

Vero API varmenteen uusiminen varmennepalvelun web service-rajapintaa käyttäen

Oheinen ohje kuvaa yhden tavan suorittaa Verohallinnon myöntämän varmenteen uusiminen käyttäen Verohallinnon varmennepalvelun web service-rajapintaa. Esimerkin perusteella varmenteen uusimisen voi toteuttaa omaan ohjelmistoonsa.

Ohjeessa kuvattu testivarmenteen uusiminen on sovellettavissa myös tuotantovarmenteen uusimiseen, jolloin käytetään aitoja asiakastietoja sekä varmennepalvelun tuotanto-osoitetta (url).

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 8 tai uudempi: [.NET Downloads \(Linux, macOS, and Windows\) \(microsoft.com\)](https://dotnet.microsoft.com/en-us/download/linux-macos)
- 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](#)
- Vero API - asiakkaille on olemassa Slack-kanava: <https://vero-api.slack.com>
 - Liity kanavalle API-havaintolomakkeen kautta.

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 varmennepyyntö uusimista varten

Muodosta varmennepyyntö (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 varmennepyyntö 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, huom. poista rivinvaihdot templaattista 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 varmennepyyntö 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 varmennepyyntö (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 kohdassa 3. muodostettu. Voit käyttää valmiita ratkaisuja esim. XML Signer-ohjelmaa tai toteuttaa itse tai käyttää Verohallinnon esimerkkitoteutusta. Tämä ohje hyödyntää Verohallinnon c# toteutusta. Esimerkkitoteutus edellyttää nykyisen varmenteen pfx-tiedostossa.

Lataa esimerkkitoteutus täältä: https://www.vero.fi/globalassets/tietoa-verohallinnosta/ohjelmistokehittäjille/swaggerui/verohallinto_program.zip

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 `pxf`-tiedosto suojataan. Salasanaa tarvitaan allekirjoitusohjelmassa. Lopputuloksena muodostuu uusi `test.pxf`-tiedosto.

Jos kokeilet testipenkissä:

Muodosta `pxf`-tiedosto yllä olevalla komennolla, jolloin siihen viedään yksityinen avain, testipenkin `SignNewCertificate_Private.key`-tiedosto sekä testipenkistä noudettu nykyinen varmenne, mikä 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, `pxf`-tiedosto ja sille luomasi salasana:
