Version 1.03

Certifikattjänsten – Beskrivning av gränssnittet

Inkomstregisterenheten

Versionshistoria

Version	Datum	Beskrivning
1.0	30.10.2017	Dokumentet har publicerats.
1.01	15.12.2017	Följande punkter i dokumentet har uppdaterats: 1.1, 1.2, 2.1, 2.2, 3.1, 3.2, 3.3, 3.7 och 4. Punkt 2.21.2 har tagits bort.
1.02	15.10.2018	Avsnitt 1.2: Schemats url har uppdaterats.
1.03	10.4.2019	Följande punkter i dokumentet har uppdatertas 2, 3.1, 3.3, 3.5 och 4.

INNEHÅLL

1 ALLMÄNT

Dokumentet innehåller en beskrivning av hur gränssnittet Web Service i certifikattjänsten har byggts upp med tanke på den som genomför systemintegreringen. Dokumentet innehåller en beskrivning av tjänsterna i gränssnittet samt datainnehållet i tjänsterna (XML-scheman).

Dokumentet innehåller en beskrivning av den tekniska uppbyggnaden av gränssnittet för certifikattjänsten på den detaljnivå som krävs för att parterna utifrån beskrivningen kan fastställa och bygga upp sitt eget system tillsammans med integrationens certifikattjänst.

1.1 Gränssnittet Web Service

Tjänsterna i gränssnittet för certifikattjänsten har definierats i beskrivningen **CertificateServices.wsdl**.

I beskrivningen används följande namnrymder:

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

1.2 Schema

För hanteringen av livscykeln för certifikaten som beviljats i certifikattjänsten 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/2001/XMLSchema
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.

1.3 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

1.4 Läsanvisning för dokument

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

2 WEB SERVICE-GRÄNSSNITTET FÖR CERTIFIKATTJÄNSTEN

Dokumentet Certifikattjänsten – Allmän beskrivning innehåller en beskrivning av användningen av certifikattjänstens Web Service-tjänster och kopplingarna mellan tjänsterna.

I följande tabell beskrivs tjänsterna i gränssnittet:

Operation	Meddelande om begäran	Svarsmeddelande	Beskrivning
Begäran om ett nytt certifikat (SignNewCertificate)	SignNewCertificateRequestMessage	SignNewCertificateResponseMessage	Begäran om ett nytt certifikat när • användaren begär ett certifikat första gången • användaren redan har ett/flera gällande certifikat, men behöver flera certifikat • användarens tidigare certifikat inte längre är i kraft eller har revokerats, dvs. tagits ur användning.
Förnyande av ett gällande 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. Minst en 10 sekunders fördröjning ska finnas mellan certifikatbegäran eller svarsmeddelandet av ett förnyat certifikat och meddelande om begäran av hämtning av certifikatet.

Kapitel 3 innehåller en närmare beskrivning av datainnehållet i meddelanden med begäranden och svar i tjänsterna för gränssnittet.

2.1 Signering av meddelanden

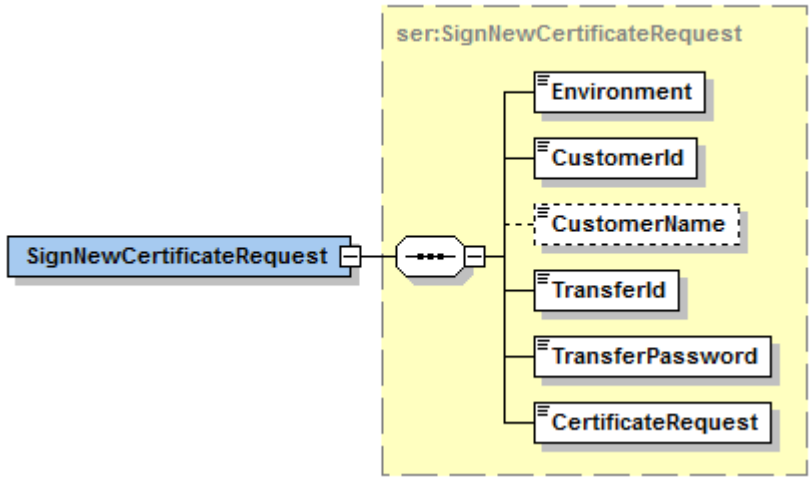
I tjänsterna för gränssnittet Web Service i certifikattjänsten används elektronisk signatur (XML Signature). Med denna verifieras vem som har skapat datainnehållet i meddelandet i de meddelanden som definieras i kapitel 3. Signaturen är också en garanti för att meddelandet inte har ändrats. Signaturen 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/). Metoderna för att skapa en signatur och preciseringar av dessa (till exempel algoritmer och standardiseringsmetoder) kommer att publiceras senare i samband med skapandet av inkomstregistrets XML-signatur.

