



Nytt Tullverkets signeringscertifikat samt nya mellanliggande certifikat för Tullverkets CA för informationsutbyte via EDI

Se till att systemansvarig för ert EDI-system får denna information.

Vad påverkas?

Förändringarna påverkar era EDI-system både när det gäller att signera information **som sänds till Tullverket** och kontrollera signaturen i information **som tas emot från Tullverket**.

De allra flesta företagen behöver ha två typer av signeringscertifikat från Tullverket för sin EDI-lösning, Företagets signeringscertifikat, som används för att signera meddelanden från företaget till Tullverket och Tullverkets signeringscertifikat, som används för att signera meddelanden från Tullverket till företaget. Förändringarna påverkar **båda** dessa typer av signeringscertifikat.

När sker förändringarna?

Från och med **den 23 mars 2021** kommer **alla nya Företagets signeringscertifikat** utfärdas med ett nytt mellanliggande utfärdarcertifikat, "Swedish Customs Public CA 1.1".

Från och med **den 13 april 2021 kl. 13.00** kommer ett nytt **Tullverkets signeringscertifikat** användas, utfärdat med ett **nytt** mellanliggande utfärdarcertifikat, "Swedish Customs Internal CA 1.1".

För att informationsutbytet via EDI ska fortsätta att fungera, måste dels de nya mellanliggande utfärdarcertifikaten, dels det nya Tullverkets signeringscertifikat installeras i ert EDI-system.

Era befintliga Företagets signeringscertifikat kan användas fram till giltighetstidens slut, som är angiven i certifikaten. **Giltighetstiden är inte i något fall längre än till den 12 januari 2022 för certifikat utfärdade med "Swedish Customs Public CA 1.0"**.

Fram till den 23 mars 2021 kommer era Företagets signeringscertifikat att utfärdas med det gamla mellanliggande certifikatet "Swedish Customs Public CA 1.0" vid beställning via certifikatbeställningstjänsten <https://foretagstjanster-certifikatbestallning.tullverket.se/certifikat> eller via Certifikatbeställning med e-post och brev. Certifikaten kommer därför att vara giltiga till den 12 januari 2022.

Hur kan ni säkerställa att det fungerar?

För att systemleverantörer och företag med egenutvecklade system ska kunna verifiera funktionen är det nu möjligt att beställa Företagets signeringscertifikat utfärdade med det nya mellanliggande certifikatet "Swedish Customs Public CA 1.1" via Certifikatbeställning med e-post och brev. Dessa signeringscertifikat kan användas samtidigt som era befintliga. Det är inte några testcertifikat utan fullt fungerande produktionscertifikat som kommer att vara giltiga 14 månader.

Ange tydligt att beställningen gäller signeringscertifikat från den nya "Swedish Customs Public CA 1.1", annars kommer det gamla "Swedish Customs Public CA 1.0" användas fram till den 23 mars 2021.

Beskrivning av beställning av Företagets signeringscertifikat finns på tullverket.se på sidan *EDI – Beställning av företagets signeringscertifikat*, <https://www.tullverket.se/sv/foretag/deklareradigitalt/komigangattdeklareraedi/edisigneringscertifikatochanmalanavkontaktperson/edibestallningavforetagetssigneringscertifikat.4.153f8c8c16ffad23c223311.html>.

Mer information finns på <https://www.tullverket.se/edisakerhet> samt nedan.

Med vänliga hälsningar
Tullverket, IT-avdelningen,
EDI-certifikat

Bilaga 1: Certifikathierarki och nedladdningslänkar

Befintligt rotcertifikat används även i fortsättningen. De nya mellanliggande utfärdarcertifikaten är giltiga till den 11 februari 2031. Signeringsalgoritm för utfärdarcertifikaten, Tullverkets signeringscertifikat och Företagets signerings-certifikat är sha256WithRSAEncryption. Den föråldrade sha1WithRSAEncryption används alltså inte längre.

Rotcertifikat

Rotcertifikatet är oförändrat.

CN=Swedish Customs Public Root CA 1.0,serialNumber=SE2021000969,OU=Root Certificate Authority,OU=Swedish Customs,O=Tullverket,C=SE

PEM-format <https://ca.tullverket.se/ca/SwedishCustomsPublicRootCA1.0.crt>

DER-format <https://ca.tullverket.se/ca/SwedishCustomsPublicRootCA1.0.cer>

Gammalt mellanliggande utfärdarcertifikat för Företagets signeringscertifikat

Detta kommer inte användas efter den 23 mars 2021. Giltighetstiden på utfärdade signeringscertifikat blir till den 12 januari 2022.

CN=Swedish Customs Public CA 1.0,serialNumber=SE2021000969,OU=Only for authorized use,OU=Public Intermediate Certificate Authority,OU=Swedish Customs,O=Tullverket,C=SE

PEM-format <https://ca.tullverket.se/ca/SwedishCustomsPublicCA1.0.crt>

DER-format <https://ca.tullverket.se/ca/SwedishCustomsPublicCA1.0.cer>

Gammalt mellanliggande utfärdarcertifikat för Tullverkets signeringscertifikat

Detta används för Tullverkets signeringscertifikat som kommer att användas fram till den 13 april 2021 kl. 13.00.

