Versio 1.03

Varmennepalvelu – Rajapintakuvaus

Tulorekisteriyksikkö

Versiohistoria

Versio	Päivämäärä	Kuvaus
1.0	30.10.2017	Dokumentti julkaistu.
1.01	15.12.2017	Dokumenttia päivitetty kohdista 1.1, 1.2, 2.1, 2.2, 3.1, 3.2, 3.3, 3.7 ja 4. 2.2.1 poistettu.
1.02	15.10.2018	Luvussa 1.2: Skeeman url on päivitetty.
1.03	10.4.2019	Dokumenttia päivitetty kohdista 2, 3.1, 3.3, 3.5 ja 4.

SISÄLLYS

1 YLEISTÄ

Tässä dokumentissa kuvataan varmennepalvelun Web Service -rajapinnan toteutus järjestelmäintegraation toteuttajan näkökulmasta. Dokumentissa kuvataan rajapinnan palvelut sekä palveluiden tietosisältö (XML-skeemat).

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

1.1 Web Service -rajapinta

Varmennepalvelun 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

1.2 Skeema

Varmennepalvelun 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.

1.3 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

1.4 Dokumentin lukuohje

Dokumentin kaavioissa olevien elementtien oikeassa alakulmassa oleva merkintä 0 .. ∞ tarkoittaa, että elementti voi toistua useita kertoja ja se voi myös puuttua kokonaan. Merkintä 1 .. ∞ 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

2 VARMENNEPALVELUN WEB SERVICE -RAJAPINTA

Varmennepalvelun Web Service -palveluiden käyttötapaukset ja palveluiden väliset kytkökset on kuvattu dokumentissa Varmennepalvelu – Yleiskuvaus.

Alla olevassa taulukossa on kuvattu rajapinnan palvelut:

Operaatio	Pyyntösanoma	Vastaussanoma	Kuvaus
Uuden varmenteen pyyntö (SignNewCertificate)	SignNewCertificateRequestMessage	SignNewCertificateResponseMessage	Uuden varmenteen pyytäminen silloin, kun • käyttäjä pyytää varmennetta ensimmäisen kerran • käyttäjällä on jo voimassaoleva varmenne/varmenteita, mutta hän tarvitsee lisää varmenteita • käyttäjän edellinen varmenne on vanhentunut tai se on revokoitu eli poistettu käytöstä.
Voimassaolevan varmenteen uusiminen (RenewCertificate)	RenewCertificateRequestMessage	RenewCertificateResponseMessage	Varmenteen uusimispyyntö, kun käyttäjän hallussa oleva varmenne on vanhenemassa ja uusiminen tehdään ennen voimassaolevan varmenteen vanhenemista.
Varmenteen noutaminen (GetCertificate)	GetCertificateRequestMessage	GetCertificateResponseMessage	Aiemmin pyydetyn uuden tai uusitun varmenteen noutaminen. Varmennepyynnön tai voimassaolevan varmenteen uusimisen vastaussanoman ja varmenteen noutamisen pyyntösanoman välillä on oltava vähintään 10 sekunnin viive.

Rajapinnan palveluiden pyyntö- ja vastaussanomien tietosisältö kuvataan tarkemmin luvussa 3.