2.2 Behandling av fel i Web Service-tjänsterna

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. Felkoderna och deras förklaringar preciseras i kapitel 4.

3 DATAINNEHÅLLET I GRÄNSSNITTETS TJÄNSTER

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

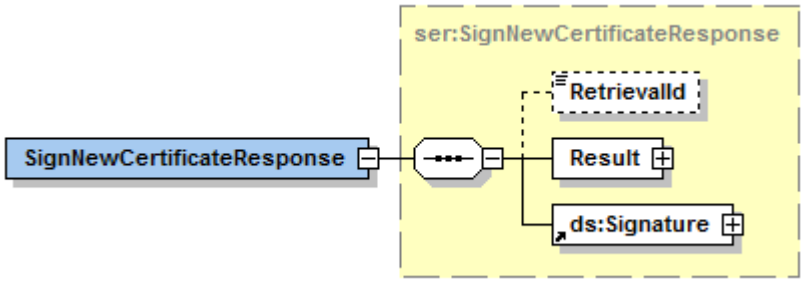


Uppgifter om datagruppen *SignNewCertificateRequest*:

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 som används i kommunikationen med inkomstregistret. Identifieraren kan vara till exempel ett FO-nummer. Om FO-nummer används

				ska identifieraren finnas i Företags- och organisationsdatasystemet (FODS) och identifieraren ska innehålla ett mellansträck.
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.
Certifikatbegäran (CertificateRequest)	ser:CertificateRequestType		1:1	Kundens certifikatbegäran. En certifikatbegäran är en Base64-kodad teckensekvens i PKCS#10-format.

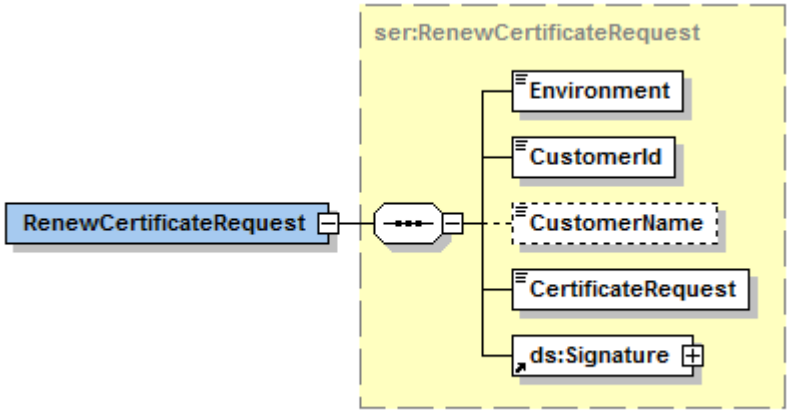
3.2 Begäran om ett nytt certifikat – svarsmeddelande (SignNewCertificateRequest)



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 certifikattjänsten bildar med sitt eget certifikat.

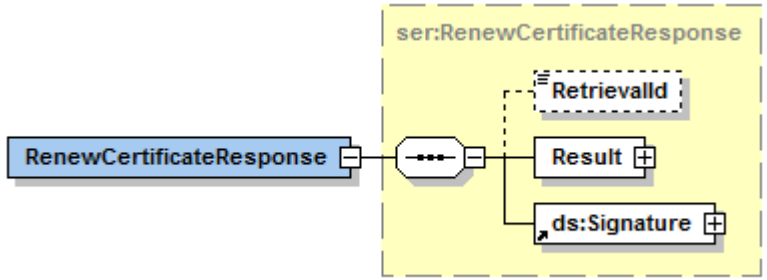
3.3 Förnyande av ett gällande certifikat – meddelande om begäran (RenewCertificateRequest)



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 som används i kommunikationen med inkomstregistret. Identifieraren kan vara till exempel ett FO-nummer. Om FO-nummer används ska identifieraren finnas i Företags- och organisationsdatasystemet (FODS) och identifieraren ska innehålla ett mellansträck.
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.
Certifikatbegäran (CertificateRequest)	ser:CertificateRequestType		1:1	Kundens certifikatbegäran. En certifikatbegäran 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.

