Version 1.0

Skatteförvaltningens certifikattjänst – beskrivning av PKI-systemet och gränssnitten

---

Skatteförvaltningen

Versionshistoria

Version	Datum	Beskrivning
1.0	19.9.2024	Vi har publicerat ett nytt dokument, i vilket avsnitten i Skatteförvaltningens certifikattjänst samt användningen av tjänsten och datainnehållet beskrivs. Dokumentet innehåller dessutom en beskrivning av testbädden och exempel som stöder användningen.

INNEHÅLL

1 ALLMÄNT OM SKATTEFÖRVALTNINGENS CERTIFIKATTJÄNST

1.1 Certifikattjänstens avsnitt och användning av tjänsten

Skatteförvaltningens certifikattjänst baserar sig på PKI-systemet och e-tjänsten, som utgör kundens webbläsarbaserade användargränssnitt. Certifikaten i Skatteförvaltningens certifikattjänst används av organisationer som lämnar eller hämtar material via tekniska gränssnitt eller begär information från systemen via gränssnittstjänsterna. Ett certifikat beviljas för organisationer som svarar för att leverera uppgifter till eller som har rätt att få uppgifter. Certifikattjänsten tillhandahåller certifikat för både testning och produktion.

Skatteförvaltningen beviljar kunder certifikat för Skatteförvaltningens, inkomstregistrets och det positiva kreditupplysningsregistrets gränssnitt. I detta dokument beskrivs systemet på ett allmänt plan och endast ur ett tekniskt perspektiv. När du använder olika instansers gränssnitt ska du alltid också ta del av den instansens egna anvisningar. Till exempel användning av uppgifter i inkomstregistret eller det positiva kreditupplysningsregistret kräver uppgiftstillstånd som beviljas av den aktuella instansen.

Skatteförvaltningens certifikat baserar sig på PKI-lösningen (Public Key Infrastructure). Kunden har en eller flera nyckelpar (privat och offentlig nyckel) och ett certifikat som anknyter till nyckelparet och som är i förenlig med X.509-standarden. Certifikatet används för att identifiera kunden och underteckna inlämnat material med elektronisk signatur (XML Signature).

Kunden administrerar sin organisations gränssnittsrättigheter via certifikattjänstens e-tjänst. Via tjänsten lämnar kunden in ansökningar om gränssnitt, beställer certifikat och administrerar certifikatuppgifterna. Certifikaten skapas och förvaras i det bakomliggande PKI-systemet. Certifikat kan hämtas antingen från e-tjänsten eller PKI-systemets gränssnitt.

Man loggar in i e-tjänsten via Skatteförvaltningens certifikattjänst. På samma sida finns anvisningar för ansökan om gränssnitt samt beställning av certifikat för testning och produktion. Inloggning i e-tjänsten sker med bankkoder, mobilcertifikat eller certifikatkort.

1.2 Användningsändamål för och typer av certifikat

Certifikaten beviljas alltid för en viss kund och för ett visst användningsändamål, och kan inte användas för ett ändamål som avviker från det ursprungliga. Kunden bör ta del av användarvillkoren för Skatteförvaltningens och inkomstregistrets gränssnittstjänster och iaktta dem.

Om kunden använder Skatteförvaltningens tekniska gränssnitt för olika ändamål (till exempel som producent av löne- eller förmånsuppgifter och användare av uppgifter i inkomstregistret) ska separata certifikat beställas för de olika användningsändamålen. Likaså kräver olika gränssnitt separata certifikat. En aktör kan alltså ha flera certifikat. Om kunden använder flera certifikat i samma programvara ska särskild uppmärksamhet fästas vid administrationen av certifikaten.

Gränssnitt	Kanal	Certifikatutfärdare
Producent av löneuppgifter (Web Service)	Web Service (SOAP)	Data Providers Issuing CA
Producent av löneuppgifter (SFTP)	SFTP	Data Providers SFTP Issuing CA
Producent av förmånsuppgifter (WS)	Web Service (SOAP)	IR Benefit Data Providers Issuing CA
Producent av förmånsuppgifter (SFTP)	SFTP	IR Benefit Data Providers SFTP Issuing CA
Informationsanvändare (WS)	Web Service (SOAP)	IR Income Data Users Issuing CA
Informationsanvändare (SFTP)	SFTP	IR Income Data Users SFTP Issuing CA
Inkomstregistrets utomstående stödtjänster	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
Anmälare av kreditupplysningar	Web Service (REST)	Data Providers Issuing CA
Användare av kreditupplysningar	Web Service (REST)	PCR Credit Data Users Issuing CA v1

Tabell 1: Typer och utfärdare av certifikat

Certifikaten skapas enligt ovan nämnda utfärdare (Certificate Authority, CA), och motsvarande publikationspaket kan laddas ner i Dokumentation i certifikattjänsten.

1.3 Beställning av certifikat

Certifikat beställs alltid via certifikattjänstens e-tjänst. I samband med beställningen anger kunden en teknisk kontaktperson för certifikatet, och certifikattjänsten skickar den information som behövs för hämtning av certifikatet till kontaktpersonen: överföringskod (TransferId) och engångslösenord (TransferPassword). Denna

information skickas till den tekniska kontaktpersonen i ett säkert e-postmeddelande som kontaktpersonen öppnar med en pinkod som skickas per sms. Engångslösenordet är giltigt i 14 dygn. Om certifikatet inte hämtas inom denna tid går engångslösenordet ut, och kunden måste göra en ny certifikatbeställning.

På bild 1 finns en beskrivning av hur ett nytt certifikat beställs. Detaljerade anvisningar för beställning finns i e-tjänsten på sidan Skatteförvaltningens certifikattjänst.

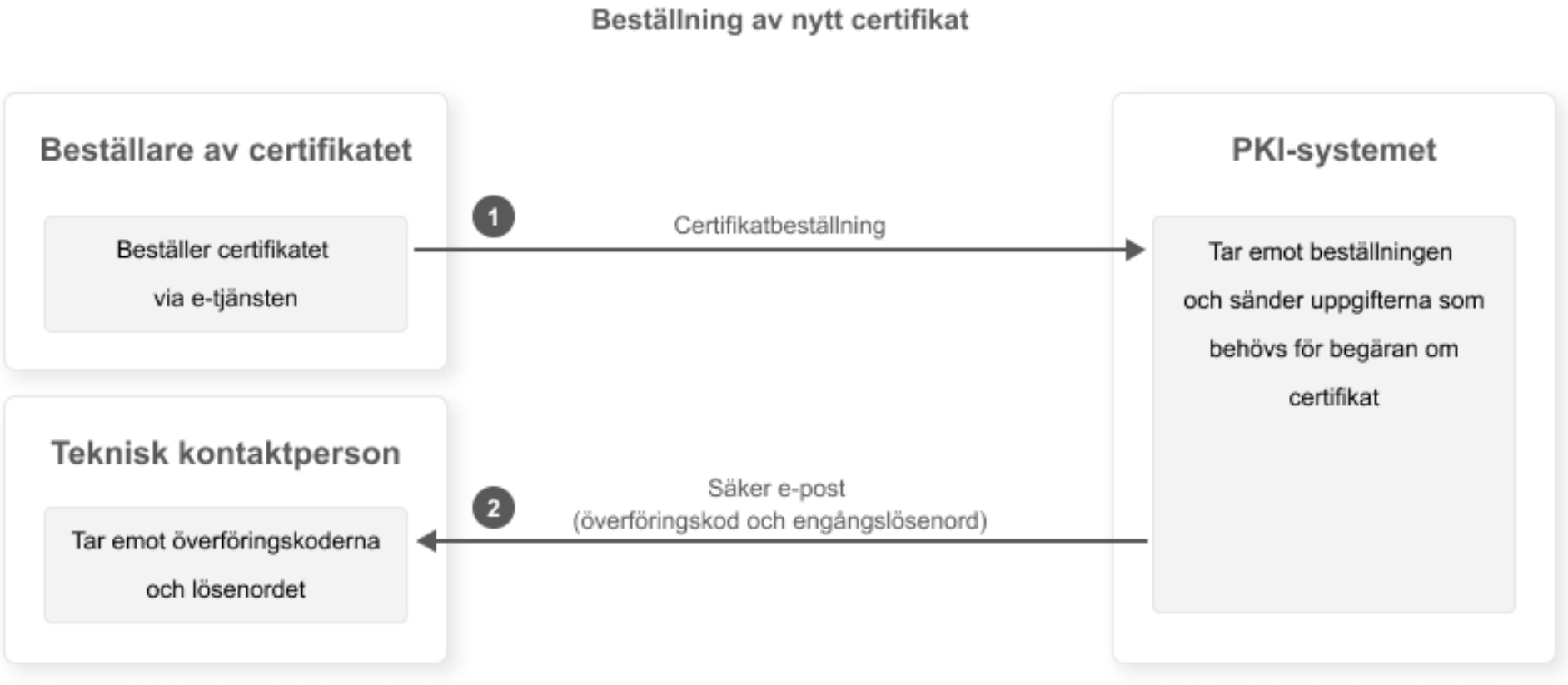


Bild 1: Beställning av certifikat.

1.4 Hämtning av certifikat

Certifikat kan hämtas antingen via gränssnittet eller e-tjänsten. Bägge sätten förutsätter en överföringskod, ett engångslösenord och en signaturbegäran för certifikatet (CSR). För begäran om certifikat ska kunden skapa ett nyckelpar med 2048-bitar med hjälp av en RSA-algoritm. Dessutom skapar kunden en signaturbegäran för certifikatet i enlighet med PKCS#10-definitionen (Certificate Signing Request, CSR), och denna innehåller kundens offentliga nyckel.

När certifikatet hämtas från e-tjänsten (bild 2), anger kunden överföringskoden, lösenordet och signaturbegäran i användargränssnittet. Certifikatet laddas ner på datorn.

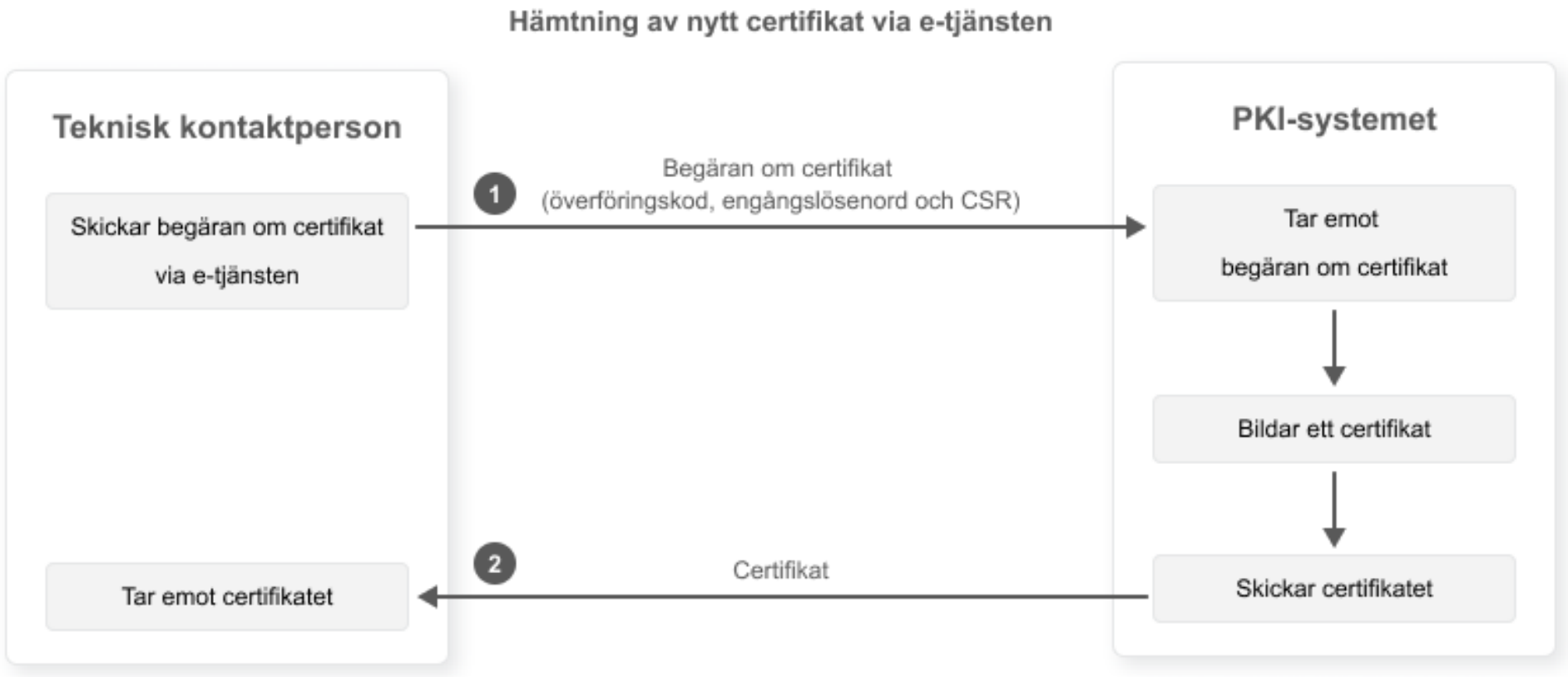


Bild 2: Hämtning av certifikat via e-tjänsten.