2.1 Sanomien allekirjoitus

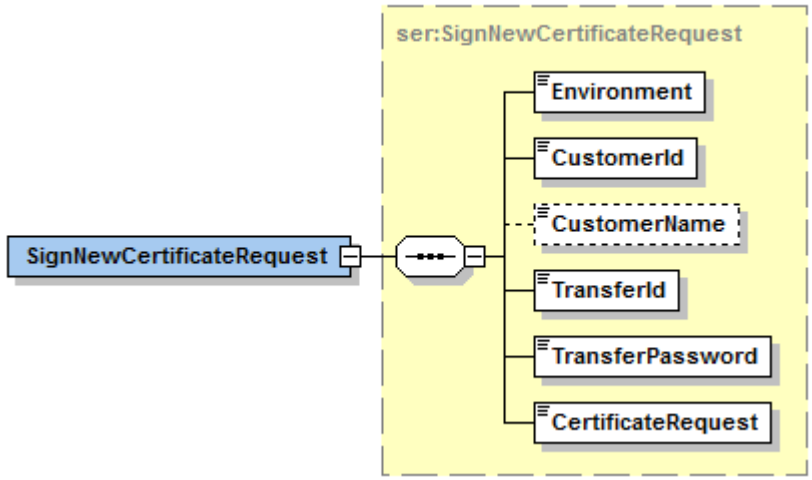
Varmennepalvelun Web Service -rajapinnan palveluissa käytetään sähköistä allekirjoitusta (XML Signature). Sillä todennetaan viestin tietosisällön muodostaja luvussa 3 määriteltävissä sanomissa. Allekirjoitus takaa myös viestin muuttumattomuuden. Allekirjoitus toteutetaan XML Enveloped Signature -mekanismilla, jonka käsittelysäännöt ja rakenne kuvataan dokumentissa XML Signature Syntax and Processing (http://www.w3.org/TR/xmldsig-core/). Allekirjoituksen muodostamisen menettelytavat ja siihen liittyvät tarkennukset (kuten käytettävät algoritmit ja kanonikalisointitavat) julkaistaan myöhemmin tulorekisterin XML-signature muodostuksen yhteydessä.

2.2 Virheiden käsittely Web Service -palveluissa

Palvelut palauttavat virhetilanteissa niihin liittyvät virheilmoitukset vastaussanoman mukana, tietosisällössä kuvatun rakenteen mukaisesti. Virheen tiedot -elementti sisältää virheen koodin ja virhekoodin selitteen. Mikäli 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. Virhekoodit ja virhekoodien selitteet on kuvattu luvussa 4.

3 RAJAPINNAN PALVELUIDEN TIETOSISÄLTÖ

3.1 Uuden varmenteen pyytäminen – pyyntösanoma (SignNewCertificateRequest)

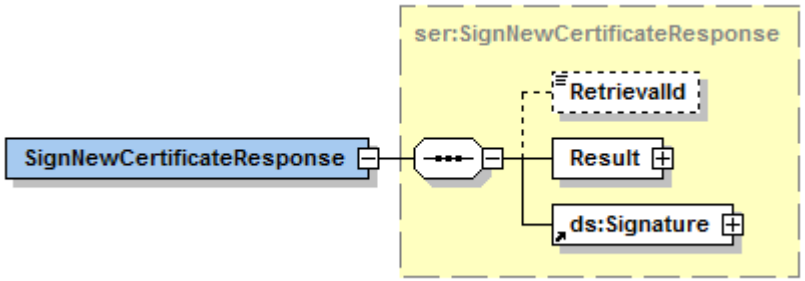


Tietoryhmän *SignNewCertificateRequest* tiedot:

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 tunniste (CustomerId)	ser:String30		1:1	Asiakkaan tunniste. Tunnisteena käytetään organisaation virallista, tulorekisterin kanssa asiointiin käytettyä tunnistetta. Tunniste voi olla esimerkiksi Y-tunnus. Jos käytetään Y-tunnusta, tunnisteen 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.
Siirtotunnus (TransferId)	ser:String32		1:1	Asiakkaalle varmenteen pyytämistä varten toimitettu tunnus.
Kertakäyttösalasana (TransferPassword)	ser:String16		1:1	Asiakkaalle varmenteen pyytämistä varten toimitettu kertakäyttöinen salasana.
Varmennepyyntö (CertificateRequest)	ser:CertificateRequestType		1:1	Asiakkaan tekemä varmennepyyntö. Varmennepyyntö on PKCS#10-muotoinen Base64-koodattu merkkijono.