`SignXmlNew.exe renew.xml test.pxf 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>MIICjTCCAXUCAQAwwSDELMAGGA1UEBhMCRkxkEzARBgNVBAgMCINvbWUuU3RhdGUx
JDAiBgNVBAoMGOFIFBLSSEBZXBG9wZXIqQ29tcGFueSBPeTCCASlwdQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBAJkBP88eLdbxbJfPluDI/rNP0EUpluRohxgX
MNfuYVv9kXgrMsOZpCsV/QjwZFPWBSFY6PDJIKyVAqe83XSfoGPT9apy3QaUJUxR
4/P5H6VT+eZpt1TCf5CEaKb0aW4bZ1kN9BLerrJ81HsR6cutpE/t0bzArc4kna/
rz/yB3tIU34YoHyx9bXNwKSPsUdL7N32vluSO8Me/3NjFzA9CBYRrP58qnXlyTmm
0x5GJXGBJqJm2xBRCmpMWg5WGUOF8mAGxkPDxyEfZpaHXbSLaBQ1nJyDPg0+n/Ak
rcweydE0BKmMh3rSITH/M5DYZ6yKgHABEWERg1Nz06ei+a+KJUcAawEAAaAAMA0G
CSqGSIb3DQEBcwUAA4IBAQBslqCulgyrfU+DVZxS60Hvu4d8GcKRGctFBt508BM
c+NSnevgaKwZXXMwKOJStsDHSOPnwfalvImFLWRKAsqxt2dIlgVWMzFh9NaX0Anwm
CbiUruot9C8zguP7Y/67AFSeageNYrHmgIbHoZyNle+tPR4Y5DxcQBI/6HtyzJ/q
Nej5mp2zSIW5P1QoEks3MU8Gm0mpCBylyAvCzeYHOop6caZMQctVCmPto+0PYx0T
qEmO15vGj/rIN4btjEKSYfjNj56MMN8lsic/6vqdikKKmMwTLRXjq73liOYyJ11s
9433VK1J/UMvay3y2YKVDUuW567HD8C3IsT+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/qx4yhvyysDvcKnoiNijUdj7Arr1A=</DigestValue></Reference></SignedInfo><SignatureValue>VEja4
6Y171aMXHMJfCZMRM+3zPTLSev/zWeR2JLMMcZ3nWidJynhs1MjGMBqJ3glsebmK3UX10ToZ0LObtbeACFYz78dDKbWHTc4cU
1IWkZU3DpXQ5svgJWNk1L+B2SDH7V+ethFNqBmwLcgsE2d78pt7rXwsBOnZe/Rt30fEMd5sSWYYJeb1FzMXAcaFVloVs31T9HcoCF
upgMH9YVsgzpknQHTSTKfjBZbhsjBnvnDlwSceFhxxNpcmy/zVjRVB56WeC2qhQgZFN7PsnCJ6KnNOTkYr2w7CVCFNwofCMU3eXUI
+n5khTJmNQV+S2ZS0qPzBSp6TD/reCVJHA==</SignatureValue><X509Data><X509Certificate>MIIFqzCCAaAwIwAgILG
ZoeTGyXo3IwDQYJKoZIhvcNAQELBQAwSjEKMCIgA1UEAwwbUETjIFNlcuZpY2UgRGV2ZWxvcGVyIENBIHYxMRUwEwYDVQQLKDA
xWZxJvaGFsbGludG8xGzAjbG9uYm90bWUwSDELMAGGA1UEBhMCRkxkEzARBgNVBAgMCINvbWUuU3RhdGUxJDAiBgNVBAoMGOFIFBLSSEBZXBG9wZXIqQ29tcGFueSBPeTCCASlwdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJkBP88eLdbxbJfPluDI/rNP0EUpluRohxgX
MNfuYVv9kXgrMsOZpCsV/QjwZFPWBSFY6PDJIKyVAqe83XSfoGPT9apy3QaUJUxR4/P5H6VT+eZpt1TCf5CEaKb0aW4bZ1kN9BLerrJ81HsR6cutpE/t0bzArc4kna/rz/yB3tIU34YoHyx9bXNwKSPsUdL7N32vluSO8Me/3NjFzA9CBYRrP58qnXlyTmm