När ett certifikat hämtas via ett gränssnitt (bild 3) ska kunden foga överföringskoden, lösenordet och signaturbegäran till tjänsteanropet för det nya certifikatet (SignNewCertificateRequest). Tjänsteanropet skickar som mottagningskvittering en hämtningskod (RetrievalID). Efter att ha fått hämtningskoden ska kunden vänta i cirka 10–30 sekunder. Därefter skapar kunden ett tjänsteanrop för4r hämtning av certifikatet (GetCertificateRequest) och fogar det till hämtningskoden. Kunden får certifikatet med svaret på tjänsteanropet Om certifikatet inte kan bildas på grund av ett fel skickas ett felmeddelande i stället för certifikatet.

Adress till gränssnittet för produktionscertifikat: https://pkiws.vero.fi/2017/10/CertificateServices

Adress till gränssnittet för testcertifikat: https://pkiws-testi.vero.fi/2017/10/CertificateServices

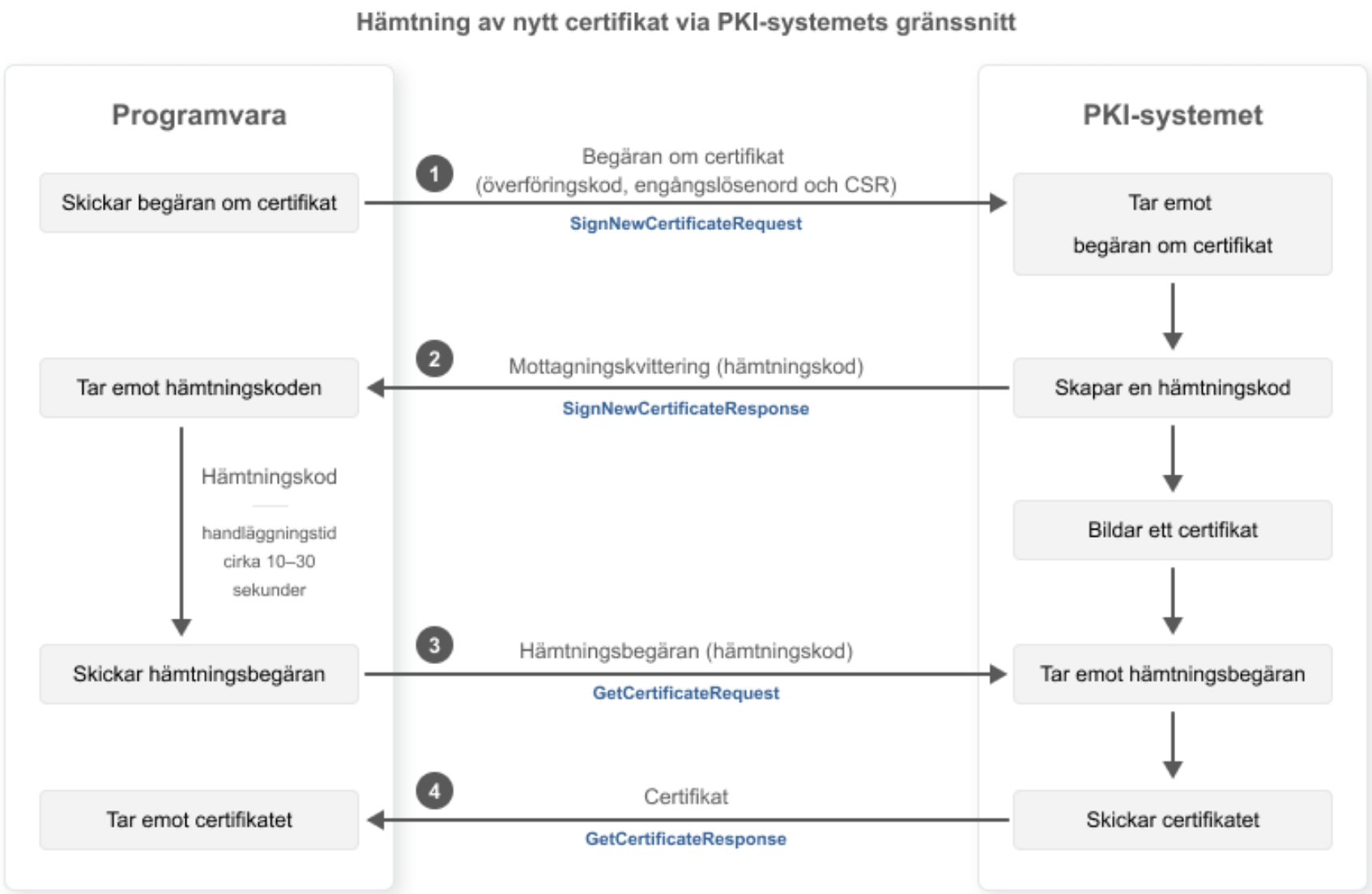


Bild 3: Hämtning av certifikat via gränssnitt.

1.5 Stängning av certifikaten

Kunden ska begära stängning av ett produktionscertifikat, om man känner till eller misstänker att certifikatinnehavarens privata nyckel har försvunnit eller hamnat i fel händer. Ett certifikat måste också stängas, om det är onödigt. Certifikatutfärdaren dvs. Skatteförvaltningen kan stänga ett certifikat till exempel när ett avtal som berättigar till användning av tjänsten upphör eller om det är uppenbart att det beviljade certifikatet har missbrukats.

Kunden stänger produktionscertifikatet genom att kontakta inkomstregistrets kundservice. Detaljerade anvisningar finns på sidan Stängning av certifikaten. Inkomstregistrets kundservice ansvarar för stängning av Skatteförvaltningens, inkomstregistrets och det positiva kreditupplysningsregistrets produktionscertifikat.

Man kan begära stängning av produktionscertifikat när som helst. När en kund utanför tjänstetid begär att certifikatet ska stängas, stängs det först tillfälligt (tillfälligt användningsförbud). I detta fall har användningen av certifikatet spärrats, men certifikatet kan aktiveras på nytt. Om kunden bekräftar stängningen stängs certifikatet för gott. Kunden ska bekräfta stängningen eller aktivera certifikatet på nytt inom 14 dygn från att tillfälligt användningsförbud aktiverats. Om kunden inte under denna tid aktiverar certifikatet på nytt stänger Skatteförvaltningen det slutgiltigt.

Ett certifikat som för gott stängts kan inte återställas för användning, och det kan inte heller förnyas, utan kunden måste beställa ett nytt certifikat. Då ska kunden göra en ny ansökan om gränssnitt i certifikattjänstens e-tjänst och hämta certifikatet certifikat samma sätt som första gången.

Du kan stänga ett testcertifikat genom att fylla i certifikattjänstens observationsblankett.

1.6 Certifikatens livscykel och förnyande av dessa

Kundens produktions- eller testcertifikat gäller i två år. Om man vill förnya certifikatet ska det göras innan det går ut. Certifikatinnehavaren ska regelbundet kontrollera certifikatens giltighetstid. Det går att kontrollera den sista giltighetsdagen i certifikattjänstens e-tjänst eller på certifikatet.

Certifikat förnyas via PKI-systemets gränssnitt. Ett certifikat kan förnyas tidigast sextio (60) dygn innan det går ut. Det gamla certifikatet förblir i kraft till slutet av den ursprungliga giltighetstiden. Om certifikatet förnyas i tid behöver inget nytt certifikat beställas, och kunden behöver inte nya överföringskoder eller engångslösenord.

På bild 4 finns en beskrivning av hur ett certifikat förnyas via gränssnitt.

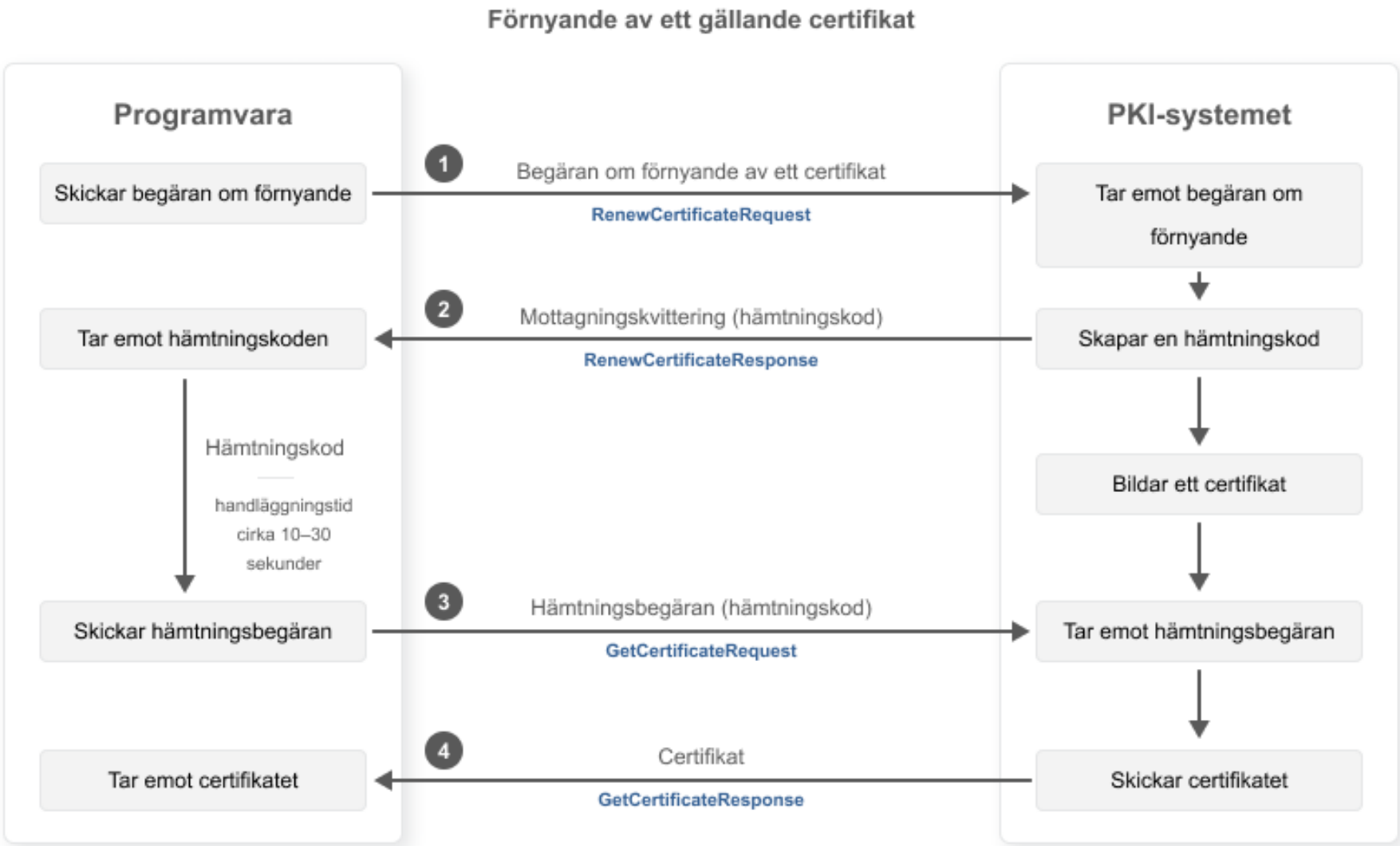


Bild 4: Förnyelse av certifikat via gränssnitt.