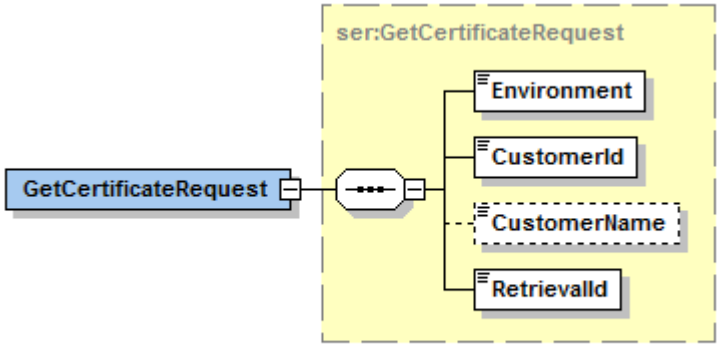
3.4 Förnyande av ett gällande certifikat – svarsmeddelande (RenewCertificateResponse)



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 certifikattjänsten bildar med sitt eget certifikat.

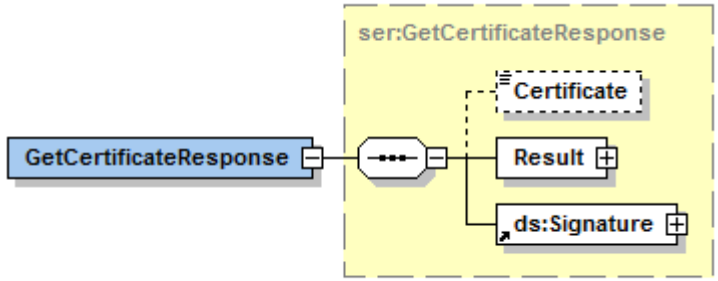
3.5 Hämtning av ett certifikat – meddelande om begäran (GetCertificateRequest)



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 som används i kommunikationen med inkomstregistret. Identifieraren kan vara till exempel ett FO-nummer. Om FO-nummer används ska identifieraren finnas i Företags- och organisationsdatasystemet (FODS) och identifieraren ska innehålla ett mellansträck.
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 certifikattjänsten returnerar på meddelanden om begäran om ett certifikat eller meddelanden för förnyande av ett certifikat.

3.6 Hämtning av ett certifikat – svarsmeddelande (GetCertificateResponse)

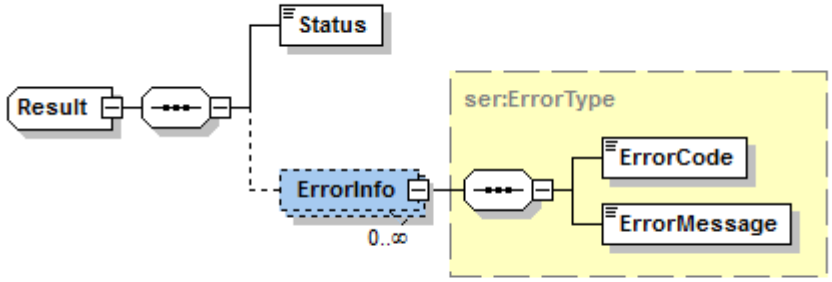


Uppgifter om datagruppen *GetCertificateResponse*:

Uppgiftens namn	Typ	Tillåtna värden	Elementets obligatoriskhet (minOccurs: maxOccurs)	Förklaring till uppgiften
Kundens certifikat (Certificate)	ser:CertificateType		0:1	Kundens certifikat som undertecknats av certifikattjänsten. 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 certifikattjänsten bildar med sitt eget certifikat.

3.7 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 preciseras i kapitel 4.

