

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/tulorekisteri/kuvat/varmennepalvelu-rajapinta_v1.01.zip
- Uusi avainpari varmennepyyntöä varten (CSR)
- Nykyinen varmenne ja siihen liittyvä yksityinen avain xml-sanoman allekirjoittamista varten.
- Käytössäsi oleva tiedon tuottajan Web Service varmenteen keinotekoinen y-tunnus ja testiyrityksen nimi.
- Mahdollinen pfx-tiedosto, jossa yksityinen avain nykyinen varmenne. Nykyisen pfx-tiedoston salasana.

Tarvittavat työvälineet

- OpenSSL: <https://wiki.openssl.org/index.php/Binaries>
- .NET Core 3.1: <https://dotnet.microsoft.com/download/dotnet/3.1>
- Visual Studio Code: <https://code.visualstudio.com/>
- Lataa Verohallinnon allekirjoitusohjelman esimerkkitoteutus täältä (SignXmlNew.exe):
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:

- Tulorekisterin varmenteen uusimisen ohjeet: <https://www.vero.fi/tulorekisteri/yritykset-ja-organisaatiot/suorituksen-maksajat/varmenne/varmenteen-uusiminen/>
- Varmennepalvelun dokumentaatio Tulorekisterin sivuilla:
<https://vero.fi/tulorekisteri/ohjelmistokehittajille/C3%A4j%C3%A4t/varmennepalvelu/dokumentatio/>
- Varmennepalvelun testipenkin ohje Tulorekisterin sivuilla:
<https://vero.fi/globalassets/tulorekisteri/dokumentatio-2021/varmennepalvelu---ohjelmistokehittajille/C3%A4j%C3%A4n-testipenkki.pdf>
- Vero API 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 esimerkkisanoman 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.

```
<?xml:namespace prefix="http://www.w3.org/2000/09/xmldsig#" />
<Environment>TEST</Environment>
<CustomerId>0123456-7</CustomerId>
<CustomerName>Ab PKI Developer Company Oy</CustomerName>
<CertificateRequest>MIICjTCCAXUCAQAwSDELMAG1UEBhMCRkxkEzARBgNVBAGMCINvbWUuU3RhdGUx
JDAiBgNVBAAoMG0FIFBLSSBEZXLbG9wZXlGQ29tcGFueSBPeTCCASlwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBAJkBP88eLdbxbJfPluDI/rNP0EUpluRohxgx
MnFuYVv9kXgrMgQpCsV/CjwZFpWBSFY6PDJlKyvAqe83XSfoGpt9apy3QaUJuXR
4/P5H6VT+eZpt1TCf5CEaKb0aW4bZ1kN9BLerrJ81HsR6cutPe/t0bzArc4kna/l
rz/yB3tlU34YyHox9bXNwKSPsUdL7N32vluSO8Me/3NjFzA9CBYRrP58qnXlyTmm
0x5GJXGBJqJM2xBRCmpMWg5WGUOF8mAGxkPDxyEfzpaHXbSLaBQ1nJyDPg0+n/Ak
rcweyDE0BKmMh3rSITH/M5DY26yKgHABEWERg1Nz06ei+a+KJUcCAwEAAaAAMA0G
CSqGSIb3DQEBQwUAA4IBAQBslqCulgyrU+DVZxS60Hvu4d8GcCKRGCTfBt508BM
c+nSnevgaKWXMMWKOJStsDHsOPnwfalvmlFLWRKAsqxt2dlGgWMzFh9NaX0Anwm
CbiUruot9C8zguP7Y/67AFSeageNYrHmgIBhoZyNle+tpR4Y5DxcQB1/6HtyzJ/q
Nej5mp2ZSiW5P1QoEks3MU8Gm0mpCBylyAvCzeYHOop6caZMQqctVCmPto+OPYx0T
qEmO15wGj/rN4btjEKSyYfjN56MMN8lscl6vqdkKkMmWTLRXjq73liOYyJ11s
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/qx4yhvyysDvcKnoiNijUdj7Arr1A=</DigestValue></Reference></SignedInfo><SignatureValue>VEja4
6Y171aMXHMJfcZMRM+3zPTLSeplzWvR2JLMMcZ3nWldJynhs1MjGMbqJ3glsebmK3UX10ToZ0LobtbEACFYz78dDKbWHTc4cU
1lwKZu3DpXq5svsgJWNtK1j+B2SDH7V+ethFNqBmwLcgsE2dT8pt7rXswBOnZe/Rt30fIEmd5sSWYYJeb1FzMXAcFvIoVs31T9HcoCF
upwMH9Y7WsgzpkqJHTSKfljBzhnsJbnvDlWScEfhxNpcmyZ/yJVRjBw6WCE2qKgZFEN7PsnCJ6KknN0TKYr2w7CVCFNwofCM3eXU1
+n5khTJmNQV+SZ2S0qPzBSp6TD/reCVJHA==</SignatureValue><KeyInfo><X509Data><X509Certificate>MIIFqzCCA5OgAwIwAgIlG
ZoeTGyXo3lwDQYJKoZlhcNAQELBQAwSjEKMCIgA1UEAwWbUETJfNlcnZpY2UgRGV2ZWxvcGVyIENBIHYxMRUwEwYDVQQKDA
xWZXJvaGFsbGdG8xCzAJBgNVBAYTAkZJMB4XDTEwMDcwNjA4MzYzMi0XDTMwMDcwNDA4MzYzMi0wZjESMBAG1UEAwWJM
dEYmZmQ1Ni03MzkwJyYDVQFEYBDNDY4MTkxMDdCNDAxNU0MUlZMTA0MTEeXmUEOREE2RDEKMCIA1UECgwbGwUgUETJIERl
dMvSb3B3b3BkBD21wYyY5S5IE9MSQwSCQYDVQGEWJSTGCCASlwDQYJKoZlhcNAQEBBQADggEPADCCAQoCggEBAMrf+UUX2nu
YBOeG3PxqzleMmMVRwqlmBTH/jdW0AmRZ34cuh+Do/T6U0mqg9G4IVsj8WaM8fmh7tdCQ3xcCPnqpQrkeGuWQV4nlhok74kDnQb1
2FrOKCsLIOMONHS2+9E8HKwS8gFfXzKP8UUnJK8PmptJQo+E6jIEy+vsZsHouf0UMCgpp9MutN9RlAtjqS6lyHtpq8BLn2hdEM1srlqCX
BRigkAH5w1mqbBSiVkgScaYJ+I5AY201ZTUlb138SY/bYk9gflS1aY1eGF+667Bms0aJk4JRLHujMqfEuHrfRwO1ps739H+8UPqkRm
JfNyGfWpUJewcGlikXhYGPUCAwEAAEAQAwSggwFnmAwGA1UdEwEB/wQMAAwHwDVROjBgBgwFAUT1PJe8BCr9h+uQE8W6
CNC7/QfeYwUwYIKwYBBQUHAQEERzBFMEMGCCsGAQUFBzAChjdodHRwOi8vY3JsLXRlc3RlLnZlcm8uZmkvY2EvUETJU2VydmljZ
URldmVsb3B3b3BkNDdjEuY3J0MBMGA1UdJQQMMAoGCCsGAQUFBwMCMIGcBgNVHR8EgZQwgZQwgZQwgY6gPKA6hjhdHRwOi8vY3JsL
XRlc3RlLnZlcm8uZmkvY3JsL1BLSVNlcnZpY2VEZXZlbg9wZXJlQXQyYXlmNyBkKjOpEwwSjEKMCIgA1UEAwWbUETJfNlcnZpY2UgRG
V2ZWxvcGVyIENBIHYxMRUwEwYDVQQKDAxWZXJvaGFsbGdG8xCzAJBgNVBAYTAkZJMB0GA1UdDgQWBQBQwQXl5AZJVyZf4
DEemCjLnw+mtAOBNAVH08BAf8EBMCAAwDQYJKoZlhcNAQELBQADggEABADzKk4t+rVIAe9a53/9zrWLUJae+WePxl0Ek5ozX
```