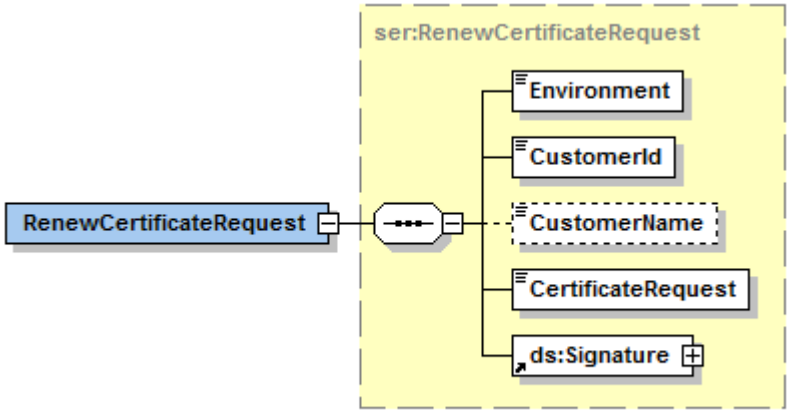
3.2 Uuden varmenteen pyytäminen – vastaussanoma (SignNewCertificateResponse)



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 varmennepalvelu muodostaa omalla varmenteellaan.

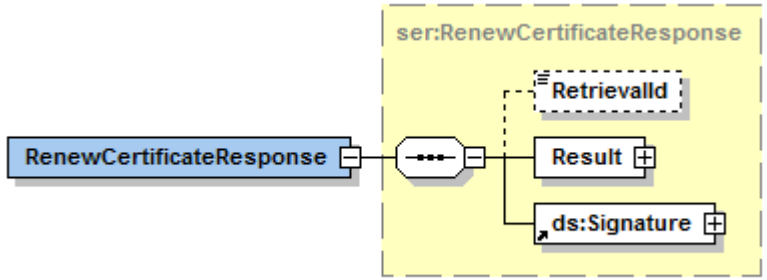
3.3 Voimassaolevan varmenteen uusiminen – pyyntösanoma (RenewCertificateRequest)



Tietoryhmän *RenewCertificateRequest* 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, tulorekisterin kanssa asiointiin käytettyä tunnistetta. Tunniste voi olla esimerkiksi Y-tunnus. Jos käytetään Y-tunnusta, tunnisteen 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:CertificateRequestType		1:1	Asiakkaan tekemä varmennepyyntö. Varmennepyyntö on PKCS#10-muotoinen Base64-koodattu merkkijono.
XML-allekirjoitus (Signature)	ds:Signature		1:1	XML-allekirjoitus, jonka asiakas muodostaa voimassaolevalla varmenteellaan.

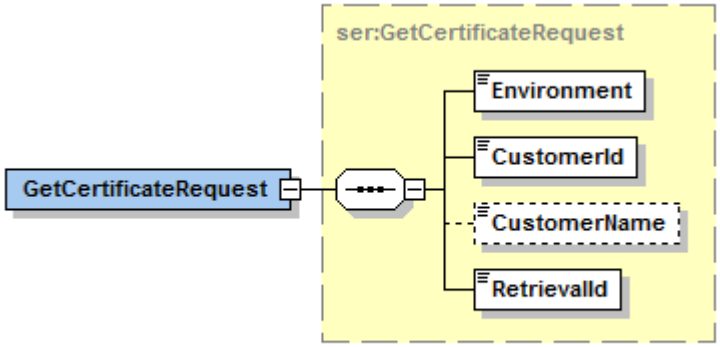
3.4 Voimassaolevan varmenteen uusiminen – vastaussanoma (RenewCertificateResponse)



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 varmennepalvelu muodostaa omalla varmenteellaan.