Det finns en separat tjänst för förnyelse i gränssnittet (RenewCertificate). För förnyelse skapar kunden ett nytt nyckelpar och signaturbegäran för certifikatet samt undertecknar tjänsteanropet med den privata nyckeln för certifikatet.

Vid undertecknande av certifikatet används samma form som när kunden skickar material med ett giltigt certifikat via gränssnitt. Vid begäran om förnyelse av certifikat får kunden en hämtningskod för certifikatet med mottagningskvitteringen. Kunden hämtar certifikatet på samma sätt som ett nytt certifikat. Kunden ska först vänta i cirka 10–30 sekunder. Därefter skapar kunden ett tjänsteanrop för4r hämtning av certifikatet (GetCertificateRequest) och fogar det till hämtningskoden. Kunden får certifikatet med svaret på tjänsteanropet

Obs! Det tidigare certifikatet ska ersättas med ett nytt utan dröjsmål, dock senast innan det tidigare certifikatets giltighetstid går ut. Om samma certifikat har använts på flera än ett ställe, ska alla kopior av det gamla certifikatet ersättas med det nya för att undvika felsituationer som det gamla certifikatet kan ge upphov till.

Om certifikatet har gått ut ska kunden beställa ett nytt certifikat via e-tjänsten. I detta fall beställs och hämtas ett nytt certifikat på samma sätt som när man beställer ett certifikat första gången.

2 TERMER OCH FÖRKORTNINGAR

Förkortningar som används i certifikattjänsten och de viktigaste termerna.

Förkortning eller term	Förklaring
CSR (Certificate Signing Request) Begäran om att underteckna ett certifikat	Signaturbegäran för certifikat av användaren av certifikattjänsten. Det är en Base64-kodad teckensekvens i PKCS#10-format.
Kryptering med offentlig nyckel	Asymmetrisk kryptering där den ena nyckeln är offentlig och den andra privat.
Hämtningskod (RetrievalID)	En kod som kan användas för att hämta ett certifikat senare.
PKCS#10 (Public Key Cryptography Standards # 10)	En standard där formen för och innehållet i begäran om att underteckna ett certifikat fastställs.
PKI (Public Key Infrastructure)	Ett system som utnyttjar metoden med en offentlig nyckel och som används av certifikatutfärdaren för att tillhandahålla och upprätthålla certifikat.
Private key (Privat nyckel)	En sekretessbelagd del som består av ett asymmetriskt nyckelpar som används i kryptering med offentlig nyckel. Vanligtvis används en privat nyckel för en elektronisk signatur eller för att öppna ett meddelande som har krypterats med en offentlig nyckel.
Public Key (Offentlig nyckel)	Den offentliga delen av det asymmetriska nyckelparet. Den offentliga nyckeln används vanligtvis för att kryptera ett meddelande och den privata nyckeln för att verifiera signaturen.
Gränssnitt	En standardenlig praxis eller förbindelse som möjliggör överföring av information mellan enheter, programvara eller användare.
RSA-kryptering	En krypteringsmetod med offentlig nyckel som baserar sig på en krypteringsalgoritm som utvecklats av Rivest, Shamir och Adleman
SFTP (Secure File Transfer Protocol)	Ett dataöverföringsprotokoll som möjliggör en krypterad dataöverföringsförbindelse mellan två system.
SGML (Standard Generalized Markup Language)	Ett markeringsspråk som används för att markera de olika delarna i materialet och deras inbördes förhållande.
Överföringskod (TransferID)	En kod som skickats till kunden för begäran om ett certifikat.
Certifikatbeställning	Beställning av certifikat via Skatteförvaltningens certifikattjänst.
Begäran om certifikat	Meddelande om begäran i gränssnittets SignNewCertificate-tjänst via vilken kunden påbörjar hämtningen av ett tidigare beställt certifikat.
Begäran om hämtning av certifikat	Meddelande om begäran i gränssnittets GetCertificate-tjänst via vilken kunden hämtar ett tidigare beställt certifikat.
Begäran om förnyande av ett certifikat	Meddelande om begäran i gränssnittets RenewCertificate-tjänst via vilken kunden förnyar ett giltigt certifikat.

WS (Web Service)	En programvara som används i webbservern och som med hjälp av standardiserad webbförbindelsepraxis ställer tjänster till förfogande för applikationerna. De tjänster som certifikattjänsten tillhandahåller är begäran om, hämtning och förnyande av certifikat.
XML (Extensible Markup Language)	Ett för internetanvändning särskilt avgränsat markeringsspråk som grundar sig på SGML-språket och som lätt kan utvidgas.
XML Signature (underskrift)	En XML-underskrift som bildats med hjälp av kundens giltiga certifikat.
X.509	En standard som fastställer certifikatets struktur.

Tabell 2: Termer och förkortningar.

3 GRÄNSSNITTETS NAMNRYMD, TECKEN OCH LÄSANVISNING

Nedan beskrivs hur gränssnittet Web Service i PKI-systemet i Skatteförvaltningens certifikattjänst har byggts upp med tanke på den som förverkligar systemintegreringen. Dokumentet innehåller en beskrivning av tjänsterna i gränssnittet samt datainnehållet i tjänsterna (XML-scheman).

Den tekniska uppbyggnaden av gränssnittet för PKI-systemets gränssnitt beskrivs på den detaljnivå som krävs för att parterna utifrån den kan fastställa och bygga upp sitt eget system tillsammans med integrationen i PKI-systemet.

3.1 PKI-systemets Web Service-gränssnitt

Tjänsterna i gränssnittet definieras i beskrivningen **CertificateServices.wsdl**.

I beskrivningen används följande namnrymder:

Filens namn	Prefix	Namespace
XMLSchema	xmlns:xs	http://www.w3.org/TR/2001/NOTE-SOAP-20000508/
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 Schema

För hanteringen av livscykeln för certifikaten som beviljats i PKI-systemet används element i enlighet med XML-schemat **CertificateServices.xsd**.

I schemat används följande namnrymder:

Filens namn	Prefix	Namespace
XMLSchema	xmlns:xs	http://www.w3.org/TR/2001/NOTE-SOAP-20000508/
CertificateServices.xsd	xmlns:ser	http://certificates.vero.fi/2017/10/certificateservices

Tomma element godkänns inte i meddelandena. Om ett element inte får ett värde, utelämnas det helt från meddelandet. Tomma teckensekvenser godkänns inte, dvs. längden på alla värden är minst 1.

3.3 Teckentabell

I schemana används standardteckentabellen för XML, UTF-8. Filen får inte innehålla tecknet Byte Order Mark (BOM).

I tabellen nedan presenteras kraven på konvertering av specialtecken som förekommer i meddelandena.

Märke	Beskrivning	Format som entitet
&	et-tecken	& obligatorisk konvertering
<	mindre än	< obligatorisk konvertering
>	större än	> konvertering är inte obligatorisk, men förenlig med god praxis
'	apostrof	' konvertering är inte obligatorisk, men förenlig med god praxis
"	citattecken	" konvertering är inte obligatorisk, men förenlig med god praxis
--	dubbelstreck	Tecknet får inte förekomma i en xml-fil
/*	snedstreck asterisk	Tecknet får inte förekomma i en xml-fil
&#	et-tecken nummertecken	Tecknet får inte förekomma i en xml-fil

3.4 Läsanvisning för scheman

Markeringen 0 .. längst nere till höger i elementen i dokumentets scheman ∞ betyder att elementet kan upprepas flera gånger och kan också saknas helt. Markeringen 1 .. ∞ betyder att elementet kan upprepas flera gånger, men alltid minst en gång. Obligatoriska element har märkts ut med en sammanhängande kantlinje och frivilliga element med en streckad kantlinje.

I dokumenttabellerna anges elementens obligatoriskhet och även antalet förekomster i kolumnen ”Elementens obligatoriskhet”. Antalet element står i formen A:B där A anger minimiantalet av det aktuella elementet som meddelandet ska innehålla (minOccurs), och maximiantalet av det aktuella elementet som meddelandet får innehålla (maxOccurs). Som värden används följande värden:

0 = elementet kan saknas

1 = elementet förekommer en gång

N = N är ett numeriskt värde, och elementet förekommer N gånger

unbounded = elementet förekommer i ett antal som inte fastställs på förhand

4 GRÄNSSNITTETS TJÄNSTER OCH ÅTGÄRDANDE AV FEL

4.1 Gränssnittets tjänster

I följande tabell beskrivs tjänsterna i gränssnittet:

Operation	Meddelande om begäran	Svarsmeddelande	Beskrivning
Begäran om ett nytt certifikat (SignNewCertificate)	SignNewCertificateRequestMessage	SignNewCertificateResponseMessage	Begäran om certifikat genom vilken kunden påbörjar hämtningen av ett nytt certifikat. Före begäran om certifikat ska kunden beställa ett nytt certifikat via Skatteförvaltningens certifikattjänst. Begäran om certifikat används när • kunden hämtar organisationens första certifikat • kunden redan har ett eller flera gällande certifikat, men behöver fler certifikat • kundens tidigare certifikat inte längre är i kraft eller har revokerats, dvs. tagits ur användning.
Förnyelse av ett giltigt certifikat (renewCertificate)	RenewCertificateRequestMessage	RenewCertificateResponseMessage	Begäran om förnyande av ett certifikat när det certifikat som innehas av en användare håller på att gå ut, och förnyandet görs innan det gällande certifikatet går ut.
Hämtning av certifikat (GetCertificate)	GetCertificateRequestMessage	GetCertificateResponseMessage	Hämtning av ett tidigare begärt certifikat eller ett förnyat certifikat. Tiden mellan svarsmeddelandet om begäran om certifikat eller förnyelse av giltigt certifikat och meddelandet om begäran om hämtning av certifikat ska vara minst 10 sekunder.

Datainnehållet i meddelandena i tjänsterna för gränssnittet beskrivs i avsnitt 5.

4.2 Signering av meddelanden

I tjänsterna för gränssnittet Web Service används elektronisk signatur (XML Signature). Med denna verifieras vem som har skapat datainnehållet i meddelandet i de meddelanden som definieras i kapitel 5. Signaturen är också en garanti för att meddelandet inte har ändrats. Signaturen utförs med mekanismen XML

Enveloped Signature, vars processeringsregler och struktur beskrivs i dokumentet XML Signature Syntax and Processing (http://www.w3.org/TR/xmldsig-core/). Ett exempel på elektronisk signatur finns i avsnitt 9 i detta dokument.

4.3 Åtgärdande av fel

I felsituationer returneras felmeddelanden med svarsmeddelandet i enlighet med strukturen som beskrivs i datainnehållet. Elementet Uppgifter om felet innehåller en kod för felet och en förklaring till felkoden. Om ett fel upptäcks innan den egentliga tjänstebegäran behandlas (behandling av ett SOAP-meddelande), returnerar tjänsten endast ett HTTP-fel. HTTP-felet kan vara till exempel HTTP 404 Not found. Tjänsten kan också returnera ett felmeddelande i enlighet med strukturen SOAP 1.1 Fault med felkoden HTTP 500 (Internal Server Error). SOAP Fault kan returneras bland annat i situationer i vilka SOAP-ramen inte är valid, om det mottagna meddelandet inte kan struktureras som ett XML-dokument eller om dokumentet inte godkänns i schemavalideringen.

I allmänhet returneras informationen om fel omedelbart med tjänstens svar. En del fel upptäcks dock först när begäran om certifikat behandlas, och då returnerar tjänsteanropet för ansökan om certifikat ett felmeddelande i stället för certifikatet.