WDb2FeR0uEyUS2Ba0gVJwPm9Go6CAia3J9nFGyVUUNCm2ofdDGxEX4JkrRc7cO8JPaMY74tJR9wwj8R5sshAXPDVMWh9MI8LHG6hqz0ic0IK9cSsAHBGJ3GBIckS/6y+SPWGMHOf0QIm5of63qQ8a1950y4aUjL7td2Yxiu6jKUFp4haL0BvJFM///o6Ge5LxT3nfPZxESBLbLE21D0ksyO+fZljleflxleQk9rWY7Zyq/Go9+ElvEILXE2aDjqQrwoNIQHmqLgG0DuKpJKzSi7nRvDVHaB5YldtLDJ4PXZITkib8QBOZWmHCw58lvfEdL0WfuRpzJmCf8oyzLWRagtnEQhwnWnkXOtPqivRq3Rh35M4mQPNVPikduzYlhvQzwCAVkgzspEZVT5hQITEXBiZZQ8jC8Mb6U1u7G/NndHGwdWn0WtNYDMrhqEZGoHxgLTlwaU4d5suHzkv0glxkreR4fnVdiVWd4zCNQk6rt9Jo3p0yLFGM49G3ksZHPcYxxBmzqSrSBoBKX5Sn9+jOF39fxE6LNCmJBizZ49WhSOTSLjX/kL8B0T4NBCTz6EdhQk0lz1JC5GvNuVVnmKeZYElit3qLv4kct6QxIH2zZ48BR+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 Tulorekisterin varmennepalvelun ohjeistusta.

7. Lähetä uusittu varmenne Verohallintoon

Vero API käyttöön tarkoitettu testivarmenne (julkinen allekirjoitettu avain) tulee lähettää osoitteeseen ohjelmistotalot (at) vero.fi base64 muodossa, jolloin varmenne asennetaan Verohallinnon testiympäristöön. Tuotantovarmennetta ei tarvitse lähettää, ne latautuvat automaattisesti kerran vuorokaudessa. Älä lähetä pfx-tiedostoa taikka yksityistä avainta.