CN=Swedish Customs Internal CA 1.0,serialNumber=SE2021000969,OU=Only for authorized use,OU=Internal Intermediate Certificate Authority,OU=Swedish Customs,O=Tullverket,C=SE

PEM-format <https://ca.tullverket.se/ca/SwedishCustomsInternalCA1.0.crt>

DER-format <https://ca.tullverket.se/ca/SwedishCustomsInternalCA1.0.cer>

Nytt mellanliggande utfärdarcertifikat för Företagets signeringscertifikat

Detta kommer att användas för alla Företagets signeringscertifikat från den 23 mars 2021. Giltighetstiden på utfärdade signeringscertifikat blir 14 månader.

CN=Swedish Customs Public CA 1.1,serialNumber=SE2021000969,OU=Only for authorized use,OU=Public Intermediate Certificate Authority,OU=Swedish Customs,O=Tullverket,C=SE

PEM-format <https://ca.tullverket.se/ca/SwedishCustomsPublicCA1.1.crt>

DER-format <https://ca.tullverket.se/ca/SwedishCustomsPublicCA1.1.cer>

Nytt mellanliggande utfärdarcertifikat för Tullverkets signeringscertifikat

Detta används för Tullverkets signeringscertifikat som kommer att användas från och med den 13 april 2021 kl. 13.00 samt för kommande Tullverkets signeringscertifikat.

CN=Swedish Customs Internal CA 1.1,serialNumber=SE2021000969,OU=Only for authorized use,OU=Internal Intermediate Certificate Authority,OU=Swedish Customs,O=Tullverket,C=SE

PEM-format <https://ca.tullverket.se/ca/SwedishCustomsInternalCA1.1.crt>

DER-format <https://ca.tullverket.se/ca/SwedishCustomsInternalCA1.1.cer>

Bilaga 2: Nytt Tullverkets signeringscertifikat för informationsutbyte via EDI

Tullverkets signeringscertifikat, som vi använder för att signera meddelanden vi sänder till er, kommer att bytas ut **den 13 april 2021 kl. 13.00**, vilket innebär att det nya certifikatet måste installeras i ert system före den tidpunkten. I och med att Tullverkets signeringscertifikat utfärdats med ett **nytt** mellanliggande utfärdarcertifikat, "Swedish Customs Internal CA 1.1" måste även det installeras.

Observera att det nuvarande Tullverkets signeringscertifikat måste finnas kvar i ert system till dess ni hämtat och signaturkontrollerat samtliga dokument som Tullverket signerat till och med den 13 april 2021.

Giltighetstiden på det nya signeringscertifikatet är 14 månader.

Tullverkets signeringscertifikat

serialNumber=SE2021000969,OU=Swedish Customs,O=Tullverket,C=SE,CN=Tullverket EDI

Nytt Tullverkets signeringscertifikat, som används från och med den 13 april 2021, kan hämtas från följande adresser:

PEM-format <https://ca.tullverket.se/ca/TullverketEDI20210216.crt>

DER-format <https://ca.tullverket.se/ca/TullverketEDI20210216.cer>

Nuvarande Tullverkets signeringscertifikat, används till och med den 13 april 2021, kan hämtas från följande adresser:

PEM-format <https://ca.tullverket.se/ca/TullverketEDI20200225.crt>

DER-format <https://ca.tullverket.se/ca/TullverketEDI20200225.cer>

Bilaga 3: Tekniska detaljer angående EDIFACT-dataelementen "Key name" och "Certificate reference" i AUTACK

Dataelementen "Key name" och "Certificate reference" i AUTACK-meddelandet används för att avgöra vilket signeringscertifikat som har använts. Dessa uppgifter kan räknas ut automatiskt av tullsystemen men det kan finnas system där dessa uppgifter måste registreras manuellt.

Tekniska specifikationer SCTS-SC för AUTACK-meddelandet finns på:

<https://www.tullverket.se/sv/foretag/deklareradigitalt/ediforsystemutvecklare/editekniska/specifikationer/sctssc.4.4481397d16411b864651709.html>

Tullverkets signeringscertifikat

"Key name" för nytt Tullverkets signeringscertifikat, som används från och med den 13 april 2021 är "swhPGb2wmoFps6OSYUhb21IT208=" och "Certificate reference" är "AXerWRNq".

"Key name" för nuvarande Tullverkets signeringscertifikat, som används till och med den 13 april 2021 är "esJUyYUyvQ02Sc+P1gNA0/tfOMc=" och "Certificate reference" är "AXB7U+bV".

Företagets signeringscertifikat

Både "Key name" och "Certificate reference" visas i e-postbekräftelsen med Företagets signeringscertifikat och i certifikatbeställningstjänsten.

"Key name" anges i e-postbekräftelsen som "Base64-kodad identitet för CA-certifikatet (authorityKeyIdentifier[keyIdentifier])" och i certifikatbeställningstjänsten som "Authority key identifier".

"Certificate reference" anges i e-postbekräftelsen som "Base64-kodat certifikatserienummer" och i certifikatbeställningstjänsten som "Certifikatserienummer".

Se även avsnitt 6.1.2, Kontrollera signatur för elektroniskt dokument från Tullverket, samt avsnitt 6.3, Att tänka på vid hantering av binära tal, i "Riktlinjer och anvisningar avseende säkerhet vid informationsutbyte via EDI":

https://www.tullverket.se/download/18.156454ca12c96d03cf28000790/riktlinjer_sakerhet_EDI_version_2.0.pdf