4 FELKODER OCH DERAS FÖRKLARINGAR

Begäran om ett nytt certifikat – felsituationer som eventuellt returneras med ett svarsmeddelande:

Felkod	Felkodens förklaring	Beskrivning
PKI005	Wrong environment type specified	Värdet för miljön (Environment) av parametern av meddelande om begäran motsvarar inte det värde som definierats i målsystemet. Efter korrigering av parametervärdet kan man prova funktionen på nytt.
PKI020	Invalid credentials	Någon av de angivna identifierarna, kundens identifierare (CustomerID), överföringskod (TransferId) eller engångslösenord (TransferPassword) är felaktig. Efter kontrollering och korrigering av de angivna parametrarna måste en ny certifikatbegäran göras.
PKI030	Attached CSR is not valid	Certifikatbegäran (CSR) i meddelandet om begäran är felaktig. Efter att en ny certifikatbegäran har skapats kan man prova funktionen på nytt.
PKI099	Generic Technical Error	Felsituation utan en separat fastställd felkod. Formen av och uppgifterna i det felaktiga anropet ska kontrolleras. Om felet upprepas, kontakta inkomstregistret.

Förnyelse av ett befintligt certifikat – felsituationer som eventuellt returneras med ett svarsmeddelande:

Felkod	Felkodens förklaring	Beskrivning
PKI005	Wrong environment type specified	Värdet för miljön (Environment) av parametern av meddelande om begäran motsvarar inte det värde som definierats i målsystemet. Efter korrigering av parametervärdet kan man prova funktionen på nytt.
PKI010	Signature verification failed	Kontrollen av signaturen för innehållet i meddelandet Förnyelse av certifikatet misslyckades. Meddelandet ska skrivas under med det certifikat som man vill förnya. Anropet kan skickas på nytt efter att den eventuellt felaktiga signaturen har korrigerats.
PKI015	Invalid certificate to be renewed received	Det certifikat som använts för underskrift av meddelandet om begäran är felaktigt eller saknar de uppgifter som behövs. Certifikatbegäran kan skickas på nytt, när meddelandet har skrivits under med det rätta certifikatet.
PKI030	Attached CSR is not valid	Certifikatbegäran (CSR) är felaktig. Efter att en ny certifikatbegäran har skapats kan man prova funktionen på nytt.
PKI080	Certificate renewal not yet allowed	Certifikatet kan förnyas först när dess giltighet upphör om högst 60 dygn.
PKI099	Generic Technical Error	Felsituation utan en separat fastställd felkod. Formen av och uppgifterna i det felaktiga anropet ska kontrolleras. Om felet upprepas, kontakta inkomstregistret.

Hämtning av ett certifikat – felsituationer som eventuellt returneras med ett svarsmeddelande:

Felkod	Felkodens förklaring	Beskrivning
PKI005	Wrong environment type specified	Värdet för miljön (Environment) av parametern av meddelande om begäran motsvarar inte det värde som definierats i målsystemet. Efter korrigering av parametervärdet kan man prova funktionen på nytt.
PKI020	Invalid credentials	Någon av de angivna identifierarna, kundens identifierare (CustomerID), överföringskod (TransferId) eller engångslösenord (TransferPassword) är felaktig då man begär ett nytt certifikat eller förnyar ett certifikat. Efter att identifieringsuppgifterna har kontrollerats måste den ursprungliga certifikatbegäran eller förnyandet av ett giltigt cetifikat och hämtning av certifikatet genomföras på nytt. Förnyandet av enbart certifikatbegäran returnerar det ursprungliga PKI020-felet.
PKI099	Generic Technical Error	Felsituation utan en separat fastställd felkod. Formen av och uppgifterna i det felaktiga anropet ska kontrolleras. En felsituation uppstår till exempel om certifikatet hämtas för snabbt efter begäran av certifikatet eller förnyande av meddelande om begäran. I sådana fall har certifikattjänsten inte hunnit behandla meddelandet om begäran. Om felet upprepas, kontakta inkomstregistret. Eftersom tjänsten är asynkron till sin natur, kan felet ha uppkommit redan tidigare. Man kan ha angett felaktiga uppgifter t.ex. vid begäran av ett certifikat eller vid förnyelse av certifikatet, och skapandet av certifikatet har misslyckats.