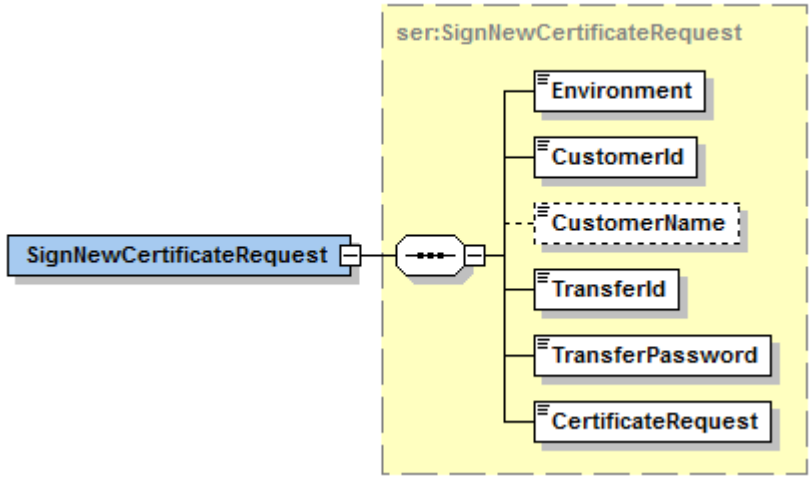
Omedelbart i mottagningskvitteringen för tjänsteanropet ges information om fel när

- tjänsteanropet inte är i enlighet med schemat
- fel överföringskod
- den signaturbegäran för certifikatet som eventuellt har fogats till begäran har skapats på ett felaktigt sätt
- kontrollen av den elektroniska signaturen som används för att förnya certifikatet misslyckas
- det uppstår något annat tekniskt fel som orsakats av en avvikande situation.

Om certifikatet inte går att skapa ska eventuella fel, såsom felaktiga koder, korrigeras. Därefter ska tjänsteanropet för certifikatbegäran skickas på nytt. Ett undantag utgörs dock av situationer där systemet inte har hunnit behandla begäran om certifikat innan kunden försöker hämta certifikatet. Då kan man försöka hämta certifikatet på nytt efter 10–30 sekunder.

5 DATAINNEHÅLLET I GRÄNSSNITTETS TJÄNSTER

5.1 Begäran om ett nytt certifikat – meddelande om begäran (SignNewCertificateRequest)

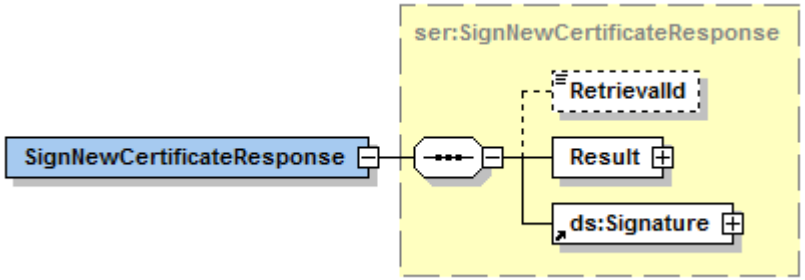


Uppgifter om datagruppen *SignNewCertificateRequest*:

Uppgiftens namn	Typ	Tillåtna värden	Elementets obligatoriskhet (minOccurs: maxOccurs)	Förklaring till uppgiften
Miljö (Environment)	ser:EnvironmentTypes	PRODUCTION, TEST	1:1	I produktionsmiljö ska värdet vara PRODUCTION och i testmiljö ska värdet vara TEST.
Kundnummer (CustomerId)	ser:String30		1:1	Kundens identifierare. Som identifierare används organisationens officiella identifierare för kommunikationen med Skatteförvaltningen. Identifieraren kan vara till exempel ett FO-nummer. Om man använder FO-nummer, ska numret

Uppgiftens namn	Typ	Tillåtna värden	Elementets obligatoriskhet (minOccurs: maxOccurs)	Förklaring till uppgiften
				finnas i Företags- och organisationsdatasystemet (FODS) och ha bindestreck.
Kundens namn (CustomerName)	ser:String100		0:1	Kundens namn. Uppgiften används inte som sådan med ett certifikat, men den är till hjälp i en eventuell utredning av fel.
Överföringskod (TransferId)	ser:String32		1:1	En kod som skickats till kunden för begäran om ett certifikat.
Engångslösenord (TransferPassword)	ser:String16		1:1	Ett engångslösenord som skickats till kunden för begäran om ett certifikat.
Signaturbegäran för certifikatet (CertificateRequest)	ser:CertificateRequestType		1:1	Kundens signaturbegäran för certifikatet som är en Base64-kodad teckensekvens i PKCS#10-format.

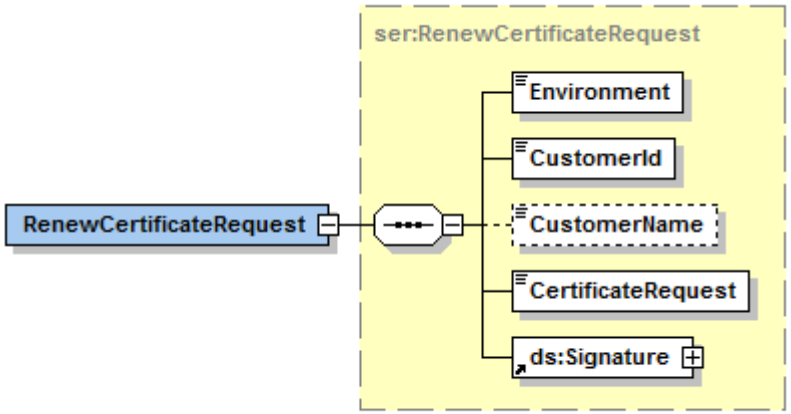
5.2 Begäran om ett nytt certifikat – svarsmeddelande (SignNewCertificateRequest)



Uppgifter om datagruppen *SignNewCertificateResponse*:

Uppgiftens namn	Typ	Tillåtna värden	Elementets obligatoriskhet (minOccurs: maxOccurs)	Förklaring till uppgiften
Hämtningskod för certifikatet (RetrievalId)	ser:String32		0:1	En kod som kan användas för att hämta ett certifikat senare.
Resultat av behandlingen (Result)	ser:Result		1:1	Resultat av behandlingen, se närmare innehåll i beskrivningen av elementet Resultat av behandlingen av ett meddelande.
XML-signatur (Signature)	ds:Signature		1:1	XML-signatur som PKI-systemet bildar med sitt eget certifikat.

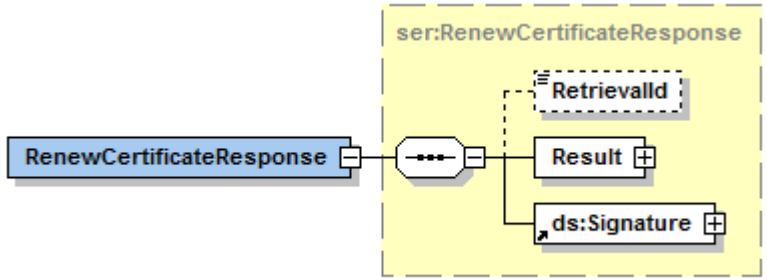
5.3 Förnyelse av giltigt certifikat – meddelande om begäran (RenewCertificateRequest)



Uppgifter om datagruppen *RenewCertificateRequest*:

Uppgiftens namn	Typ	Tillåtna värden	Elementets obligatoriskhet (minOccurs: maxOccurs)	Förklaring till uppgiften
Miljö (Environment)	ser:EnvironmentTypes	PRODUCTION, TEST	1:1	I produktionsmiljö ska värdet vara PRODUCTION och i testmiljö ska värdet vara TEST.
Kundnummer (CustomerId)	ser:String30		1:1	Kundens identifierare. Som identifierare används organisationens officiella identifierare för kommunikationen med Skatteförvaltningen. Identifieraren kan vara till exempel ett FO-nummer. Om man använder Fo-nummer, ska numret finnas i Företags- och organisationsdatasystemet (FODS) och ha bindestreck.
Kundens namn (CustomerName)	ser:String100		0:1	Kundens namn. Uppgiften används inte som sådan med ett certifikat, men den är till hjälp i en eventuell utredning av fel.
Begäran om ett certifikat (CertificateRequest)	ser:CertificateRequestType		1:1	Kundens signaturbegäran för certifikatet som är en Base64-kodad teckensekvens i PKCS#10-format.
XML-signatur (Signature)	ds:Signature		1:1	XML-signatur som kunden bildar med sitt eget gällande certifikat.

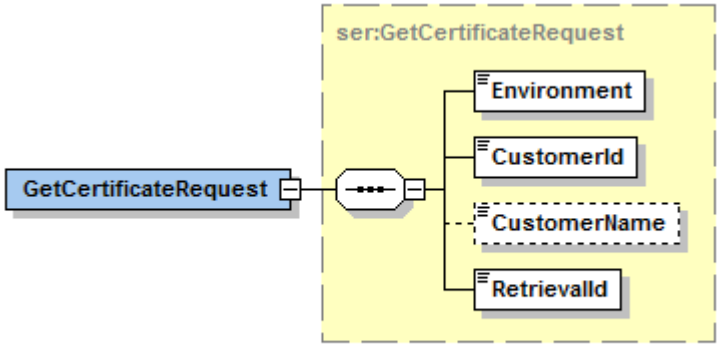
5.4 Förnyande av ett gällande certifikat – svarsmeddelande (RenewCertificateResponse)



Uppgifter om datagruppen *RenewCertificateResponse*:

Uppgiftens namn	Typ	Tillåtna värden	Elementets obligatoriskhet (minOccurs: maxOccurs)	Förklaring till uppgiften
Hämtningskod för certifikatet (RetrievalId)	ser:String32		0:1	En kod som kan användas för att hämta ett certifikat senare.
Resultat av behandlingen (Result)	ser:Result		1:1	Resultat av behandlingen, se närmare innehåll i beskrivningen av elementet Resultat av behandlingen av ett meddelande.
XML-signatur (Signature)	ds:Signature		1:1	XML-signatur som PKI-systemet bildar med sitt eget certifikat.

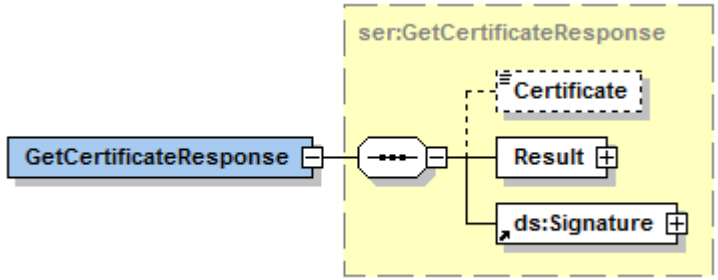
5.5 Hämtning av ett certifikat – meddelande om begäran (GetCertificateRequest)



Uppgifter om datagruppen *GetCertificateRequest*:

Uppgiftens namn	Typ	Tillåtna värden	Elementets obligatoriskhet (minOccurs: maxOccurs)	Förklaring till uppgiften
Miljö (Environment)	ser:EnvironmentTypes	PRODUCTION, TEST	1:1	I produktionsmiljö ska värdet vara PRODUCTION och i testmiljö ska värdet vara TEST.
Kundnummer (CustomerId)	ser:String30		1:1	Kundens identifierare. Som identifierare används organisationens officiella identifierare för kommunikationen med Skatteförvaltningen. Identifieraren kan vara till exempel ett FO-nummer. Om man använder FO-nummer, ska numret finnas i Företags- och organisationsdatasystemet (FODS) och ha bindestreck.
Kundens namn (CustomerName)	ser:String100		0:1	Kundens namn. Uppgiften används inte som sådan med ett certifikat, men den är till hjälp i en eventuell utredning av fel.
Hämtningskod för certifikatet (RetrievalId)	ser:String32		1:1	Hämtningskod som PKI-systemet returnerar på meddelanden om begäran om ett certifikat eller meddelanden för förnyande av ett certifikat.