0x5GJXGBJqJm2xBRCmpMWg5WGUOF8mAGxkPDxyEfZpaHXbSLaBQ1nJyDPg0+n/AkrcweydE0BKmMh3rSITH/M5DYZ6yKgHABEWERg1Nz06ei+a+KJUcAawEAAaAAMA0GCSqGSIb3DQEBcwUAA4IBAQBslqCulgyrfU+DVZxS60Hvu4d8GcKRGctFBt508BMc+NSnevgaKwZXXMwKOJStsDHSOPnwfalvImFLWRKAsqxt2dIlgVWMzFh9NaX0AnwmCbiUruot9C8zguP7Y/67AFSeageNYrHmgIbHoZyNle+tPR4Y5DxcQBI/6HtyzJ/qNej5mp2zSIW5P1QoEks3MU8Gm0mpCBylyAvCzeYHOop6caZMQctVCmPto+0PYx0TqEmO15vGj/rIN4btjEKSYfjNj56MMN8lsic/6vqdikKKmMwTLRXjq73liOYyJ11s
9433VK1J/UMvay3y2YKVDUuW567HD8C3IsT+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/qx4yhvyysDvcKnoiNijUdj7Arr1A=</DigestValue></Reference></SignedInfo><SignatureValue>VEja4
6Y171aMXHMJfCZMRM+3zPTLSev/zWeR2JLMMcZ3nWidJynhs1MjGMBqJ3glsebmK3UX10ToZ0LObtbeACFYz78dDKbWHTc4cU
1IWkZU3DpXQ5svgJWNk1L+B2SDH7V+ethFNqBmwLcgsE2d78pt7rXwsBOnZe/Rt30fEMd5sSWYYJeb1FzMXAcaFVloVs31T9HcoCF
upgMH9YVsgzpknQHTSTKfjBZbhsjBnvnDlwSceFhxxNpcmy/zVjRVB56WeC2qhQgZFN7PsnCJ6KnNOTkYr2w7CVCFNwofCMU3eXUI
+n5khTJmNQV+S2ZS0qPzBSp6TD/reCVJHA==</SignatureValue><X509Data><X509Certificate>MIIFqzCCAaAwIwAgILG
ZoeTGyXo3IwDQYJKoZIhvcNAQELBQAwSjEKMCIgA1UEAwwbUETjIFNlcuZpY2UgRGV2ZWxvcGVyIENBIHYxMRUwEwYDVQQLKDA
xWZxJvaGFsbGludG8xGzAjbG9uYm90bWUwSDELMAGGA1UEBhMCRkxkEzARBgNVBAgMCINvbWUuU3RhdGUxJDAiBgNVBAoMGOFIFBLSSEBZXBG9wZXIqQ29tcGFueSBPeTCCASlwdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJkBP88eLdbxbJfPluDI/rNP0EUpluRohxgX
MNfuYVv9kXgrMsOZpCsV/QjwZFPWBSFY6PDJIKyVAqe83XSfoGPT9apy3QaUJUxR4/P5H6VT+eZpt1TCf5CEaKb0aW4bZ1kN9BLerrJ81HsR6cutpE/t0bzArc4kna/rz/yB3tIU34YoHyx9bXNwKSPsUdL7N32vluSO8Me/3NjFzA9CBYRrP58qnXlyTmm
0x5GJXGBJqJm2xBRCmpMWg5WGUOF8mAGxkPDxyEfZpaHXbSLaBQ1nJyDPg0+n/AkrcweydE0BKmMh3rSITH/M5DYZ6yKgHABEWERg1Nz06ei+a+KJUcAawEAAaAAMA0GCSqGSIb3DQEBcwUAA4IBAQBslqCulgyrfU+DVZxS60Hvu4d8GcKRGctFBt508BMc+NSnevgaKwZXXMwKOJStsDHSOPnwfalvImFLWRKAsqxt2dIlgVWMzFh9NaX0AnwmCbiUruot9C8zguP7Y/67AFSeageNYrHmgIbHoZyNle+tPR4Y5DxcQBI/6HtyzJ/qNej5mp2zSIW5P1QoEks3MU8Gm0mpCBylyAvCzeYHOop6caZMQctVCmPto+0PYx0TqEmO15vGj/rIN4btjEKSYfjNj56MMN8lsic/6vqdikKKmMwTLRXjq73liOYyJ11s
9433VK1J/UMvay3y2YKVDUuW567HD8C3IsT+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/qx4yhvyysDvcKnoiNijUdj7Arr1A=</DigestValue></Reference></SignedInfo><SignatureValue>VEja4
6Y171aMXHMJfCZMRM+3zPTLSev/zWeR2JLMMcZ3nWidJynhs1MjGMBqJ3glsebmK3UX10ToZ0LObtbeACFYz78dDKbWHTc4cU
