Version 1.04

Certifikattjänsten – Allmän beskrivning

Inkomstregisterenheten

Versionshistoria

Version	Datum	Beskrivning
1.0	30.10.2017	Dokumentet har publicerats.
1.01	15.12.2017	Följande punkter i dokumentet har uppdaterats: 2. Termer och förkortningar, 3.1 Begäran om ett nytt certifikat, 3.3. Certifikatens livscykel och förnyande av dessa, 3.4. Felsituationer, 4. Användning av certifikat i inkomstregistrets SFTP-kanal, 5 Testning av tjänsten. Det tidigare kapitlet 3 Behörighet för tjänsten och avtal om användningen har tagits bort.
1.02	16.10.2018	Följande punkter i dokumentet har uppdaterats: 1. Inledning, 3. Certifikattjänsten, 3.4 Certifikatens livscykel och förnyande av dessa, 4. Användning av certifikat i inkomstregistrets tekniska gränssnitt, 4.1 Web Service-kanal, 4.2 SFTP-kanal Tillägg: 3.1 Certifikattyper
1.03	10.04.2019	Följande punkter i dokumentet har uppdaterats: 3. Certifikattjänsten, 3.2 Begäran om ett nytt certifikat, 3.4 Certifikatens livscykel och förnyande av dessa, 3.5 Felsituationer, 4. Användning av certifikat av certifikat i inkomstregistrets tekniska gränssnitt, 5. Testning av tjänsten.
1.04	20.1.2020	Följande punkt i dokumentet har uppdaterats: 3.4 Certifikatens livscykel och förnyande av dessa.

INNEHÅLL

1 INLEDNING

Organisationer som använder certifikattjänsten och som lämnar in material till eller hämtar material från inkomstregistret via tekniska gränssnitt. Kanaler för inkomstregistrets tekniska gränssnitt är SFTP-kanalen och Web Service-kanalen. Ett certifikat beviljas till organisationer som svarar för att leverera uppgifter till inkomstregistret eller som har rätt att få uppgifter från inkomstregistret. Certifikaten beviljas av certifikattjänsten för inkomstregistret.

Syftet med dokumentet är att ge en allmän beskrivning av certifikattjänsten för inkomstregistret. De tekniska funktioner och scheman som används för att begära, söka och förnya ett certifikat beskrivs i det separata dokumentet Certifikattjänsten – Beskrivning av gränssnittet.

2 TERMER OCH FÖRKORTNINGAR

En förteckning över förkortningarna som används i tjänstebeskrivningen och de viktigaste termerna finns i tabell 1.

Förkortning eller term	Förklaring
CSR (Certificate Signing Request) Begäran om att underteckna ett certifikat	Begäran om certifikat som gjorts av den som använder certifikattjänsten. Begäran om certifikat är en Base64-kodad teckensekvens i PKCS#10-format.
Metoden med offentlig nyckel	Asymmetrisk kryptering där den ena krypteringsnyckeln är en offentlig nyckel och den andra en privat nyckel.
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.
Gränssnittet	En standardenlig praxis eller förbindelse som möjliggör överföring av information mellan enheter, programvara eller användare.
RSA-kryptering	Metod med offentlig nyckel som grundar sig på en krypteringsalgoritm utvecklad 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.
Informationsanvändare	Aktörer som har lagstadgad rätt att få inkomstuppgifter eller annan information från inkomstregistret för att sköta sina arbetsuppgifter. I det första skedet från och med 1.1.2019 är informationsanvändarna Skatteförvaltningen, FPA, Sysselsättningsfonden och arbetspensionsanstalterna samt PSC. I det andra skedet från och med 1.1.2020 omfattar informationsanvändarna dessutom bland annat Statistikcentralen, Sysselsättningsfonden (vuxenutbildningsförmåner), skadeförsäkringsanstalterna, arbetslöshetskassorna, ANM:s förvaltningsområde, kommunerna och arbetarskyddsmyndigheten.
Informationsproducenter	Alla företag och andra aktörer som är skyldiga att anmäla information om löner, pensioner eller förmåner i Finland för någon av inkomstregistrets informationsanvändare.
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, sökning 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 gällande certifikat.
X.509	En standard som fastställer certifikatets struktur.

Tabell 1. Förkortningar som används och de viktigaste termerna.

3 CERTIFIKATTJÄNST

Inkomstregistrets certifikattjänst grundar sig på en PKI-lösning (Public key Infrastructure). I certifikattjänsten har kunden en eller flera nyckelpar (privat och offentlig nyckel) och ett certifikat som anknyter till nyckelparet och som är i enlighet med X.509-standarden.