5.6 Hämtning av ett certifikat – svarsmeddelande (GetCertificateResponse)

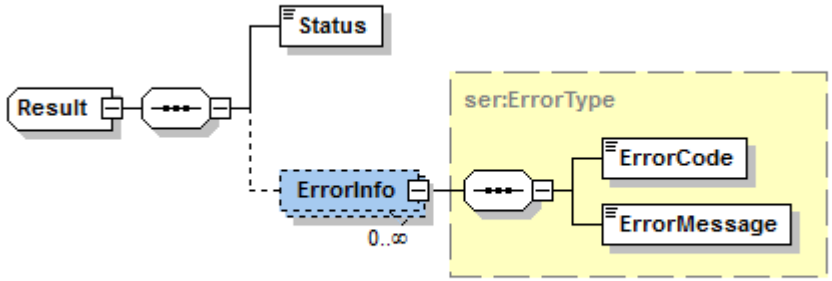


Uppgifter om datagruppen *GetCertificateResponse*:

Uppgiftens namn	Typ	Tillåtna värden	Elementets obligatoriskhet (minOccurs: maxOccurs)	Förklaring till uppgiften
Kundens certifikat (Certificate)	ser:CertificateType		0:1	Kundens certifikat som PKI-systemet undertecknat. Certifikatet levereras Base64-kodat.
Resultat av behandlingen (Result)	ser:Result		1:1	Resultat av behandlingen, se närmare innehåll i beskrivningen av elementet Resultat av behandlingen av ett meddelande.
XML-signatur (Signature)	ds:Signature		1:1	XML-signatur som PKI-systemet bildar med sitt eget certifikat.

5.7 Resultat av behandlingen av ett meddelande (Result)

Denna datastruktur beskriver datainnehållet i elementet Result. Elementet beskriver resultatet av behandlingen av svarsmeddelanden i anslutning till att ett certifikat begärs, förnyas eller hämtas. I en felsituation innehåller elementet förutom resultatet av behandlingen även uppgifter om felet.



Uppgifter om datagruppen *Result*:

Uppgiftens namn	Typ	Tillåtna värden	Elementets obligatoriskhet (minOccurs: maxOccurs)	Förklaring till uppgiften
Resultat av behandlingen av ett meddelande (Status)	ser:ResultTypes	FAIL, OK	1:1	Resultat av behandlingen av ett meddelande. I felsituationer återställs värdet FAIL, och närmare information om felet sänds i elementet Uppgifter om felet. Om behandlingen lyckas, återställs värdet OK, och elementet Uppgifter om felet återställs inte.
Uppgifter om felet (ErrorInfo)	ser:ErrorType		0:unbounded	I elementet returneras felmeddelandena.
Felkod (ErrorCode)	ser:String10		1:1	Felets kod returneras i elementet.
Felkodens förklaring (ErrorMessage)	ser:String255		1:1	Felkodens förklaring returneras i elementet.

Felkoderna för felsituationerna och förklaringarna till dessa beskrivs i avsnitt 6.

6 FELKODER OCH FÖRKLARINGAR TILL DEM

Begäran om ett nytt certifikat – eventuella felsituationer som svarsmeddelandet returnerar:

Felkod	Förklaring till felkoden	Beskrivning av felet
PKI005	Wrong environment type specified	Värdet på parametermiljön (Environment) i meddelande om begäran motsvarar inte värdet som definierats i målsystemet. Efter korrigering av parametervärdet kan man försöka på nytt.
PKI020	Invalid credentials	Någon av de angivna identifierarna, kundnumret (CustomerId), överföringskoden (TransferId) eller engångslösenordet (TransferPassword) är felaktig. Efter kontrollen och korrigeringen av parametrarna ska en ny begäran om certifikat göras.
PKI030	Attached CSR is not valid	Signaturbegäran för certifikatet (CSR) i meddelandet om begäran är felaktig. Efter en ny signaturbegäran kan man försöka på nytt.
PKI040	The certificate signing request (CSR) is invalid or has been used already.	Signaturbegäran för certifikatet (CSR) är felaktig eller har redan använts tidigare. Skapa en ny signaturbegäran och försök på nytt. Om problemet fortgår ska du ta kontakt med observationsblanketten i certifikattjänsten.
PKI099	Generic Technical Error	Felsituation som saknar en definierad felkod. Format för felaktigt anrop, kontrollera uppgifterna. Kontakta Skatteförvaltningens certifikattjänst på observationsblanketten om felet återkommer ofta.

Förnyelse av ett gällande certifikat – eventuella felsituationer som svarsmeddelandet returnerar:

Felkod	Förklaring till felkoden	Beskrivning av felet
PKI005	Wrong environment type specified	Värdet på parametermiljön (Environment) i meddelande om begäran motsvarar inte värdet som definierats i målsystemet. Efter korrigering av parametervärdet kan man försöka på nytt.
PKI010	Signature verification failed	Kontrollen av innehållet i begäran om förnyelse av certifikat misslyckades. Meddelandet ska undertecknas med det

Felkod	Förklaring till felkoden	Beskrivning av felet
		certifikat som förnyas. Efter korrigering av eventuell felaktig signatur kan anropet skickas på nytt.
PKI015	Invalid certificate to be renewed received	Certifikatet med vilket meddelandet om begäran har undertecknats är felaktigt eller innehåller inte de obligatoriska uppgifterna. Begäran om certifikat kan skickas på nytt efter att meddelandet har undertecknats med rätt certifikat.
PKI030	Attached CSR is not valid	Signaturbegäran för certifikatet (CSR) är felaktig. Efter en ny signaturbegäran kan man försöka på nytt.
PKI040	The certificate signing request (CSR) is invalid or has been used already.	Signaturbegäran för certifikatet (CSR) är felaktig eller har redan använts tidigare. Skapa en ny signaturbegäran och försök på nytt. Om problemet fortgår ska du ta kontakt med observationsblanketten i certifikattjänsten.
PKI080	Certificate renewal not yet allowed	Certifikat kan förnyas först när det återstår högst 60 dygn innan det går ut.
PKI099	Generic Technical Error	Felsituation som saknar en definierad felkod. Format för felaktigt anrop, kontrollera uppgifterna. Kontakta Skatteförvaltningens certifikattjänst på observationsblanketten om felet återkommer ofta.

Hämtning av certifikat – eventuella felsituationer som svarsmeddelandet returnerar:

Felkod	Förklaring till felkoden	Beskrivning av felet
PKI005	Wrong environment type specified	Värdet på parametermiljön (Environment) i meddelande om begäran motsvarar inte värdet som definierats i målsystemet. Efter korrigering av parametervärdet kan man försöka på nytt.
PKI020	Invalid credentials	Någon av de angivna identifierarna, kundnumret (CustomerId), överföringskoden (TransferId) eller engångslösenordet (TransferPassword) är felaktig vid begäran om nytt certifikat eller förnyelse av certifikat. Efter kontrollen av identifierarna ska den ursprungliga begäran om certifikat eller förnyelsen av giltigt certifikat och hämtningen av certifikatet göras på nytt.

Felkod	Förklaring till felkoden	Beskrivning av felet
		Enbart förnyelse av hämtningen av certifikatet returnerar det ursprungliga PKI020-felet.
PKI099	Generic Technical Error	Felsituation som saknar en definierad felkod. Format för felaktigt anrop, kontrollera uppgifterna. Denna felsituation uppstår till exempel om certifikatet hämtas för snabbt efter begäran eller förnyelse av certifikat, eftersom PKI-systemet då inte hunnit behandla meddelandet om begäran. Kontakta Skatteförvaltningens certifikattjänst på observationsblanketten om felet återkommer ofta. Eftersom tjänsten är asynkronisk till sin karaktär, kan felet ha uppstått tidigare. Vid begäran om och förnyelse av certifikat har man till exempel lämnat felaktiga uppgifter och skapandet av certifikatet har misslyckats.

7 ANVISNINGAR FÖR TESTBÄDDEN

Syftet med testbädden för certifikattjänsten är att underlätta utvecklingen av en applikation som använder certifikattjänstens gränssnitt. I testbädden kan man testa sändningen av en signaturbegäran för certifikatet, sändningen av en begäran om förnyande av ett certifikat och hämtningen av ett certifikat.

I testbädden används på förhand specificerade engångsidentifierare, PKI-nycklar och certifikat. På grund av detta kan Web Service-begäran upprepas flera gånger med samma parametrar. Till exempel överföringskoden (TransferId) för ”Signaturbegäran för ett nytt certifikat” och ”engångslösenord” (TransferPassword) kan användas flera gånger.

Certifikat från testbädden kan inte användas i Skatteförvaltningens, inkomstregistrets eller det positiva kreditupplysningsregistrets gränssnitt.

7.1 Testmaterial

Testbädden har en stående certifikatbeställning samt två förberedda certifikat för ”Certifikatbegäran” och ”Förnyelse av certifikatet ”. Detta avsnitt innehåller anvisningar för användningen av testbädden. Användaren behöver även testnycklarna som publicerats för testningen (PKI privat nyckel).

Dessa testnycklar har publicerats som zip-paket: https://vero.fi/globalassets/tietoa-verohallinnosta/ohjelmistokehittajille/varmennepalvelu/varmennepalvelu-testipenkki.zip

Zip-paketet innehåller följande filer:

- SignNewCertificate_Private.key
  - Denna privata nyckel är avsedd för skapande av en signaturbegäran för ett nytt certifikat (CSR, signNewCertificate) och en XML-signatur för SOAP-meddelandet för förnyelsen av certifikatet (renewCertificate).
- RenewCertificate_Private.key
  - Denna privata nyckel är avsedd för skapande av en signaturbegäran för certifikatet (CSR) i samband med förnyelse av certifikatet (renewCertificate).

Testcertifikaten relaterade till testnycklarna förnyades i juli 2020 och gäller till juli 2030. Samtidigt byttes RetrievalId-identifierarna som behövs vid hämtningen av testcertifikaten. De nya identifierarna räknas upp i detta dokument.

7.1.1 Parametrar som används i testbäddens tjänster

I testbäddens Web Service-tjänster ska de på förhand definierade uppgifter som listas nedan **användas**.

1. Sändning av en signaturbegäran för ett nytt certifikat (signNewCertificate)

- Environment: TEST
- CustomerId: 0123456-7
- CustomerName: Ab PKI Developer Company Oy
- TransferId: 12345678903
- TransferPassword: Pw8a1d4u3HhOqhlo
- CertificateRequest: <en Base64-kodad teckensekvens i PKCS#10-format>

Skapandet av uppgiften CertificateRequest (CSR) ska ske med nyckeln 'SignNewCertificate_Private.key'. Då är det möjligt att förknippa det certifikat som tjänsten returnerar till samma privata nyckel. Man kan skapa CSR även med en nyckel som man själv har skapat, men då kan det returnerade certifikatet inte förknippas med användarens nyckel.

2. Sändning av en signaturbegäran för förnyelse av ett giltigt certifikat (renewCertificate)

- Environment: TEST
- CustomerId: 0123456-7
- CustomerName: Ab PKI Developer Company Oy
- CertificateRequest: <en Base64-kodad teckensekvens i PKCS#10-format>
- Signature: <element som motsvarar XML Signature>

Skapandet av uppgiften CertificateRequest (CSR) ska ske med nyckeln 'RenewCertificate_Private.key'. Då är det möjligt att förknippa det certifikat som tjänsten returnerar till den privata nyckel som används i detta sammanhang. Också i detta fall är det möjligt att skapa CSR med en nyckel som man själv har skapat, men då kan den inte förknippas med användarens nyckel.

Elementet Signature ska skapas med nyckeln 'SignNewCertificate_Private.key'. Ett certifikat som returnerats från certifikattjänstens testbädd med hämtningsnyckeln (RetrievalId) 990639930742461205 ska fogas till Signature-elementets uppgift X509Certificate (se punkt 3. Hämtning av certifikat).

3. Hämtning av certifikat (getCertificate)

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

- RetrievalId: <Svar till begäran om ett nytt certifikat>

Två förberedda certifikat kan hämtas genom hämtning av certifikat. Vid hämtning av ett certifikat som ”skapats” med den privata nyckel som använts vid testbäddens operation signNewCertificate ska hämtningskoden (RetrievalId) 990639930742461205 användas. Vill man hämta ett certifikat som förknippas med en privat nyckel som använts vid operationen renewCertificate, ska hämtningskoden 11885819811430372306 användas.

