaa itse tai käyttää Verohallinnon esimerkkitoteutusta. Tämä ohje hyödyntää Verohallinnon C#-toteutusta. Esimerkkitoteutus olettaa, että nykyinen varmenne on pfx-tiedostossa.

Lataa allekirjoitusohjelman esimerkkitoteutus sivulta [Dokumentaatio](#) tai luvun 9 alusta.

Suorittaaksesi ohjelman lataa .net core 3.1 -kirjastot sekä sopiva kehitysympäristö, esim. Visual Studio Code: <https://code.visualstudio.com/>

4.1 Muodosta pfx-tiedosto allekirjoitusohjelmalle Open SSL:n avulla

Uutta pfx-tiedostoa ei tarvitse tehdä, jos sinulla on jo sellainen olemassa Vero API -käyttöä varten. Etene tällöin suoraan vaiheeseen 4.2.

Suorita oheinen komento, joka muodostaa pfx-tiedoston. Tiedostoon viedään nykyinen varmenne ja yksityinen avain, jolla se on muodostettu.

Jos pfx-tiedostoa ei jo ole, muodosta pfx-tiedosto seuraavalla komennolla, jolloin siihen viedään yksityinen avain sekä nykyinen varmenne (tallennettu cert.cer-tiedostoon base64 muodossa):

```
openssl.exe pkcs12 -export -out test.pfx -inkey private.key -in cert.cer
```

Nykyisin käytössä olevan varmenteen yksityinen avain on komennon syötteessä private.key-tiedostossa base64-muodossa suojaamattomana sekä varmenteen julkinen osa (= allekirjoitettu julkinen avain) on cert.cer-tiedostossa base64-muodossa.

OpenSSL kysyy salasanaa, jolla pfx-tiedosto suojataan. Salasanaa tarvitaan allekirjoitusohjelmassa. Lopputuloksena muodostuu uusi test.pfx-tiedosto.

Jos kokeilet testipenkissä:

Muodosta pfx-tiedosto yllä olevalla komennolla, jolloin siihen viedään yksityinen avain, testipenkin SignNewCertificate_Private.key-tiedosto sekä testipenkistä noudettu nykyinen varmenne, joka on tallennettu cert.cer-tiedostoon base64 muodossa.

4.2 Aja allekirjoitusohjelma

Käännä ja suorita allekirjoitusohjelma (SignXmlNew.exe) ja anna komentoriviparametrina kohdassa 3 luomasi allekirjoitettava xml-sanoma, pfx-tiedosto ja sille luomasi salasana:

SignXmlNew.exe renew.xml test.pfx password

Lopputuloksena syntyy allekirjoitettu xml-tiedosto renew_signed.xml, alla oleva esimerkki testipenkistä:

```
<cer:RenewCertificateRequest xmlns:cer="http://certificates.vero.fi/2017/10/certificateservices" xmlns:xd="http://www.w3.org/2000/09/xmldsig#">
  <Environment>TEST</Environment>
  <CustomerId>0123456-7</CustomerId>
  <CustomerName>Ab PKI Developer Company Oy</CustomerName>
  <CertificateRequest>MIICJTCCAXUCAQAwSDELMAGGA1UEBhMCRkkxEzARBgNVBAGMCINvbWUuU3RhZGUx
  JDAiBgNVBAoMGOiFBLSSEBZlG9wZXIqQ29tcGFueSBPeTCCASlwDQYJKoZI
  hvCNAQEBAQADggEPADCCAQoCggEBAJkBP88eLdbxbJfPluDI/rNP0EUpluRohxgx
  MNfuYVV9kXgrMsOZpCsV/QjwZFpWBSFy6PDJIKyVAqe83XSfoGPt9apy3QaUJUxR
  4/P5H6VT+eZpt1TCf5CEaKb0aW4bZ1kN9BLerrJ81HsR6cutpE/t0bzArc4kna/I
  rz/yB3tIU34YoHyx9bXNwKSPsUdL7N32vluSO8Me/3NjFzA9CBYRrP58qnXlyTmm
  0x5GJXGBJqJM2xBRCompMWg5WGUOF8mAGxkPDxyEfZpaHXbSLaBQ1nJyDPg0+n/Ak
  rcweydE0BKmMh3rSITH/M5DYZ6yKgHABEWERg1Nz06ei+a+KJUcCAwEAAaAAMA0G
  CSqGSIB3DQEBECwUAA4IBAQBslqCulgyrfU+DVZxS60Hvu4d8GcKKRGCTFBt508BM
  c+NsnvgaKwZXXMWKOJStsDHsOPnwfalvImFLWRkAsqxt2dIGgWMzFh9NaX0Anwm
  CbiUruot9C8zguP7Y/67AFSeageNYrHmgIBHoZyNle+tPR4Y5DxcQBI/6HtyzJ/q
  Nej5mp2zSIW5P1QoEkS3MU8Gm0mpCBylyAvCzeYHOop6caZMQctVCmPto+0PYx0T
  qEmO15vGj/rIN4btjEKSYfjNj56MMN8lslc/6vqdikkKmMwTLRXjq73liOYyJ11s
  9433VK1J/UMvay3y2jYKVDUuW567HD8C3lsT+A+ifkCo</CertificateRequest>
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#"><SignedInfo><CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
  /><SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" /><Reference URI=""><Transforms><Transform
  Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" /></Transforms><DigestMethod
  Algorithm="http://www.w3.org/2001/04/xmldsig#sha256"
  /><DigestValue>i13a6CV9yr+uqy/qx4yhvyysDvcKnoiNlUdj7Arr1A=</DigestValue></Reference></SignedInfo><SignatureValue>VEja46Y17laMXHMJfcZMRM+3zPTL
  Sepv/zWeR2JLMMcz3nWldJynhs1MjGMBqj3gLsebmokE3UX10ToZ0LObtbeACFYz78dDKbWHTc4cU1IWkZU3DpXQ5svgJWNk1L+B2SDH7V+ethFNqBmwLCgsE2dT8p
  t7rXwsBOnZe/Rt30fIEMd5sSWYYJeb1FzMXAcafVloVs31T9HcoCFupgMH9YWsgzpknQHTSTKfjBZbhsjBnvnDIwSceFhxxNpcmy/zVjRVB56WeC2qhQgZFN7PsnCJ6KnNO
  TkYr2w7CVCfNwofCMU3eXUI+n5khTJmNQV+SZ2S0qPzBSp6TD/reCVJHA==</SignatureValue><KeyInfo><X509Data><X509Certificate>MIIFqzCCA5OgAwIBAgIIIGZoe
  TGyXo3IwDQYJKoZIhvcNAQELBQAwSjEKMCIgA1UEAwWbUETjIFNlcnZpY2UgRGV2ZWxvcGVyIENBIHYxMRUwEwYDVQKDAxWZlJvaGFsGludG8xCzAJBgNVBAYTAk
```