1IWkZU3DpXQ5svgJWNk1L+B2SDH7V+ethFNqBmwLcgsE2d78pt7rXwsBOnZe/Rt30fEMd5sSWYYJeb1FzMXAcaFVloVs31T9HcoCF
upgMH9YVsgzpknQHTSTKfjBZbhsjBnvnDlwSceFhxxNpcmy/zVjRVB56WeC2qhQgZFN7PsnCJ6KnNOTkYr2w7CVCFNwofCMU3eXUI
+n5khTJmNQV+S2ZS0qPzBSp6TD/reCVJHA==</SignatureValue><X509Data><X509Certificate>MIIFqzCCAaAwIwAgILG
ZoeTGyXo3IwDQYJKoZIhvcNAQELBQAwSjEKMCIgA1UEAwwbUETjIFNlcuZpY2UgRGV2ZWxvcGVyIENBIHYxMRUwEwYDVQQLKDA
xWZxJvaGFsbGludG8xGzAjbG9uYm90bWUwSDELMAGGA1UEBhMCRkxkEzARBgNVBAgMCINvbWUuU3RhdGUxJDAiBgNVBAoMGOFIFBLSSEBZXBG9wZXIqQ29tcGFueSBPeTCCASlwdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJkBP88eLdbxbJfPluDI/rNP0EUpluRohxgX
MNfuYVv9kXgrMsOZpCsV/QjwZFPWBSFY6PDJIKyVAqe83XSfoGPT9apy3QaUJUxR4/P5H6VT+eZpt1TCf5CEaKb0aW4bZ1kN9BLerrJ81HsR6cutpE/t0bzArc4kna/rz/yB3tIU34YoHyx9bXNwKSPsUdL7N32vluSO8Me/3NjFzA9CBYRrP58qnXlyTmm
0x5GJXGBJqJm2xBRCmpMWg5WGUOF8mAGxkPDxyEfZpaHXbSLaBQ1nJyDPg0+n/AkrcweydE0BKmMh3rSITH/M5DYZ6yKgHABEWERg1Nz06ei+a+KJUcAawEAAaAAMA0GCSqGSIb3DQEBcwUAA4IBAQBslqCulgyrfU+DVZxS60Hvu4d8GcKRGctFBt508BMc+NSnevgaKwZXXMwKOJStsDHSOPnwfalvImFLWRKAsqxt2dIlgVWMzFh9NaX0AnwmCbiUruot9C8zguP7Y/67AFSeageNYrHmgIbHoZyNle+tPR4Y5DxcQBI/6HtyzJ/qNej5mp2zSIW5P1QoEks3MU8Gm0mpCBylyAvCzeYHOop6caZMQctVCmPto+0PYx0TqEmO15vGj/rIN4btjEKSYfjNj56MMN8lsic/6vqdikKKmMwTLRXjq73liOYyJ11s
9433VK1J/UMvay3y2YKVDUuW567HD8C3IsT+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/qx4yhvyysDvcKnoiNijUdj7Arr1A=</DigestValue></Reference></SignedInfo><SignatureValue>VEja4
6Y171aMXHMJfCZMRM+3zPTLSev/zWeR2JLMMcZ3nWidJynhs1MjGMBqJ3glsebmK3UX10ToZ0LObtbeACFYz78dDKbWHTc4cU
1IWkZU3DpXQ5svgJWNk1L+B2SDH7V+ethFNqBmwLcgsE2d78pt7rXwsBOnZe/Rt30fEMd5sSWYYJeb1FzMXAcaFVloVs31T9HcoCF
upgMH9YVsgzpknQHTSTKfjBZbhsjBnvnDlwSceFhxxNpcmy/zVjRVB56WeC2qhQgZFN7PsnCJ6KnNOTkYr2w7CVCFNwofCMU3eXUI
+n5khTJmNQV+S2ZS0qPzBSp6TD/reCVJHA==</SignatureValue><X509Data><X509Certificate>MIIFqzCCAaAwIwAgILG
ZoeTGyXo3IwDQYJKoZIhvcNAQELBQAwSjEKMCIgA1UEAwwbUETjIFNlcuZpY2UgRGV2ZWxvcGVyIENBIHYxMRUwEwYDVQQLKDA
xWZxJvaGFsbGludG8xGzAjbG9uYm90bWUwSDELMAGGA1UEBhMCRkxkEzARBgNVBAgMCINvbWUuU3RhdGUxJDAiBgNVBAoMGOFIFBLSSEBZXBG9wZXIqQ29tcGFueSBPeTCCASlwdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJkBP88eLdbxbJfPluDI/rNP0EUpluRohxgX