Testbädden har inget certifikat för förnyelse av ett förnyat certifikat (dvs. ett certifikat från operationen renewCertificate), utan testbädden returnerar alltid samma förberedda certifikat som respons till ”Förnyelse av ett giltigt certifikat”.

7.2 Testbäddens kontaktadress

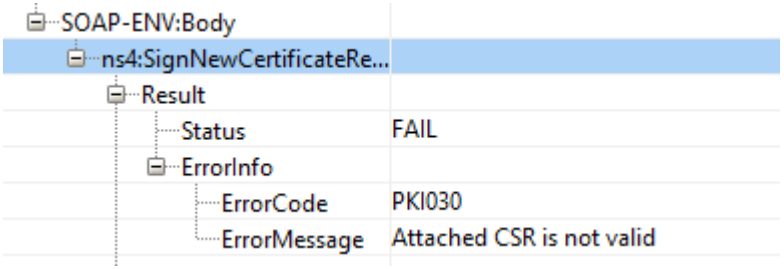
Certifikattjänstens testbädd finns i certifikattjänstens testmiljö. Testbäddens adress avviker från adressen till den egentliga testmiljön på /DEV-sekvensen av tjänstens kontext. Hela adressen är: https://pkiws-testi.vero.fi/DEV/2017/10/CertificateServices

Obs! Adressen öppnas inte i webbläsaren, utan används för gränssnittens testprogramvara såsom SoapUI eller Curl.

7.3 Felsituationer hos testbäddens tjänster

Testbäddens felhantering motsvarar på grund av dess begränsade certifikat och deras livscykel inte helt produktionen. De vanligaste felsituationerna presenteras i detta kapitel. En heltäckande lista över felkoderna finns i avsnitt 6.

Felaktig CSR i begäran om ett nytt certifikat: felkoden PKI030, Attached CSR is not valid, returneras.



Felaktig TransferId i begäran om ett nytt certifikat: felkoden PKI020, Invalid Credentials, returneras.

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

Felaktig RetrievalId vid hämtning av certifikatet: felkoden PKI099, Generic Technical Error, returneras.

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

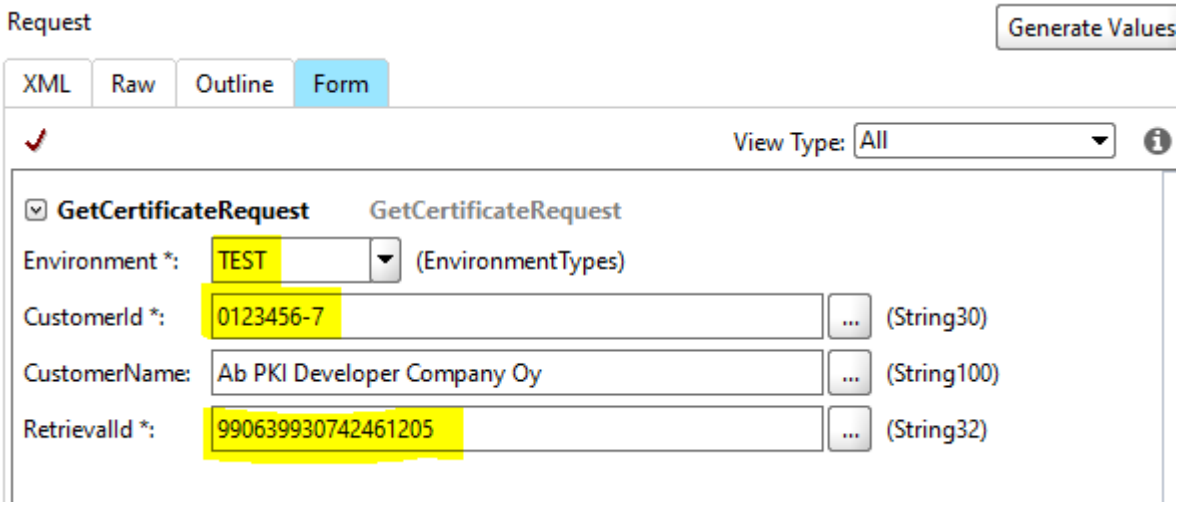
Felaktig signatur för förnyelse av ett certifikat: felkoden PKI010, Signature verification failed, returneras.

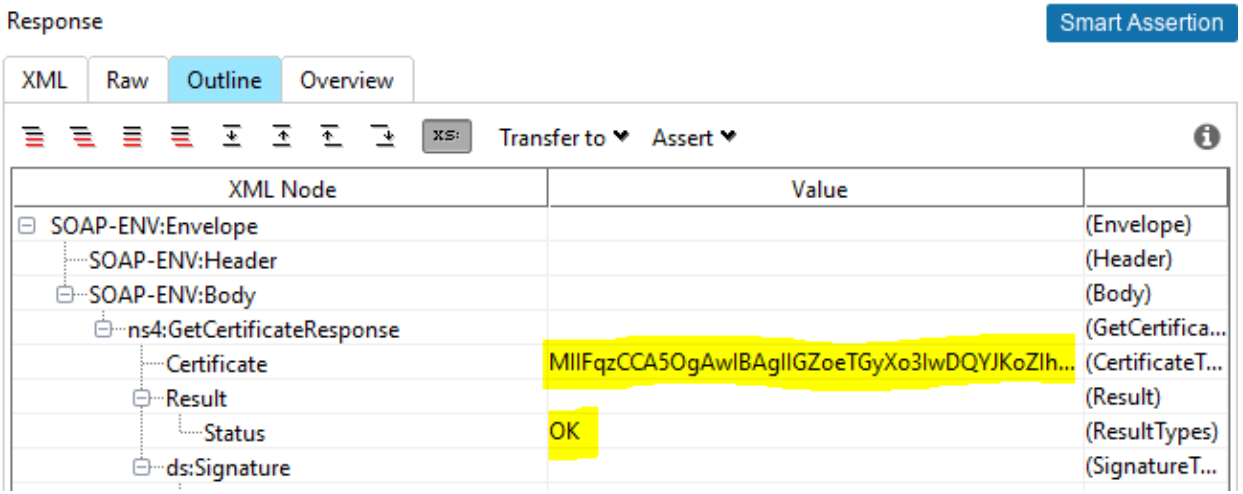
SOAP-ENV:Body	
ns3:RenewCertificateResponse	
Result	
Status	FAIL
ErrorInfo	
ErrorCode	PKI010
ErrorMessage	Signature verification failed

8 EXEMPEL PÅ MEDDELANDEN

I följande exempel har man använt programmet SmartBear Software ReadyAPI.

8.1 Hämtning av certifikat (getCertificate)





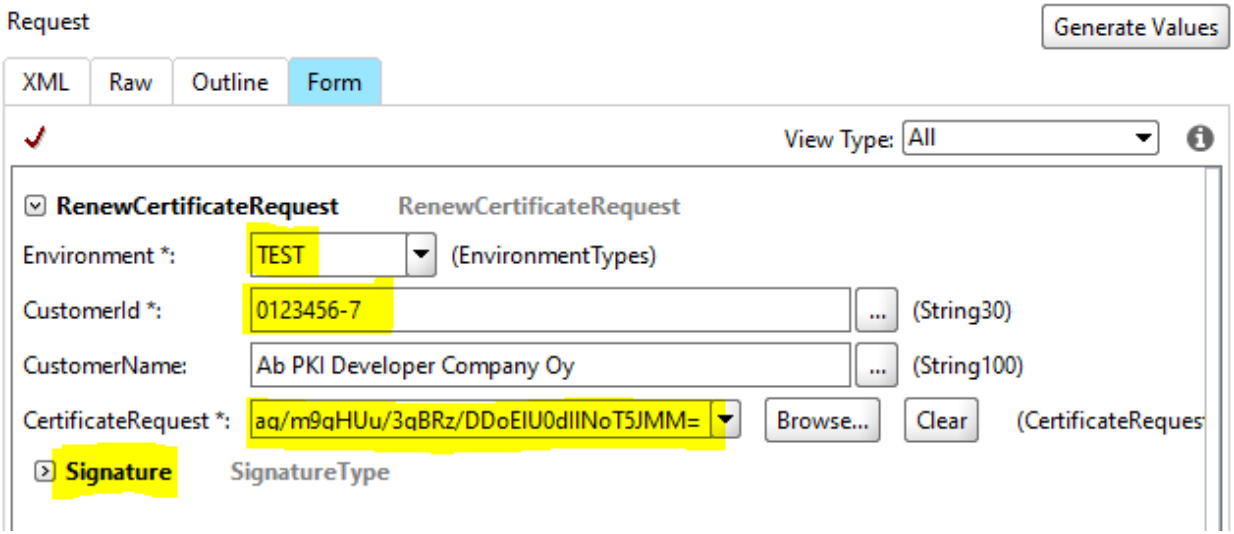
Om kunden sparar det certifikat som returnerats som respons till filen, kan hen bli tvungen att lägga till identifierare (BEGIN och END) på certifikatet:

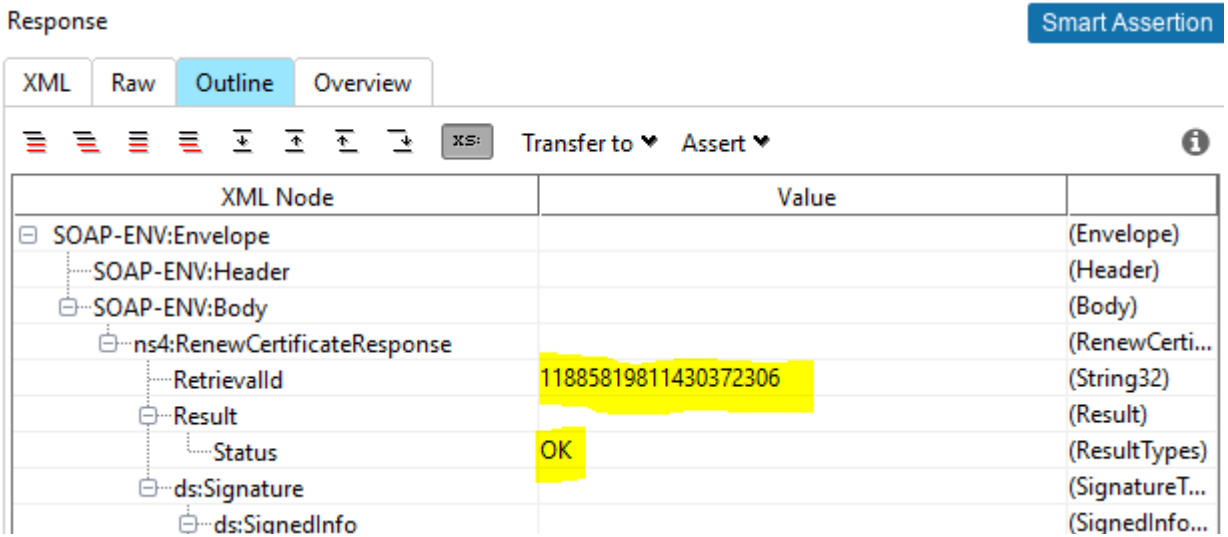
-----BEGIN CERTIFICATE-----
…. base64-kodat certifikat…
-----END CERTIFICATE-----

Vissa program och operativsystem kräver identifierare för att kunna öppna certifikatet.