ZJMB4XDTIwMDcwNjA4MzYzMloXDTMwMDcwNDA4MzYzMlowcjESMBAGA1UEAwWJMDEyMzQ1Ni03MSkwJwYDVQQFEyBDNDY4MTkxMDdCNDAXNUlOMUIzMTA0MTEwMUEOREE2RDEkMCIGA1UECgwbQWlglUEtJERldmVsb3BlciBDb21wYW55IE95MQswCQYDVQQGEWJGSTCCASlwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAmrF+WUx2nuYBOeG3PxqzleMmMVRwlqmBTH/jdW0AmRZ34cuH+Do/T6U0mqg9G4IVsj8WaM8fmh7tdCQ3xcCPnqpQrkeGuWQV4nIhok74kDnQb12FrOKCsLIOMONHS2+9E8HKwS8giFXzKP8UUnJK8PmptJQo+E6jIEy+VzSsHouf0UMCgp9MutN9RIAtjqS6lyHtqp8BLn2hdEM1srIqCXBRIgAH5w1mqbBSiVkgScaYJ+I5AY201ZTUlb138SY/bYk9gflS1aY1gEF+667Bmys0aJk4JRLHujMqfkeUhrfRwo1ps739H+8UPqkRmJfNybGFUPoJEwcfGikXdYGPUCAwEAAOCAWswggFnMAwGA1UdEwEB/wQCMAAwHwYDVROjBBgwFoAUT1PJe8BCr9h+uQE8W6CNC7/QfeYwUwYIKwYBBQUHAQEERzBFMEMGCCsGAQUFBzAChjdodHRwOi8vY3JsLXRlc3RlLnZlcm8uZmkyY2EvUetJU2VydmljZURldmVsb3BlckNBdjEuY3J0MBMGA1UdJQMMMAoGCCsGAQUFBwMCMIGcBgNVHR8EgZQwgZewG6Y6PKA6hjhodHRwOi8vY3JsLXRlc3RlLnZlcm8uZmkyY3JsL1BLSVNlcnZpY2VEZXZlbG9wZXJkDQYxLmNybKJOPewwSjEkMCIGA1UEAwWbUetJIFNlcnZpY2UgRGV2ZWxvcGVyIENBIHYxMRUwEwYDVQQKDAXWZlJvaGFsGfSbGludG8xCzAJBgNVBAYTAkZJMB0GA1UdDgQWBBQwtQwXI5AZJVyZf4DEemCYLnw+mzAOBgNVHQ8BAf8EBAMCBaAwDQYJKoZIhvcNAQELBQADggIBADZkkj4T+rVIAe9a53/9zrWLuJqe+WePxIoEk5ozXWDb2FeR0uEyUS2Ba0gVJwPm9Go6CAia3J9nFGyVUUNCm2ofdDGxEX4JkrRc7c08JPaMY74tJR9wwj8R5sshAXPDVMWh9MI8LHG6hqz0ic0IK9cSsAHBGJ3GBIckS/6y+SPWGGKMHOf0QIm5of63qQ8aI950y4aUJL7td2Yxiu6jKUfP4haL0BvJFM///o6Ge5LxT3nfPzXESBLbLE21D0ksyO+fZljleflxleQk9rWY7zYq/Go9+ElvEILXE2aDjqQrwoNIQHmqLgG0DuKpJKzSi7nRvDVHaB5YIdtLDJ4PXZITkib8QBOZWmHCw58IvfEdL0WfuRzpJmIcf8oyzLWRagtnEQhwnWnkXOtPqivRq3Rh35M4mQPNVPikduzYlhvQzwCAVkgzspEZVT5hQITEXBiZZQ8jC8Mb6U1u7G/NndHGwdWn0WtNYDMrhqEZGoHxglTLwaU4d5suHzkv0gIxxkre4fnVdiVWd4zCNQk6rt9Jo3p0yLFGM49G3ksZHPcYxxBmzqSrSBoBKX5Sn9+jOF39fxE6LNCmJBizZ49WhSOTSJx/kL8B0T4NBCtz6EdhQk0Iz1JC5GvNuVVnmKeZYelt3qLvX4ktc6QxIH2zZ48BR+m/cXycvyLzy2fgyAIW</X509Certificate></X509Data></KeyInfo></Signature></cer:RenewCertificateRequest>