MNfuYVv9kXgrMsOZpCsV/QjwZFPWBSFY6PDJIKyVAqe83XSfoGPT9apy3QaUJUxR4/P5H6VT+eZpt1TCf5CEaKb0aW4bZ1kN9BLerrJ81HsR6cutpE/t0bzArc4kna/rz/yB3tIU34YoHyx9bXNwKSPsUdL7N32vluSO8Me/3NjFzA9CBYRrP58qnXlyTmm
0x5GJXGBJqJm2xBRCmpMWg5WGUOF8mAGxkPDxyEfZpaHXbSLaBQ1nJyDPg0+n/AkrcweydE0BKmMh3rSITH/M5DYZ6yKgHABEWERg1Nz06ei+a+KJUcAawEAAaAAMA0GCSqGSIb3DQEBcwUAA4IBAQBslqCulgyrfU+DVZxS60Hvu4d8GcKRGctFBt508BMc+NSnevgaKwZXXMwKOJStsDHSOPnwfalvImFLWRKAsqxt2dIlgVWMzFh9NaX0AnwmCbiUruot9C8zguP7Y/67AFSeageNYrHmgIbHoZyNle+tPR4Y5DxcQBI/6HtyzJ/qNej5mp2zSIW5P1QoEks3MU8Gm0mpCBylyAvCzeYHOop6caZMQctVCmPto+0PYx0TqEmO15vGj/rIN4btjEKSYfjNj56MMN8lsic/6vqdikKKmMwTLRXjq73liOYyJ11s
9433VK1J/UMvay3y2YKVDUuW567HD8C3IsT+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/qx4yhvyysDvcKnoiNijUdj7Arr1A=</DigestValue></Reference></SignedInfo><SignatureValue>VEja4
6Y171aMXHMJfCZMRM+3zPTLSev/zWeR2JLMMcZ3nWidJynhs1MjGMBqJ3glsebmK3UX10ToZ0LObtbeACFYz78dDKbWHTc4cU
1IWkZU3DpXQ5svgJWNk1L+B2SDH7V+ethFNqBmwLcgsE2d78pt7rXwsBOnZe/Rt30fEMd5sSWYYJeb1FzMXAcaFVloVs31T9HcoCF
upgMH9YVsgzpknQHTSTKfjBZbhsjBnvnDlwSceFhxxNpcmy/zVjRVB56WeC2qhQgZFN7PsnCJ6KnNOTkYr2w7CVCFNwofCMU3eXUI
+n5khTJmNQV+S2ZS0qPzBSp6TD/reCVJHA==</SignatureValue><X509Data><X509Certificate>MIIFqzCCAaAwIwAgILG
ZoeTGyXo3IwDQYJKoZIhvcNAQELBQAwSjEKMCIgA1UEAwwbUETjIFNlcuZpY2UgRGV2ZWxvcGVyIENBIHYxMRUwEwYDVQQLKDA
xWZxJvaGFsbGludG8xGzAjbG9uYm90bWUwSDELMAGGA1UEBhMCRkxkEzARBgNVBAgMCINvbWUuU3RhdGUxJDAiBgNVBAoMGOFIFBLSSEBZXBG9wZXIqQ29tcGFueSBPeTCCASlwdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJkBP88eLdbxbJfPluDI/rNP0EUpluRohxgX
MNfuYVv9kXgrMsOZpCsV/QjwZFPWBSFY6PDJIKyVAqe83XSfoGPT9apy3QaUJUxR4/P5H6VT+eZpt1TCf5CEaKb0aW4bZ1kN9BLerrJ81HsR6cutpE/t0bzArc4kna/rz/yB3tIU34YoHyx9bXNwKSPsUdL7N32vluSO8Me/3NjFzA9CBYRrP58qnXlyTmm
0x5GJXGBJqJm2xBRCmpMWg5WGUOF8mAGxkPDxyEfZpaHXbSLaBQ1nJyDPg0+n/AkrcweydE0BKmMh3rSITH/M5DYZ6yKgHABEWERg1Nz06ei+a+KJUcAawEAAaAAMA0GCSqGSIb3DQEBcwUAA4IBAQBslqCulgyrfU+DVZxS60Hvu4d8GcKRGctFBt508BMc+NSnevgaKwZXXMwKOJStsDHSOPnwfalvImFLWRKAsqxt2dIlgVWMzFh9NaX0AnwmCbiUruot9C8zguP7Y/67AFSeageNYrHmgIbHoZyNle+tPR4Y5DxcQBI/6HtyzJ/qNej5mp2zSIW5P1QoEks3MU8Gm0mpCBylyAvCzeYHOop6caZMQctVCmPto+0PYx0TqEmO15vGj/rIN4btjEKSYfjNj56MMN8lsic/6vqdikKKmMwTLRXjq73liOYyJ11s