Kunden beställer certifikatet i inkomstregistrets certifikattjänst, som beviljar det. Certifikatet används för att identifiera kunden och underteckna material som sänds till inkomstregistret elektroniskt (XML Signature) i inkomstregistrets tekniska gränssnitt. Certifikaten beviljas för en viss kund och för ett visst användningsändamål, och kan inte användas för ett ändamål som avviker från det ursprungliga. Användaren av certifikatet ska godkänna och iaktta Skatteförvaltningens och inkomstregistrets användarvillkor för gränssnittstjänster (pdf).

Om den som använder inkomstregistrets tjänster är både producent av löne- och förmånsuppgifter och informationsanvändare, måste olika certifikat för de olika användningsändamålen beställas. Om kunden använder både SFTP- och Web Service-kanalen i det tekniska gränssnittet ska också certifikat beställas för respektive kanal. En aktör kan alltså ha flera certifikat. Om kunden använder sig av flera certifikat som är avsedda för olika användningsändamål och kanaler i till exempel samma programvara bör man fästa extra uppmärksamhet vid hanteringen av certifikaten.

3.1 Typ av certifikat

Roll	Kanal	Utgivare av certifikatet
Producent av löneuppgifter	Web Service	Data Providers Issuing CA
	SFTP	Data Providers SFTP Issuing CA
Producent av förmånsuppgifter	Web Service	IR Benefit Data Providers Issuing CA
	SFTP	IR Benefit Data Providers SFTP Issuing CA
Informationsanvändare	Web Service	IR Income Data Users Issuing CA
	SFTP	IR Income Data Users SFTP Issuing CA
Inkomstregistrets utomstående stödtjänster	Web Service	IR External Data Providers Issuing CA
	SFTP	IR External Data Providers SFTP Issuing CA

3.2 Begäran om ett nytt certifikat

På bild 1 visas hur man begär och hämtar ett nytt certifikat.