8.2 Förnyande av ett certifikat (renewCertificate)

Om programmet med vilket en signaturbegäran för certifikatet (CertificateRequest) har skapats lägger till identifierare (BEGIN och END) på CSR-filen, **ska användaren radera dem**. Endast den base64-kodade sekvensen sänds:
-----BEGIN CERTIFICATE REQUEST-----
…. base64-kodad signaturbegäran för certifikat ….
-----END CERTIFICATE REQUEST-----





I XML-format ser meddelandet ut så här:

<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:cer="http://certificates.vero.fi/2017/10/certificateservices"
xmlns:xd="http://www.w3.org/2000/09/xmldsig#">
<soapenv:Header/>
<soapenv:Body>
<cer:RenewCertificateRequest>
<Environment>TEST</Environment>
<CustomerId>0123456-7</CustomerId>
<CustomerName>Ab PKI Developer Company Oy</CustomerName>
<CertificateRequest>MIICUjCCf.....kEwVXN30KnChlGw2fI79uB5W0HvyQdY69Y6uqbf6P3SGe7g==</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/xmlenc#sha256"/><DigestValue>/R8PqacpnI39cWR3Yzrszu4gDzR3Jv6FjXo8gP95viM=</DigestValue></Reference></SignedInfo><SignatureValue>nlW0x+q5IEIDtoD5z0MXS60ThEtSWChv7FGFssq6Y8J0K86CazBltZleGG28r7C0OT4rFIIM3bbk
eP3wfgHXpA74cS6UWl0Bv132/HmrgE4kEGZ4Hk8B0SaFcMeyF5UY23dHor+V+VJ7OeuSgosMyJAt

WUD2GERpWFsB+L6zuj5poihoW0yGW88dxi+J3I9VekbyPXErFbWtw5VaJaiL+s6rX22puGevM/Ah
8VL7+eiOgzhjF87p01Yh+WpodMSHvPA5IprrCE1gUxlgKpMl7iWSs0GiogpoqU5g6TxW/SZYZySm
aD0OSL38aPa/Nz/xC2naianFWe/SDhTI5/wE9Q==</SignatureValue><KeyInfo><KeyValue><RSAKeyValue><Modulus>yt/5ZTHae5gE54bc/GrMh4yYxVHCWqYFMf+N
1bQCZFnfhy6H4Oj9PpTSaqD0biVWyPxZozx+aHu1
0JDfFwI+eqlCuR4a5ZBXiciGiTviQOdBvXYWs4oKwsg4w40dLb70TwcrBLyCIVfMo/xRSckrw+am
0lCj4TqOUTL6/NKwei5/RQwKCn0y6031GUC2OpLqXIe2qnwEufaF0QzWysioJcFGKCQAfnDWapsF
KJWSCwJpgn4jkBjbTVlNSVvXfxJj9tiT2B8tLVpjWAQX7rrsGbKzRomTglEse6Myp+QS4et9FajW
mzvf0f7xQ+qRGYl83JsYVQ+gkTBx8YiRd1gY9Q==</Modulus><Exponent>AQAB</Exponent></RSAKeyValue></KeyValue><X509Data><X509SubjectName>C=FI,
O=Ab PKI Developer Company Oy, SERIALNUMBER=C46819107B4015B41B31041111A4DA6D, CN=0123456-7
</X509SubjectName><X509Certificate>MIIFqzCCA5OgAwIBAgIIPNOqyfq5YUgwDQYJKoZIhvcNAQELBQAwSjEkMCIGA1UEAwwbUEtJIFNl
cnZpY2UgRGV2ZWxvcGVyIENBIHYxMRUwEwYDVQQKDAxWZXJvaGFsbGludG8xCzAJBgNVBAYTAkZJ
MB4XDTE4MDQxNjEzMjA0M1oXDTIwMDQxNTEzMjA0M1owcjESMBAGA1UEAwwJMDEyMzQ1Ni03MSkw
JwYDVQQFEyBDNDY4MTkxMDdCNDAxNUI0MUIzMTA0MTExMUE0REE2RDEkMCIGA1UECgwbQWIgUEtJ
IERldmVsb3BlciBDb21wYW55IE95MQswCQYDVQQGEwJGSTCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAMrf+WUx2nuYBOeG3PxqzIeMmMVRwlqmBTH/jdW0AmRZ34cuh+Do/T6U0mqg9G4l
Vsj8WaM8fmh7tdCQ3xcCPnqpQrkeGuWQV4nIhok74kDnQb12FrOKCsLIOMONHS2+9E8HKwS8giFX
zKP8UUnJK8PmptJQo+E6jlEy+vzSsHouf0UMCgp9MutN9RlAtjqS6lyHtqp8BLn2hdEM1srIqCXB
RigkAH5w1mqbBSiVkgsCaYJ+I5AY201ZTUlb138SY/bYk9gfLS1aY1gEF+667Bmys0aJk4JRLHuj
MqfkEuHrfRWo1ps739H+8UPqkRmJfNybGFUPoJEwcfGIkXdYGPUCAwEAAaOCAWswggFnMAwGA1Ud
EwEB/wQCMAAwHwYDVR0jBBgwFoAUZeehBs4guH858QDh/4DceYSqbCAwUwYIKwYBBQUHAQEERzBF
MEMGCCsGAQUFBzAChjdodHRwOi8vY3JsLXRlc3RpLnZlcm8uZmkvY2EvUEtJU2VydmljZURldmVs
b3BlckNBdjEuY2VyMBMGA1UdJQQMMAoGCCsGAQUFBwMCMIGcBgNVHR8EgZQwgZEwgY6gPKA6hjho
dHRwOi8vY3JsLXRlc3RpLnZlcm8uZmkvY3JsL1BLSVNlcnZpY2VEZXZlbG9wZXJDQXYxLmNybKJO
pEwwSjEkMCIGA1UEAwwbUEtJIFNlcnZpY2UgRGV2ZWxvcGVyIENBIHYxMRUwEwYDVQQKDAxWZXJv
aGFsbGludG8xCzAJBgNVBAYTAkZJMB0GA1UdDgQWBBQwtQwXI5AZJVyZf4DEemCYLnw+mzAOBgNV
HQ8BAf8EBAMCBaAwDQYJKoZIhvcNAQELBQADggIBAEWSy5VOm5gsk7YYAesYRCB3IMAR1VTGtbKH
s+oZxUJKHl8/K2bgGMLKyYbAySxDMd/SFnxO4TXU/1IOedBYp4D9oe8eKIyBmWwG1XdpJ8W2LCvx
+CMrolcwF/5D38pMnxW5sFebTFp7v7m2ZnI5nrdDLNG1XGdF/A4M3ZJ8RymJYG8jC/F3dTao1LWx
9wAevsRwzYm2Y4+CdW/J1wN28vHXJKG6qJsMLrpeBRC27MAqgN2h9NsJnimLKCKdXHPqrW4HKNEe
uXs2bxzHLN17A45RxBpTGnDY3Y6seu4Uw/4U/1ptFyeE8cdC8Gsu++3oOWRfJv5O4mVczGtX4iEk
hgmZTJNYRDEmKqtDN7aNxKoHZ66IgU31vK6M/aiu0FTWr7tugdKVydfNy65XBixM4GCYyGtWRuwu
89ojQnrSQ3h6a4N6jtweAaui0T04UCTr0aZFL6TiGBicjMez/8w1YzAmJ3+a0/ZGL6Q/WU5jPiJf
vNldJoNqyk+IKESr01IoT5Cy+kg2Bzt5Pk+R4KdOERX8TedTxH5U/L/QfUXqGtyfl1768QxB7kaF

9T1CSuXAdR2O+JeYUkekV7WgtrbXA/Y8mZ04HZe7kglH4WJRAkdZXIhPJqS4GudEx6YKZsrC6W0T
wQ9x/30aaIdulABePI3nVEUkGOYRetjoRBOQNckW</X509Certificate></X509Data></KeyInfo></Signature></cer:RenewCertificateRequest></soapenv:Body>

9 EXEMPEL PÅ FÖRNYELSE AV CERTIFIKAT OCH SKAPANDE AV UNDERSKRIFT (CSR)

Denna anvisning beskriver ett sätt på vilket certifikat som utfärdats av Skatteförvaltningens certifikattjänst kan förnyas och signeras med hjälp av PKI-systemets Web Service-gränssnitt i Skatteförvaltningens certifikattjänst. På basis av exemplet kan man införa förnyelse av certifikat i den egna programvaran.

I anvisningen beskrivs förnyelse av testcertifikat. Anvisningen kan också tillämpas på förnyelse av produktionscertifikat. Då används genuina kunduppgifter och certifikattjänstens produktionsadress Produktionens kunduppgifter får inte användas i testmiljön.

Kompetens som behövs:

- PKI-kompetens för bildande av nyckelpar och signaturbegäran
- Programmeringskompetens, översättning och processering
- Certifikattjänstens meddelandestrukturer, WSDL-paket: https://vero.fi/globalassets/tietoa-verohallinnosta/ohjelmistokehittajille/varmennepalvelu/varmennepalvelu-rajapinta_v1.01.zip
- Nytt nyckelpar för signaturbegäran för certifikatet (CSR)
- Nuvarande certifikat och relaterad privat nyckel för signatur av xml-meddelande
- Artificiellt FO-nummer och företagsnamn för organisationens Web Service-certifikat
- Eventuell pfx-fil med det nuvarande certifikatets privata nyckel
- Lösenord för den nuvarande pfx-filen

Verktyg som behövs:

- OpenSSL: https://wiki.openssl.org/index.php/Binaries
- .NET Core 3.1 eller nyare: .NET Downloads (Linux, macOS, and Windows) (microsoft.com)
- Visual Studio Code: https://code.visualstudio.com/
- Exempel på Skatteförvaltningens signaturprogram kan laddas ner här (SignXmlNew.cs): https://www.vero.fi/globalassets/tietoa-verohallinnosta/ohjelmistokehittajille/swaggerui/verohallinto_program.zip
- SoapUI https://www.soapui.org/downloads/soapui/ eller Curl https://curl.se/download.html

Mer information:

- Anvisningar för förnyelse: Förnyande av certifikat
- Dokumentation i Skatteförvaltningens certifikattjänst i avsnittet Dokumentation
- Anvisning för certifikattjänstens testbädd (i avsnitt 7 i detta dokument 7)
- För Vero API - och ApitamoPKI-kunder finns kanalen Slack: https://vero-api.slack.com
    - Anslut dig till kanalen via API-observationsblanketten.

- Observationsblankett för Skatteförvaltningens certifikattjänst

Förnyelse av testcertifikat

1. Skapa en ny privat nyckel för nytt certifikat

Skapa en privat nyckel i programmet OpenSSL med kommandot:
openssl genrsa -out newprivate.key 2048

En ny skapad privat nyckel sparas i filen newprivate.key

2. Skapa signaturbegäran för certifikat för förnyelse

Bilda signaturbegäran för certifikatet (CSR) genom att använda den privata nyckel som skapats enligt punkt till exempel i programmet OpenSSL med kommandot:
openssl req -new -key newprivate.key -out certificaterequest.csr

Ange följande uppgifter i OpenSSL enligt uppgifterna om det certifikat som ska förnyas:
Country Name = *FI*
Organization Name = *Testföretagets namn*
Common Name = *artificiellt FO-nummer*

Signaturbegäran för det nya certifikatet sparas i filen certificaterequest.csr

3. Bilda xml-meddelande för signatur

Bilda innehållet i xml-meddelandet för förnyelse av certifikatet för gränssnittet för förnyelse. **Endast denna del av meddelandet signeras**. Använd bifogade template, observera att editorn kan lägga till radbyten. Vi **rekommenderar** att dessa radbyten tas bort innan signaturen bildas:

<cer:RenewCertificateRequest xmlns:cer="http://certificates.vero.fi/2017/10/certificateservices" xmlns:xd="http://www.w3.org/2000/09/xmldsig#">
<Environment>TEST</Environment>
<CustomerId>*Artificiellt FO-nummer*</CustomerId>
<CustomerName>*Testföretagets namn*</CustomerName>
<CertificateRequest>*Signaturbegäran för certifikatet som bildats enligt punkt 2 dvs. csr-filens base64 teckensekvens utan rubrikerna --- begin certificate request -- och --- end certificate request* --- </CertificateRequest>

</cer:RenewCertificateRequest>

Fyll testcertifikatets FO-nummer (artificiellt FO-nummer), artificiellt företagsnamn och ny signaturbegäran för certifikatet som skapats enligt punkt 2 (base 64 teckensekvens utan rubrikerna "--- begin certificate request---" i fälten i exempelmeddelandet). Spara xml-filen utan radbyten på disken för signatur.