9433VK1J/UMvay3y2YKVDUuW567HD8C3IsT+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/qx4yhvyysDvcKnoiNijUdj7Arr1A=</DigestValue></Reference></SignedInfo><SignatureValue>VEja4
6Y171aMXHMJfCZMRM+3zPTLSev/zWeR2JLMMcZ3nWidJynhs1MjGMBqJ3glsebmK3UX10ToZ0LObtbeACFYz78dDKbWHTc4cU
1IWkZU3DpXQ5svgJWNk1L+B2SDH7V+ethFNqBmwLcgsE2d78pt7rXwsBOnZe/Rt30fEMd5sSWYYJeb1FzMXAcaFVloVs31T9HcoCF
upgMH9YVsgzpknQHTSTKfjBZbhsjBnvnDlwSceFhxxNpcmy/zVjRVB56WeC2qhQgZFN7PsnCJ6KnNOTkYr2w7CVCFNwofCMU3eXUI
+n5khTJmNQV+S2ZS0qPzBSp6TD/reCVJHA==</SignatureValue><X509Data><X509Certificate>MIIFqzCCAaAwIwAgILG
ZoeTGyXo3IwDQYJKoZIhvcNAQELBQAwSjEKMCIgA1UEAwwbUETjIFNlcuZpY2UgRGV2ZWxvcGVyIENBIHYxMRUwEwYDVQQLKDA
xWZxJvaGFsbGludG8xGzAjbG9uYm90bWUwSDELMAGGA1UEBhMCRkxkEzARBgNVBAgMCINvbWUuU3RhdGUxJDAiBgNVBAoMGOFIFBLSSEBZXBG9wZXIqQ29tcGFueSBPeTCCASlwdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJkBP88eLdbxbJfPluDI/rNP0EUpluRohxgX
MNfuYVv9kXgrMsOZpCsV/QjwZFPWBSFY6PDJIKyVAqe83XSfoGPT9apy3QaUJUxR4/P5H6VT+eZpt1TCf5CEaKb0aW4bZ1kN9BLerrJ81HsR6cutpE/t0bzArc4kna/rz/yB3tIU34YoHyx9bXNwKSPsUdL7N32vluSO8Me/3NjFzA9CBYRrP58qnXlyTmm
0x5GJXGBJqJm2xBRCmpMWg5WGUOF8mAGxkPDxyEfZpaHXbSLaBQ1nJyDPg0+n/AkrcweydE0BKmMh3rSITH/M5DYZ6yKgHABEWERg1Nz06ei+a+KJUcAawEAAaAAMA0GCSqGSIb3DQEBcwUAA4IBAQBslqCulgyrfU+DVZxS60Hvu4d8GcKRGctFBt508BMc+NSnevgaKwZXXMwKOJStsDHSOPnwfalvImFLWRKAsqxt2dIlgVWMzFh9NaX0AnwmCbiUruot9C8zguP7Y/67AFSeageNYrHmgIbHoZyNle+tPR4Y5DxcQBI/6HtyzJ/qNej5mp2zSIW5P1QoEks3MU8Gm0mpCBylyAvCzeYHOop6caZMQctVCmPto+0PYx0TqEmO15vGj/rIN4btjEKSYfjNj56MMN8lsic/6vqdikKKmMwTLRXjq73liOYyJ11s
9433VK1J/UMvay3y2YKVDUuW567HD8C3IsT+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/qx4yhvyysDvcKnoiNijUdj7Arr1A=</DigestValue></Reference></SignedInfo><SignatureValue>VEja4
6Y171aMXHMJfCZMRM+3zPTLSev/zWeR2JLMMcZ3nWidJynhs1MjGMBqJ3glsebmK3UX10ToZ0LObtbeACFYz78dDKbWHTc4cU
1IWkZU3DpXQ5svgJWNk1L+B2SDH7V+ethFNqBmwLcgsE2d78pt7rXwsBOnZe/Rt30fEMd5sSWYYJeb1FzMXAcaFVloVs31T9HcoCF
upgMH9YVsgzpknQHTSTKfjBZbhsjBnvnDlwSceFhxxNpcmy/zVjRVB56WeC2qhQgZFN7PsnCJ6KnNOTkYr2w7CVCFNwofCMU3eXUI
+n5khTJmNQV+S2ZS0qPzBSp6TD/reCVJHA==</SignatureValue><X509Data><X509Certificate>MIIFqzCCAaAwIwAgILG
ZoeTGyXo3IwDQYJKoZIhvcNAQELBQAwSjEKMCIgA1UEAwwbUETjIFNlcuZpY2UgRGV2ZWxvcGVyIENBIHYxMRUwEwYDVQQLKDA