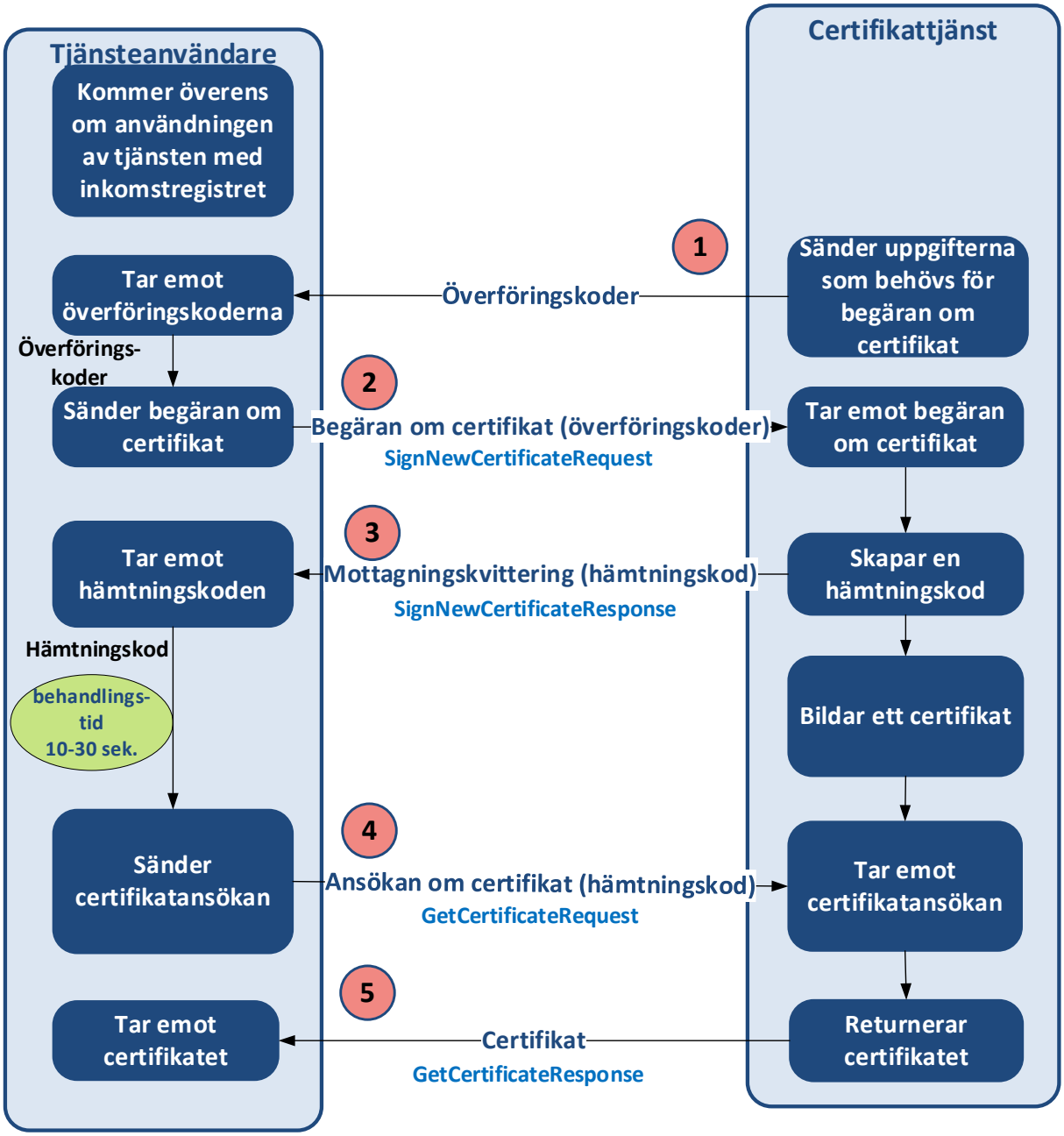

Bild 1. Begäran om och hämtning av ett nytt certifikat.

Användarrättigheterna till de tekniska gränssnitten som behövs för informationsproduktion hämtas från inkomstregistrets e-tjänst. När en organisation gör en anmälan om att införa det tekniska gränssnittet godkänner den användarvillkoren för Skatteförvaltningens och inkomstregistrets gränssnittstjänster. Ansökan startar certifikatbeställningen. Man ansöker om användarrättigheter till det tekniska gränssnittet som behövs för användning av information genom att fylla i informationsanvändarens anmälan för informationstillstånd.

Certifikattjänsten sänder uppgifterna som behövs för begäran om certifikat till kunden: en överföringskod (TransferId) och ett engångslösenord (TransferPassword). Kunden kan sända en begäran om certifikat när hen fått överföringskoden och engångslösenordet som sänts för begäran om certifikat. Engångslösenordet är giltigt i 14 dygn.

- Om certifikat inte begärs under denna tid, upphör engångslösenordet att gälla och kunden ska göra en ny ansökan för att börja använda det tekniska gränssnittet.
- Överföringskoden och engångslösenordet skickas till certifikatets tekniska kontaktperson per säker e-post. Kunden får ett lösenord för meddelandet per sms.

För begäran om certifikat skapar kunden ett 2048-bit nyckelpar med RSA-algoritmen. Kunden skapar även en signaturbegäran för certifikatet (Certificate Signing Request, CSR) i enlighet med PKCS#10-definitionen. Begäran innehåller kundens offentliga nyckel.

Till tjänsteanropet för certifikatbegäran fogas signaturbegäran som skapats. I syfte att specificera och skydda begäran fogas dessutom den överföringskod och det engångslösenord som kunden fått till tjänsteanropet. Tjänsteanropet för certifikatbegäran returnerar en hämtningskod i mottagningskvitteringen för specificering av certifikatbegärans respons och det certifikat som ska skapas för ansökan i samband med en lyckad begäran. I samband med att certifikatet hämtas bör behandlingstiden för certifikatbegäran beaktas. Certifikatet kan inte hämtas direkt efter en lyckad certifikatbegäran. Certifikatet erhålls som respons för tjänsteanropet för ansökan om certifikat, och till denna fogas en hämtningskod. Efter en lyckad certifikatansökan har kunden det certifikat som behövs för att använda inkomstregistrets tjänster. Om certifikatet inte kan bildas på grund av en felsituation returnerar tjänsteanropet för certifikatansökan ett felmeddelande i stället för ett certifikat.

3.3 Stängning av certifikaten

Ett certifikat måste stängas, 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. Inkomstregisterenheten 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.

Inkomstregisterenheten ska kontaktas när ett certifikat ska stängas. Om stängning av certifikat finns ytterligare information på certifikattjänstens sidor. Man kan när som helst begära stängning av certifikat. 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 begäran om avstängning stängs certifikatet för gott.
- Kunden ska bekräfta stängning eller reaktivering av ett tillfälligt stängt certifikat inom 14 dygn från det tillfälliga användningsförbudets begynnelsetidpunkt. Om kunden inte inom denna tid bekräftar reaktiveringen stänger Certifikattjänsten certifikatet för gott.

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 ibruktagandet av det tekniska gränssnittet i inkomstregistrets e-tjänst och hämta certifikatet på samma sätt som första gången.