4. Underteckna xml-meddelande

Bilda signatur för meddelandets innehåll, dvs. den del som bildats enligt punkt 3. Du kan använda färdiglösningar såsom programmet XML Signer eller Skatteförvaltningens exempellösning. Denna anvisning utgår från Skatteförvaltningens C#-lösning. Exemplet antar att det nuvarande certifikatet finns i en pfx-fil.

Ladda ner exempellösningen på signaturprogrammet på sidan Dokumentation eller i början av avsnitt 9.

För att köra programmet ska du ladda ner biblioteken .net core 3.1 och en lämplig utvecklingsmiljö, till exempel Visual Studio Code: https://code.visualstudio.com/

4.1 Skapa en pfx-fil för signaturprogrammet med Open SSL

En ny pfx-fil behöver inte skapas om du redan har en sådan för Vero API. Gå då direkt till steg 4.2.

Använd det här kommandot för att skapa en pfx-fil. I filen laddas det nuvarande certifikatet och den privata nyckel med vilken det skapats.

Om pfx-fil saknas ska du skapa en med följande kommando, varvid den förses med en privat nyckel och det nuvarande certifikatet (som sparats i cert.cer-filen i base64-format):
openssl.exe pkcs12 -export -out test.pfx -inkey private.key -in cert.cer

I dag finns den privata nyckeln för certifikatet i den okrypterade filen private.key i base64-format medan certifikatets offentliga del (= signerad offentlig nyckel) finns i filen cert.cer i base64-format.

OpenSSL ber om lösenord med vilket pfx-filen krypteras. Lösenord krävs i signaturprogrammet. Slutresultatet är en ny test.pfx-fil.

Om du använder testbädden:
Skapa pfx-filen med ovan nämnda kommando, varvid den förses med en privat nyckel, testbäddens SignNewCertificate_Private.key-fil och det nuvarande certifikatet som hämtats från testbädden och som sparats i cert.cer-filen i base64-format.

4.2 Kör signaturprogrammet

Kör signaturprogrammet (SignXmlNew.exe) och ange som kommandoradparameter xml-fil som ska signeras och som du skapat enligt punkt 3 samt pfx-fil och lösenordet för den:
SignXmlNew.exe renew.xml test.pfx password

Slutresultatet är den signerade xml-filen renew_signed.xml, nedan exempel på testbädden:

<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>MIICjTCCAXUCAQAwSDELMAkGA1UEBhMCRkkxEzARBgNVBAgMClNvbWUtU3RhdGUx
JDAiBgNVBAoMG0FiIFBLSSBEZXZlbG9wZXIgQ29tcGFueSBPeTCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBAJkBP88eLdbxbJfPluDI/rNP0EUpluRohxgx
MNfuYVV9kXgrMsOZpCsV/QjwZFpWBSFy6PDJIKyvAqe83XSfoGPt9apy3QaUJuXR
4/P5H6VT+eZpt1TCf5CEaKb0aW4bZ1kN9BLerrJ81HsR6cutpE/t0bzArc4kna/l
rz/yB3tlU34YoHyx9bXNwKSPsUdL7N32vIuSO8Me/3NjFzA9CBYRrP58qnXIyTmm
0x5GJXGBJqJM2xBRCmpMWg5WGUOF8mAGxkPDxyEfZpaHXbSLaBQ1nJyDPg0+n/Ak
rcweydE0BKmMh3rSITH/M5DYZ6yKgHABEWERg1Nz06ei+a+KJUcCAwEAAaAAMA0G
CSqGSIb3DQEBCwUAA4IBAQBsIqCulgyrfU+DVZxS60Hvu4d8GcKKRGCtFBt508BM
c+NSnevgakWZXXMWKOJStsDHsOPnwfaIvlmFLWRkAsqxt2dIGgWMzFh9NaX0Anwm
CbiUruot9C8zguP7Y/67AFSeageNYrHmgIBHoZyNIe+tPR4Y5DxcQBl/6HtyzJ/q
Nej5mp2zSlW5P1QoEkS3MU8Gm0mpCBylyAvCzeYHOop6caZMQctVCmPto+0PYx0T
qEmO15vGj/rIN4btjEKSYfjNj56MMN8lsIc/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/xmlenc#sha256"
/><DigestValue>i13a6CV9yr+uqy/qx4yhvyysDvcKnoiNIjUdj7Arr1A=</DigestValue></Reference></SignedInfo><SignatureValue>VEja46Y17IaMXHMJfcZMRM+3zPTL
Sepv/zWeR2JLMMCz3nWldJynhs1MjGMbqJ3gLsebomkE3UX10ToZ0LObtbeACFYz78dDKbWHTc4cU1IWkZU3DpXQ5svgJWNk1L+B2SDH7V+ethFNqBmwLCgsE2dT8p
t7rXwsBOnZe/Rt30flEMd5sSWYYJeb1FzMXAcafVIoVs31T9HcoCFupgMH9YWsgzpknQHTSTKfjBZbhsjBnvnDIwSceFhxxNpcmY/zVjRVB56WeC2qhQgZFN7PsnCJ6KnNO
TkYr2w7CVCFNwofCMU3eXUl+n5khTJmNQV+SZ2S0qPzBSp6TD/reCVJHA==</SignatureValue><KeyInfo><X509Data><X509Certificate>MIIFqzCCA5OgAwIBAgIIGZoe
TGyXo3IwDQYJKoZIhvcNAQELBQAwSjEkMCIGA1UEAwwbUEtJIFNlcnZpY2UgRGV2ZWxvcGVyIENBIHYxMRUwEwYDVQQKDAxWZXJvaGFsbGludG8xCzAJBgNVBAYTAk

ZJMB4XDTIwMDcwNjA4MzYzMloXDTMwMDcwNDA4MzYzMlowcjESMBAGA1UEAwwJMDEyMzQ1Ni03MSkwJwYDVQQFEyBDNDY4MTkxMDdCNDAxNUI0MUIzMTA
0MTExMUE0REE2RDEkMCIGA1UECgwbQWIgUEtJIERldmVsb3BlciBDb21wYW55IE95MQswCQYDVQQGEwJGSTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggE
BAMrf+WUx2nuYBOeG3PxqzIeMmMVRwlqmBTH/jdW0AmRZ34cuh+Do/T6U0mqg9G4lVsj8WaM8fmh7tdCQ3xcCPnqpQrkeGuWQV4nIhok74kDnQb12FrOKCsLIOM
ONHS2+9E8HKwS8giFXzKP8UUnJK8PmptJQo+E6jlEy+vzSsHouf0UMCgp9MutN9RlAtjqS6lyHtqp8BLn2hdEM1srIqCXBRigkAH5w1mqbBSiVkgsCaYJ+I5AY201ZTUlb138
SY/bYk9gfLS1aY1gEF+667Bmys0aJk4JRLHujMqfkEuHrfRWo1ps739H+8UPqkRmJfNybGFUPoJEwcfGIkXdYGPUCAwEAAaOCAWswggFnMAwGA1UdEwEB/wQCMAAw
HwYDVR0jBBgwFoAUT1PJe8BCr9h+uQE8W6CNC7/QfeYwUwYIKwYBBQUHAQEERzBFMEMGCCsGAQUFBzAChjdodHRwOi8vY3JsLXRlc3RpLnZlcm8uZmkvY2EvUEtJU2
VydmljZURldmVsb3BlckNBdjEuY3J0MBMGA1UdJQQMMAoGCCsGAQUFBwMCMIGcBgNVHR8EgZQwgZEwgY6gPKA6hjhodHRwOi8vY3JsLXRlc3RpLnZlcm8uZmkvY3Js
L1BLSVNlcnZpY2VEZXZlbG9wZXJDQXYxLmNybKJOpEwwSjEkMCIGA1UEAwwbUEtJIFNlcnZpY2UgRGV2ZWxvcGVyIENBIHYxMRUwEwYDVQQKDAxWZXJvaGFsbGludG
8xCzAJBgNVBAYTAkZJMB0GA1UdDgQWBBQwtQwXI5AZJVyZf4DEemCYLnw+mzAOBgNVHQ8BAf8EBAMCBaAwDQYJKoZIhvcNAQELBQADggIBADZkkj4T+rVlAe9a53/
9zrWLuJqe+WePxIoEk5ozXWDb2FeR0uEyUS2Ba0gVJwPm9Go6CAia3J9nFGyVUUNCm2ofdDGxEX4JkrRc7cO8JPaMY74tJR9wwj8R5sshAXPDVMWh9Ml8LHG6hqz0ic
0lK9cSsAHBGJ3GBlckS/6y+SPWGKMHOf0QIm5of63qQ8aI950y4aUjL7td2Yxiu6jKUfP4haL0BvJFM///o6Ge5LxT3nfPZxESBLbLE21D0ksyO+fZIjIeflxIeQk9rWY7zYq/Go9
+EIvElLXE2aDjqQrwoNIQHmqLgG0DuKpJKzSi7nRvDVHaB5YIdtLDJ4PXZlTkib8QBOZWmHCw58IvfEdL0WfuRpzJmlCf8oyzLWRagtnEQhwnWnkXOtPqivRq3Rh35M4mQ
PNVPikduzYlhvQzwCAVkzgspEZVT5hQlTEXBiZZQ8jC8Mb6U1u7G/NndHGwdWn0WtNYDMrhqEZGoHxgLTLwaU4d5suHzkv0gIxkreR4fnVdiVWd4zCNQk6rt9Jo3p0yLF
GM49G3kszHPcYxxBmzqSrSBoBKX5Sn9+jOF39fxE6LNCmJBiZz49WhSOTSLjX/kL8B0T4NBCtz6EdhQk0lz1JC5GvNuVVnmKeZYElt3qLvx4ktc6QxlH2zZ48BR+m/cXycvyLz
y2fgyAlW</X509Certificate></X509Data></KeyInfo></Signature></cer:RenewCertificateRequest>

Observera att signaturprogrammet har lagt till blocket Signature i slutet av blocket RenewCertificateRequest.

Det är viktigt att se till att innehållet i filen inte förändras på något sätt innan den skickas till PKI-systemets gränssnitt. Förändringar orsakas också av radbyten och andra formateringar, vilket leder till att signaturen inte längre är valid och att certifikattjänsten meddelar felkoden PKI010.

5. Skicka det signerade meddelandet till PKI-systemets gränssnitt i certifikattjänsten

Skicka det signerade meddelandet om förnyelse av certifikat till exempel med programmet SoapUI till PKI-systemets testadress:
https://pkiws-testi.vero.fi/2017/10/CertificateServices

Du kan ladda ner mallar för meddelandestrukturer i SoapUI på basis av WSDL-beskrivningar. Ladda ner certifikattjänstens gränssnittspaket på sidan Dokumentation eller i början av avsnitt 9. Öppna WSDL-filen med SoapUI.

Skapa meddelandet så att det oförändrade signerade innehållet finns i elementet soap-envelope. Formatera inte det signerade innehållet på något sätt.

Exempel på soap-envelope och ställe dit innehållet exporteras:
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xs="http://www.w3.org/2001/XMLSchema" ><env:Body>
här det signerade innehållet som sådant och som bildats enligt punkt 4 i anvisningen

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

Kontrollera URL och skicka meddelandet. I svarsmeddelandet följer OK och retrievalID, med vilket certifikatet kan hämtas med kommandot GetCertificate.

I stället för SoapUI kan man använda programmet CURL, men då ska man till exempel i en Windows-miljö se till att det inte finns radbyten i innehållet som signeras utan allt innehåll ska stå på en rad. Kom ihåg att foga soap-envelope till den signerade filen. Med följande CURL-kommando kan du skicka begäran om förnyande:
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. Hämta det förnyade certifikatet med kommandot GetCertificate

Ta del av certifikattjänstens anvisningar när du hämtar certifikat.

Spara pfx-filen och den privata nyckeln omsorgsfullt.

10 SKAPA SIGNATUR (CSR) MED WINDOWS MMC-VERKTYG

Om du inte har tillgång till programmet OpenSSL, kan du i en Windows-miljö skapa CSR med MMC-verktyget (Microsoft Management Console). Detaljerade anvisningar för tillvägagångssättet finns till exempel på

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