xWZxJvaGFsbGludG8xGzAjbG9uYm90bWUwSDELMAGGA1UEBhMCRkxkEzARBgNVBAgMCINvbWUuU3RhdGUxJDAiBgNVBAoMGOFIFBLSSEBZXBG9wZXIqQ29tcGFueSBPeTCCASlwdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJkBP88eLdbxbJfPluDI/rNP0EUpluRohxgX
MNfuYVv9kXgrMsOZpCsV/QjwZFPWBSFY6PDJIKyVAqe83XSfoGPT9apy3QaUJUxR4/P5H6VT+eZpt1TCf5CEaKb0aW4bZ1kN9BLerrJ81HsR6cutpE/t0bzArc4kna/rz/yB3tIU34YoHyx9bXNwKSPsUdL7N32vluSO8Me/3NjFzA9CBYRrP58qnXlyTmm
0x5GJXGBJqJm2xBRCmpMWg5WGUOF8mAGxkPDxyEfZpaHXbSLaBQ1nJyDPg0+n/AkrcweydE0BKmMh3rSITH/M5DYZ6yKgHABEWERg1Nz06ei+a+KJUcAawEAAaAAMA0GCSqGSIb3DQEBcwUAA4IBAQBslqCulgyrfU+DVZxS60Hvu4d8GcKRGctFBt508BMc+NSnevgaKwZXXMwKOJStsDHSOPnwfalvImFLWRKAsqxt2dIlgVWMzFh9NaX0AnwmCbiUruot9C8zguP7Y/67AFSeageNYrHmgIbHoZyNle+tPR4Y5DxcQBI/6HtyzJ/qNej5mp2zSIW5P1QoEks3MU8Gm0mpCBylyAvCzeYHOop6caZMQctVCmPto+0PYx0TqEmO15vGj/rIN4btjEKSYfjNj56MMN8lsic/6vqdikKKmMwTLRXjq73liOYyJ11s
9433VK1J/UMvay3y2YKVDUuW567HD8C3IsT+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/qx4yhvyysDvcKnoiNijUdj7Arr1A=</DigestValue></Reference></SignedInfo><SignatureValue>VEja4
6Y171aMXHMJfCZMRM+3zPTLSev/zWeR2JLMMcZ3nWidJynhs1MjGMBqJ3glsebmK3UX10ToZ0LObtbeACFYz78dDKbWHTc4cU
1IWkZU3DpXQ5svgJWNk1L+B2SDH7V+ethFNqBmwLcgsE2d78pt7rXwsBOnZe/Rt30fEMd5sSWYYJeb1FzMXAcaFVloVs31T9HcoCF
upgMH9YVsgzpknQHTSTKfjBZbhsjBnvnDlwSceFhxxNpcmy/zVjRVB56WeC2qhQgZFN7PsnCJ6KnNOTkYr2w7CVCFNwofCMU3eXUI
+n5khTJmNQV+S2ZS0qPzBSp6TD/reCVJHA==</SignatureValue><X509Data><X509Certificate>MIIFqzCCAaAwIwAgILG
ZoeTGyXo3IwDQYJKoZIhvcNAQELBQAwSjEKMCIgA1UEAwwbUETjIFNlcuZpY2UgRGV2ZWxvcGVyIENBIHYxMRUwEwYDVQQLKDA
xWZxJvaGFsbGludG8xGzAjbG9uYm90bWUwSDELMAGGA1UEBhMCRkxkEzARBgNVBAgMCINvbWUuU3RhdGUxJDAiBgNVBAoMGOFIFBLSSEBZXBG9wZXIqQ29tcGFueSBPeTCCASlwdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJkBP88eLdbxbJfPluDI/rNP0EUpluRohxgX
MNfuYVv9kXgrMsOZpCsV/QjwZFPWBSFY6PDJIKyVAqe83XSfoGPT9apy3QaUJUxR4/P5H6VT+eZpt1TCf5CEaKb0aW4bZ1kN9BLerrJ81HsR6cutpE/t0bzArc4kna/rz/yB3tIU34YoHyx9bXNwKSPsUdL7N32vluSO8Me/3NjFzA9CBYRrP58qnXlyTmm
0x5GJXGBJqJm2xBRCmpMWg5WGUOF8mAGxkPDxyEfZpaHXbSLaBQ1nJyDPg0+n/AkrcweydE0BKmMh3rSITH/M5DYZ6yKgHABEWERg1Nz06ei+a+KJUcAawEAAaAAMA0GCSqGSIb3DQEBcwUAA4IBAQBslqCulgyrfU+DVZxS60Hvu4d8GcKRGctFBt508BMc+NSnevgaKwZXXMwKOJStsDHSOPnwfalvImFLWRKAsqxt2dIlgVWMzFh9NaX0AnwmCbiUruot9C8zguP7Y/67AFSeageNYrHmgIbHoZyNle+tPR4Y5DxcQBI/6HtyzJ/qNej5mp2zSIW5P1QoEks3MU8Gm0mpCBylyAvCzeYHOop6caZMQctVCmPto+0PYx0TqEmO15vGj/rIN4btjEKSYfjNj56MMN8lsic/6vqdikKKmMwTLRXjq73liOYyJ11s