3.4 Certifikatens livscykel och förnyande av dessa

Kundens certifikat är giltigt i två år, varefter det måste förnyas. Innehavaren av ett certifikat måste regelbundet kontrollera certifikatens giltighetstid. Certifikatets sista giltighetsdag kan kontrolleras från inkomstregistrets e-tjänst eller ur certifikatet.

Certifikatet kan förnyas via gränssnittet för certifikattjänsten. Det finns en egen tjänst (RenewCertificate) för detta syfte i gränssnittet. För förnyande av ett certifikat bildas ett nytt nyckelpar, en signaturbegäran skapas och tjänstebegäran undertecknas med en nyckel för det tidigare certifikatet som fortfarande är i kraft. Certifikatet som håller på att gå ut kan förnyas tidigast sextio (60) dygn före giltigheten upphör. Det gamla certifikatet gäller tills den ursprungliga giltighetstiden utgår. Om certifikatet förnyas i tid, behöver inte ett nytt certifikat beställas och då skickar inte inkomstregistret heller överföringskoder (överföringskod och engångslösenord).

På bild 2 finns en beskrivning av hur ett certifikat förnyas.

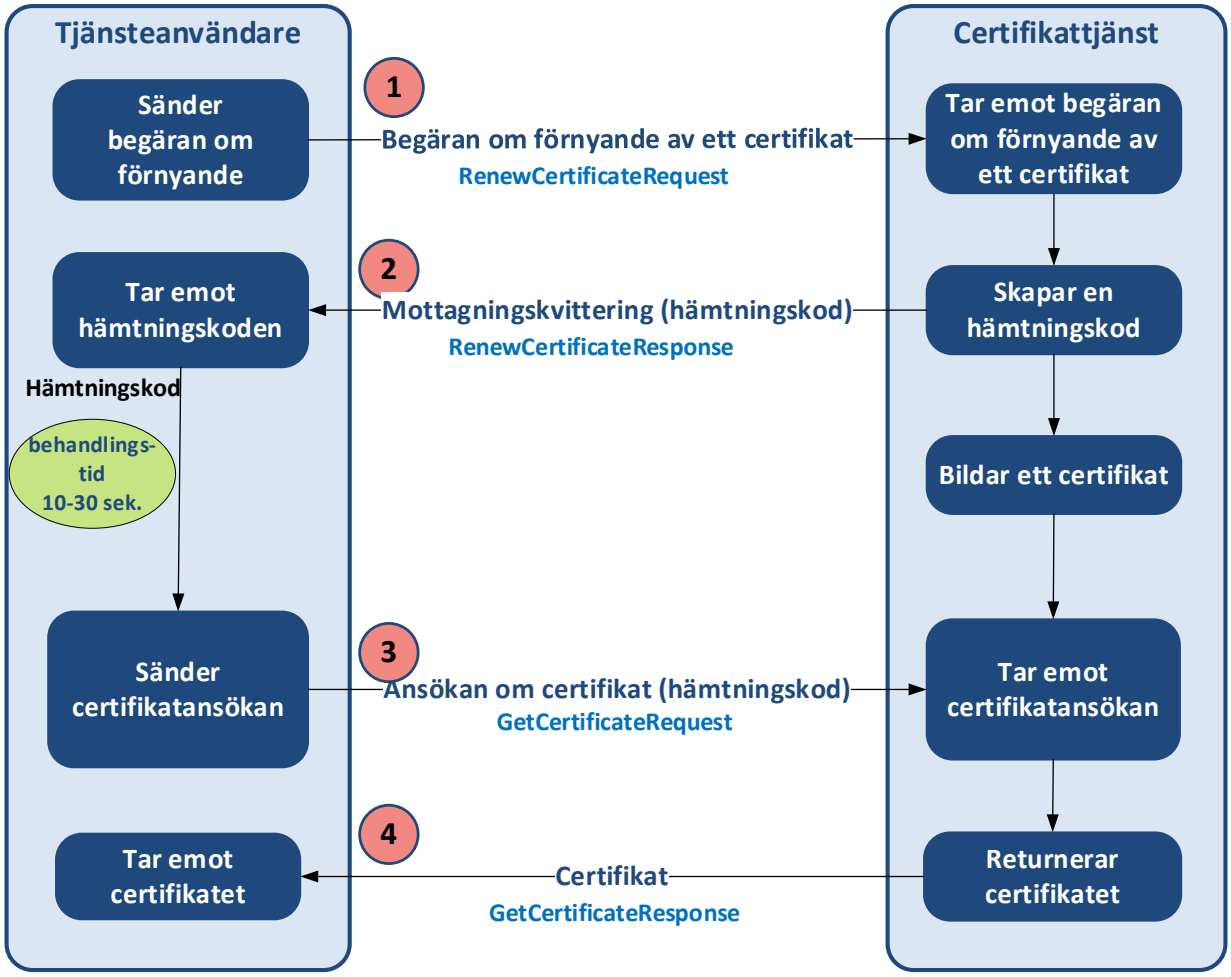

Bild 2. Förnyande av ett certifikat.