Huomaa, että allekirjoitusohjelma on lisännyt RenewCertificateRequest-lohkon loppuun Signature-lohkon.

Tärkeää on, että tiedoston sisältöä ei saa muuttaa millään tavalla ennen sen lähetystä PKI-järjestelmän rajapintaan, jotta allekirjoitettu sisältö ei muuttuisi. Muutoksen aiheuttavat myös rivinvaihdot tai muut muotoilut, jolloin allekirjoitus ei ole enää validi ja varmennepalvelu vastaa virhekoodilla PKI010.

5. Lähetä allekirjoitettu sanoma varmennepalvelun PKI-järjestelmän rajapintaan

Lähetä allekirjoitettu testivarmenteen uusimisen sanoma esimerkiksi SoapUI-ohjelmalla varmennepalvelun PKI-järjestelmän testiosoitteeseen:

<https://pkiws-testi.vero.fi/2017/10/CertificateServices>

SoapUI:hin voit ladata WSDL-kuvauksen perusteella sanomarakenteiden pohjat. Lataa varmennepalvelun rajapintapaketti sivulta [Dokumenttaatio](#) tai luvun 9 alusta. Avaa WSDL-tiedosto SoapUI:lla.

Muodosta lähtevä sanoma siten, että allekirjoitettu sisältö on muuttumattomana soap-envelopen body-elementin sisällä. Älä muotoile millään tavalla allekirjoitettua sisältöä.

Esimerkki soap-envelopesta ja kohta mihin sisältö viedään:

```
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xs="http://www.w3.org/2001/XMLSchema" ><env:Body>
```



tähän allekirjoitettu sisältö sellaisenaan, joka muodostettu ohjeen kohdassa 4

</env:Body></env:Envelope>

Tarkista URL ja lähetä sanoma. Vastauksena tulee OK sekä retrievalID, jolla uusitun varmenteen voi noutaa GetCertificate-operaatiolla.

SoapUI:n sijaan voi käyttää CURL-ohjelmaa, jolloin mm. Windows-ympäristössä on oltava tarkkana, että rivinvaihtoja ei saa olla allekirjoitettavassa sisällössä vaan kaiken sisällön on oltava yhdellä rivillä. Muista lisätä allekirjoitettuun tiedostoon soap-envelope. Oheisella CURL-komennolla voi lähettää uusimispyynnön:

`curl -i -v -d @template_signed_env.xml --header "SOAPAction:renewCertificate" -H "Content-Type: text/xml;charset=UTF-8" -H "Accept-Encoding: gzip,deflate"`
<https://pkiws-testi.vero.fi/2017/10/CertificateServices>

6. Nouda uusittu varmenne GetCertificate-operaatiolla

Hyödynnä noutamisessa varmennepalvelun ohjeistusta.

Säilö pfx-tiedosto ja yksityinen avain huolellisesti.



10 ALLEKIRJOITUKSEN (CSR) LUONTI WINDOWSIN MMC-TYÖKALULLA

Jos käytettävissä ei ole OpenSSL-ohjelmaa, Windows-ympäristössä CSR:n voi luoda myös MMC-työkalulla (Microsoft Management Console). Yksityiskohtaiset ohjeet tähän menettelyyn löytyvät esimerkiksi sivustolta:

<https://knowledge.digicert.com/solution/SO29005.html>