9433VK1J/UMvay3y2YKVDUuW567HD8C3IsT+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/qx4yhvyysDvcKnoiNijUdj7Arr1A=</DigestValue></Reference></SignedInfo><SignatureValue>VEja4
6Y171aMXHMJfCZMRM+3zPTLSev/zWeR2JLMMcZ3nWidJynhs1MjGMBqJ3glsebmK3UX10ToZ0LObtbeACFYz78dDKbWHTc4cU
1IWkZU3DpXQ5svgJWNk1L+B2SDH7V+ethFNqBmwLcgsE2d78pt7rXwsBOnZe/Rt30fEMd5sSWYYJeb1FzMXAcaFVloVs31T9HcoCF
upgMH9YVsgzpknQHTSTKfjBZbhsjBnvnDlwSceFhxxNpcmy/zVjRVB56WeC2qhQgZFN7PsnCJ6KnNOTkYr2w7CVCFNwofCMU3eXUI
+n5khTJmNQV+S2ZS0qPzBSp6TD/reCVJHA==</SignatureValue><X509Data><X509Certificate>MIIFqzCCAaAwIwAgILG
ZoeTGyXo3IwDQYJKoZIhvcNAQELBQAwSjEKMCIgA1UEAwwbUETjIFNlcuZpY2UgRGV2ZWxvcGVyIENBIHYxMRUwEwYDVQQLKDA
xWZxJvaGFsbGludG8xGzAjbG9uYm90bWUwSDELMAGGA1UEBhMCRkxkEzARBgNVBAgMCINvbWUuU3RhdGUxJDAiBgNVBAoMGOFIFBLSSEBZXBG9wZXIqQ29tcGFueSBPeTCCASlwdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJkBP88eLdbxbJfPluDI/rNP0EUpluRohxgX
MNfuYVv9kXgr
```

mzqSrSB0BKX5Sn9+jOF39fxE6LNCmJBizZ49WhSOTSLjX/kL8B0T4NBCtz6EdhQk0lz1JC5GvNuVVnmKeZYEl3qLv4ktc6QxIH2zZ48BR+m/cXycvyLzy2fgyAIW</X509Certificate></X509Data></KeyInfo></Signature></cer:RenewCertificateRequest>

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

Tärkeää on, että tiedoston sisältöä ei saa muuttaa millään tavalla ennen sen lähetystä varmennepalvelun 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 rajapintaan

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

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

SoapUI:hin voit ladata WSDL-kuvauksen perusteella avulla sanomarakenteiden pohjat. Lataa varmennepalvelun rajapintapaketti (https://vero.fi/globalassets/tulorekisteri/kuvat/varmennepalvelu-rajapinta_v1.01.zip) ja avaa WSDL-tiedosto SoapUI:lla.

Muodosta lähtevä sanoma siten, että allekirjoitettu sisältö on muuttumattomana soap-evenlophen 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 retrievealID, 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 Verohallinnon varmennepalvelun ohjeistusta.

Säilö pfx-tiedosto ja yksityinen avain huolellisesti.