För att förnya ett certifikat måste kunden skapa ett nytt nyckelpar samt göra en signaturbegäran för certifikatet (CSR) på samma sätt som när ett nytt certifikat begärs.

Signaturbegäran som tjänsteanvändaren skapat fogas till tjänsteanropet gällande förnyande av ett certifikat. Tjänsteanropet undertecknas elektroniskt med den privata nyckeln för det tidigare certifikatet som fortfarande är i kraft.

Certifikatet undertecknas på samma sätt som när man sänder material till inkomstregistret med ett giltigt certifikat. Funktionen Förnyande av ett certifikat återställer hämtningskoden för certifikatet, och när man använder denna söks ett nytt certifikat med tjänsteanropet för ansökan om ett certifikat på samma sätt som när ett certifikat söks första gången. I samband med att certifikatet hämtas bör behandlingstiden för certifikatbegäran beaktas. Certifikatet kan inte hämtas direkt efter en lyckad certifikatbegäran.

Obs! Det tidigare certifikatet måste ersättas med ett nytt certifikat utan dröjsmål, alltid senast då dess giltighetstid upphör. Om samma certifikat har använts på flera än ett ställe, måste 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 inkomstregistrets e-tjänst. I detta fall begärs och hämtas ett nytt certifikat på samma sätt som när man beställer ett certifikat första gången.

3.5 Felsituationer

I regel ger certifikattjänsten uppgifter om fel omedelbart i samband med svaret. En del av felen upptäcks dock först vid behandlingen av certifikatbegäran, då tjänsteanropet för certifikatansökan returnerar ett felmeddelande i stället för ett certifikat.

Omedelbart i mottagningskvitteringen för tjänsteanropet ges information om fel när

- tjänsteanropet inte är i enlighet med schemat
- överföringskoden är felaktig
- 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 man inte lyckas skapa ett certifikat, bör en eventuell felsituation, såsom felaktiga identifierare, korrigeras. Efter det ska tjänsteanropet för certifikatansökan som avslutades i ett fel utföras på nytt. Ett undantag utgör en situation där systemet inte har hunnit behandla certifikatbegäran före man försöker hämta certifikatet. I så fall kan man försöka på nytt efter behandlingstiden som är 10-30 sekunder.

En beskrivning av felkoderna och förklaringarna finns i beskrivningen av gränssnittet för certifikattjänsten.

4 ANVÄNDNING AV CERTIFIKAT I INKOMSTREGISTRETS TEKNISKT GRÄNSSNITT

I samband med att förbindelsen skapas kontrollerar inkomstregistrets tekniska gränssnitt certifikatets giltighet och användningsändamål. Om certifikatet inte längre är i kraft, om det är stängt eller om det har beviljats för en annan kanal misslyckas skapandet av förbindelsen. Ytterligare information om användningen av inkomstregistrets gränssnitt, identifieringen av kunden och elektronisk underskrift finns i dokumentet Tekniskt gränssnitt - Tillämpningsanvisning.

4.1 Web Service -kanal

I inkomstregistrets Web Service-kanal används certifikatet för identifiering av kunden. Certifikatet och den privata nyckeln används för elektronisk underskrift av material.

4.2 SFTP-kanalen

Inkomstregistrets SFTP-kanal använder användarnamn och certifikatets nyckelpar för identifiering av kunden. För identifiering innehar inkomstregistrets certifikattjänst och SFTP-servern den offentliga nyckeln av nyckelparet, och kunden identifierar sig med sin privata nyckel. Certifikatet och den privata nyckeln används för elektronisk underskrift av material.

5 TESTNING AV TJÄNSTEN

Certifikattjänsten och de certifikat certifikattjänsten beviljat kan testas före ibruktagandet av tjänsten. Programgenomförandet som utnyttjar det tekniska gränssnittet kan testas före användningen av de egentliga testcertifikaten i certifikattjänstens testbädd. I testbädden kan gränssnittens viktigaste funktioner testas upprepade gånger med på förhand fastställda testnycklar. Ytterligare information om testningen av certifikattjänsten och testbädden finns på webbsidan Certifikattjänstens intressentgruppstestning.