Swedish Customs

IT Department
EDI-certifikat
edi.certifikat@tullverket.se

Date	Our reference
1 March 2021	
Your date	Your reference

New Swedish Customs signature certificate and new intermediate certificates for Swedish Customs' CA for electronic data interchange (EDI)

Make sure that the system administrator for your EDI system receives this information.

What is affected?

The changes affect your EDI systems both in terms of signing information **sent to Swedish Customs** and verification of signatures of information **received from Swedish Customs.**

Most companies need two types of signature certificates from Swedish Customs for the EDI interchange, the Company Signature Certificate, used to sign messages from the company to Swedish Customs and the Swedish Customs Signature Certificate, used to sign messages from Swedish Customs. The changes affect **both** these types of signature certificates.

When do the changes take place?

From **March 23, 2021, all new Company Signature Certificates** will be issued with a new intermediate issuer certificate, "Swedish Customs Public CA 1.1".

From **April 13, 2021, at 11.00 AM UTC**, a new **Swedish Customs Signature Certificate**, issued with a **new** intermediate issuer certificate, "Swedish Customs Internal CA 1.1", will be used.

In order to ensure continued information exchange via EDI, both the new intermediate issuer certificates and the new Swedish Customs Signature Certificate must be installed in your system.

Your existing Company Signature Certificates can be used until the expiration date, as stated in the certificate. **In no case, the expiration date is later than January 12, 2022 for certificates issued by "Swedish Customs Public CA 1.0".**

Until March 23, 2021, your Company Signature Certificates will be issued with the old intermediate issuer certificate "Swedish Customs Public CA 1.0" when ordered via our web service Certifikatbeställning https://foretagstjanster-certifikatbestallning.tullverket.se/certifikat (available only in Swedish for persons with Swedish BankID) or via mail and email. The expiration date will be January 12, 2022.

How can you verify that it works?

To enable system developers and companies developing their own systems to verify the function, it is now possible to order Company Signature Certificates issued with the new intermediate issuer certificate "Swedish Customs Public CA 1.1" via e-mail and mail. These Signature Certificates can be used simultaneously with your existing certificates. It is not any test certificates but fully functional production certificates which will be valid 14 months.

Clearly state that the order applies to signature certificates from the new "Swedish Customs Public CA 1.1", otherwise the old "Swedish Customs Public CA 1.0" will be used until March 23, 2021.

Description of ordering of Company Signature Certificates can be found at tullverket.se on page *EDI – Signature certificates and registration of contact person*, https://www.tullverket.se/eng/business/ediregistrationforelectroniccommunicationviaedi/edisignaturecertificatesandregistrationofcontactperson.4.153f8c8c16ffad23c223985.html.

More information can be found on https://www.tullverket.se/edisecurity and below.

Best regards
Swedish Customs, IT Division,
EDI-certifikat

Appendix 1: Certificate hierarchy and download links

The existing root certificate is used also in the future. The new intermediate issuer certificates are valid until February 11, 2031. The signature algorithm for the intermediate certificates, Swedish Customs Signature certificates and Company Signature Certificates is sha256WithRSAEncryption. The obsolete sha1WithRSAEncryption is not used anymore.

Root certificate

The root certificate is unchanged.

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

Old intermediate issuer certificate for Company Signature Certificates

This will not be used after March 23, 2021. The expiration date for issued Company Signature Certificates will be January 12, 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

Old intermediate issuer certificate for Swedish Customs Signature Certificates

This is used for the Swedish Customs Signature Certificate used until April 13, 2021, at 11.00 AM UTC.

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

New intermediate issuer certificate for Company Signature Certificates

This will be used for all Company Signature Certificates issued from March 23, 2021. The validity period if issued signature certificates will be 14 months.

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

New intermediate issuer certificate for Swedish Customs Signature Certificates

This is used for the Swedish Customs Signature Certificate that will be used after April 13, 2021, at 11.00 AM UTC and for future Swedish Customs Signature Certificates.

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

Appendix 2: New Swedish Customs signature certificate for electronic data interchange (EDI)

Swedish Customs Signature Certificate, that we use to sign messages that we send to You, will be replaced April 13, 2021, at 11.00 AM UTC, which means that the new certificate must be installed in Your system before that time. Since the new Swedish Customs Signature Certificate is issued with a new intermediate issuer certificate, "Swedish Customs Internal CA 1.1", this must also be installed.

Observe that the current Swedish Customs Signature Certificate must remain in Your system until You have downloaded and verified the signature in all documents signed by Swedish Customs up to and including April 13, 2021.

The validity period for the new signature certificate is 14 months.

Swedish Customs Signature Certificate

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

New Swedish Customs Signature Certificate, used from and including April 13, 2021, can be downloaded from the following addresses:

PEM-format https://ca.tullverket.se/ca/TullverketEDI20210216.crt
DER-format https://ca.tullverket.se/ca/TullverketEDI20210216.cer

Current Swedish Customs Signature Certificate, used up to and including April 13, 2021, can be downloaded from:

PEM-format https://ca.tullverket.se/ca/TullverketEDI20200225.crt
DER-format https://ca.tullverket.se/ca/TullverketEDI20200225.cer

Appendix 3: Technical details regarding the EDIFACT data elements "Key name" and "Certificate reference" in AUTACK

The data elements "Key name" and "Certificate reference" in the AUTACK message are used to decide which signature certificate that has been used. These values can be calculated automatically by the customs management systems, but there may be systems where these values must be registered manually.

Technical specifications SCTS-SC for the AUTACK message can be found on:
https://www.tullverket.se/sv/foretag/deklareradigitalt/ediforsystemutvecklare/editekniska specifikationer/sctssc.4.4481397d16411b864651709.html

Swedish Customs Signature Certificate

"Key name" for the new Swedish Customs Signature Certificate, used from and including April 13, 2021, is "`swhPGb2wmoFps6OSYUhb2lIT208=`" and "Certificate reference" is "`AXerWRNq`".

"Key name" for the current Swedish Customs Signature Certificate, used up to and including April 13, 2021, is "`esJUpYUyvQ02Sc+P1gNA0/tfOMc=`" and "Certificate reference" is "`AXB7U+bV`".

Company Signature Certificates

Both "Key name" and "Certificate reference" is visible in the e-mail with the Company Signature Certificate and in our web service Certifikatbeställning.

"Key name" is stated in the e-mail as "Base64 encoded authority key identifier (authorityKeyIdentifier[keyIdentifier])" and in our web service Certifikabeställning as "Authority key identifier ".

"Certificate reference" is stated in the e-mail as "Base64 encoded certificate serial number" and in our web service Certifikatbeställning as "Certifikatserianummer".

See also section 6.1.2, Verifying a signature for an electronic document (from Swedish Customs), and section 6.3, Important to remember when using binary numbers, in in "Guidelines and instructions on security for electronic data interchange (EDI)":
https://www.tullverket.se/download/18.574422c13605990067976/1371032571298/Guidel ines%20on%20security%20for%20electronic%20interchange%20EDI%20version%202.0_EN. PDF.