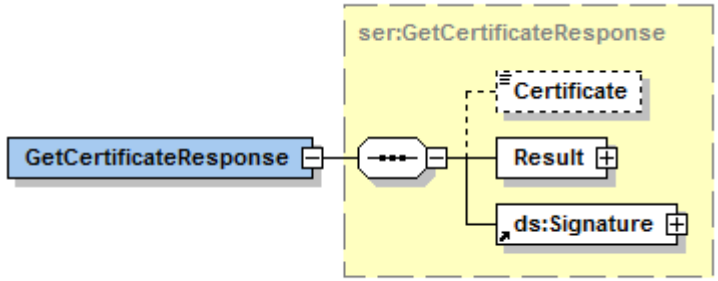
3.5 Varmenteen noutaminen – pyyntösanoma (GetCertificateRequest)



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, tulorekisterin kanssa asiointiin käytettyä tunnistetta. Tunniste voi olla esimerkiksi Y-tunnus. Jos käytetään Y-tunnusta, tunnisteen 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 varmennepalvelu palauttaa varmenteen pyyntösanomalle tai varmenteen uusimissanomalle.

3.6 Varmenteen noutaminen – vastaussanoma (GetCertificateResponse)

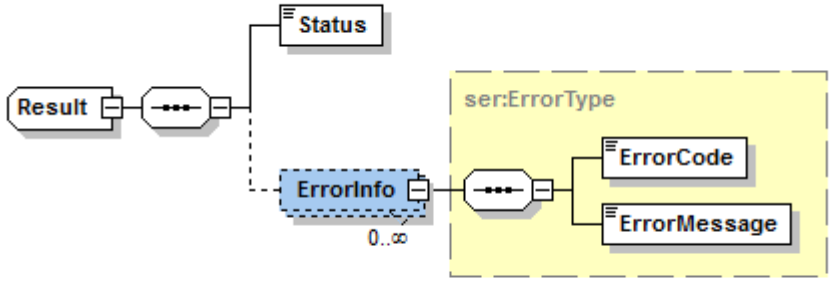


Tietoryhmän *GetCertificateResponse* tiedot:

Tiedon nimi	Tyyppi	Sallitut arvot	Elementin pakollisuus (minOccurs: maxOccurs)	Tiedon selite
Asiakkaan varmenne (Certificate)	ser:CertificateType		0:1	Varmennepalvelun 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 varmennepalvelu muodostaa omalla varmenteellaan.

3.7 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.
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 4.

4 VIRHEKOODIT JA VIRHEKOODIEN SELITTEET

Uuden varmenteen pyytäminen – vastaussanoman mahdollisesti palauttamat 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 tunnisteista, 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 varmennepyyntö (CSR) on virheellinen. Uuden varmennepyynnön luomisen jälkeen toimintoa voi yrittää uudelleen.
PKI099	Generic Technical Error	Virhetilanne, jolle ei ole erikseen määriteltyä virhekoodia. Virheellisen kutsun muoto ja tiedot tulee tarkistaa. Jos virhe toistuu usein, tulee ottaa yhteyttä tulorekisteriin.

Olemassaolevan varmenteen uusiminen – vastaussanoman mahdollisesti palauttamat 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 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	Varmennepyyntö (CSR) on virheellinen. Uuden varmennepyynnön luomisen jälkeen toimintoa voi yrittää uudelleen.
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 määriteltyä virhekoodia. Virheellisen kutsun muoto ja tiedot tulee tarkistaa. Jos virhe toistuu usein, tulee ottaa yhteyttä tulorekisteriin.

Varmenteen noutaminen – vastaussanoman mahdollisesti palauttamat 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 tunnisteista, asiakkaan tunniste (CustomerID), siirtotunnus (TransferId) tai kertakäyttösalasana (TransferPassword) on virheellinen uutta varmennetta pyydettäessä tai varmennetta uusiessa. Tunnistetietojen tarkistuksen jälkeen alkuperäinen varmennepyyntö tai voimassaolevan varmenteen uusiminen ja varmenteen haku pitää suorittaa uudelleen. Pelkkä varmenteen haun 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 varmennepalvelu ei ole vielä ehtinyt käsitellä pyyntösanomaa. Jos virhe toistuu usein, tulee ottaa yhteyttä tulorekisteriin. 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.