Tullverket

Guidelines and instructions on security for electronic data interchange (EDI)

English translation 2011-06-23
based on Swedish version 2.0

This is an unofficial translation. In case of any discrepancies between the Swedish and English versions, the Swedish version shall prevail.

Contents

Updates from the Swedish version 1.0 to 2.0 of the document

SECTIONS	COMMENTS
Section1.5	Text of the Category 2 has been updated.
Section 4.1	Editing and clarifications.
Section 4.2	A footnote has been added to clarify the certificate field "serialNumber".
Section 5.1	A new paragraph has been added at the end of requirement 1. The footnote on two-factor authentication has been clarified.
Section 6	Section 6 has been edited and clarified, for instance regarding key length, reference to RFC 3447 and subfield *keyIdentifier* to *authorityKeyIdentifier*.
Appendix A	Appendix A has been supplemented with description, format and content of the certificates.
Appendix B	Appendix B has been supplemented with examples of how a CSR file can be created in some common computing environments.

1 Introduction

1.1 Swedish Customs' security concept for EDI

Secure electronic data interchange (EDI)[1] means that the issuer of the information can be secured identified, that the information is protected against change, and that it is transferred by means of secure communication[2].

For electronic data interchange, Swedish Customs has since the early 1990s used a security concept based on the SÄKdata seal method (subsequently called Nexus Electronic Seal) to substitute handwritten signatures. The use of that security concept is also governed by a set of rules containing guidelines and instructions[3].

As from 2010, Swedish Customs uses a PKI-based security concept for EDI communication. The PKI-based security concept for EDI, hereinafter called 'the security concept', will be implemented gradually, and to start with the old concept can be used alongside the new one.

These are a few characteristic distinctions between the two solutions:

PKI-based solution	**Previous solution (Nexus Electronic Seal)**
Data is locked by an electronic signature created through PKI-based asymmetric cryptography, where only the person issuing the information has access to the private key.	Data is locked through a seal[4] created through symmetric cryptography, where the sender and the recipient both have access to the secret key.
Method based on common standards.	Proprietary method.
Within the limits of Swedish Customs' guidelines and instructions, the companies can choose their own method to identify users in their system for submission of information.	Swedish Customs makes specific demands regarding the method used to uniquely identify the users in the company's system for submission of information.
A company key is used to create a signature. This enables Swedish Customs to uniquely identify the company by the electronic signature, but not the individual user within the company. However, for certain document categories, the company must be able to provide information on the identity of the individual user associated with the message.	An individual key is used to create a seal. This enables Swedish Customs to identify the specific user directly from the seal.

[1] In this document, the term 'electronic data interchange' (EDI) refers to system-to-system exchange of information.

[2] Communications protocols and security regarding such protocols are outside the scope of Swedish Customs' security concept for EDI and is therefore not covered by this document.

[3] See i.a. *Säkerhetsfrågor i Tullverkets EDI-system* (*Security Issues in Swedish Customs' EDI system*), 2006-10-04, version 1.0.

[4] Historically, the notion *seal* has been used to describe locking data through a symmetric encryption/decryption key, where the sender and the recipient both have access to the secret key, while the notion *signature* is used to describe locking data in the PKI-based solution.

1.2 Purpose, scope and use of this document

This document is aimed at system suppliers providing standard systems for EDI communication with Swedish Customs, companies developing equivalent systems on their own, and companies choosing to buy standard systems from a system supplier. When choosing and implementing a system, the company submitting the information is the one responsible to meet the conditions set up by Swedish Customs.

The document covers EDI-based system-to-system data interchange with Swedish Customs, but does not include user-to-system interchange, for example via a web interface. Examples of common EDI communication are customs import and export declarations.

The document describes the use of the PKI-based security concept for EDI, and focuses on security and technical issues. It further includes requirements for the company's implementation of their customs management system, to ensure the protection of the electronic documents transferred as well as a reliable identification of the company and – when applicable – a reliable identification of authorised users.

The document includes technology-oriented instructions for the technical implementation, as well as guidelines aiming to achieve a reliable implementation of the security concept. The technology-oriented instructions are divided into a main part applicable regardless of the format, and a part with more specific instructions for the different formats, starting with EDIFACT.

The choice of communications protocol and the security methods incorporated, cryptography etc., is also important but is not covered in detail in this document.

1.3 Legal basis

In accordance with the Community Customs Code[5], customs declarations in writing shall be signed. In accordance with the Code's implementing provisions[6], the Customs authorities shall determine the rules for replacement of the handwritten signature in electronic declarations. This shall include i.a. measures for checking the source of data and for protecting data against the risk of unauthorised access, loss, alteration or destruction. Furthermore, the Swedish Customs Act[7] states that it must be possible to verify the contents and the issuer of an electronic document through a certain technical procedure.

According to the Modernised Customs Code[8], customs declarations made using an electronic data-processing technique shall contain an electronic signature or other means of authentication.

[5] Article 62 of the Commission Regulation (EEC) 2913/92

[6] Article 4b of the Commission Regulation (EEC) 2454/93

[7] Swedish Customs Act (SFS 2000:1281), chapter 2, section 2

[8] Article 108 of the European Parliament and Council Regulation (EC) 450/2008

In the future, other electronic documents governed by other legislation may occur, which may lead to other requirements on electronic signatures.

1.4 Responsibility for the submission of information

If the information is submitted by a legal person, the declaration shall be signed by an authorised signatory or a person to whom the signing authority has been delegated. Generally, the power to sign on behalf of the company is held by the board of directors. The Chief Executive has the signing authority in the day-to-day administration, in which the lodging of customs declarations should be included. In addition, a person can be delegated the signing authority for specific purposes, for example to lodge customs declarations. The signing authority can be delegated in writing or orally. It can also be granted implicitly to people holding a certain position in the company.

Legal representatives of a business have a direct responsibility for the business and are fully responsible even for their lack of action. This responsibility applies as long as the person holds the position as a representative. Under certain circumstances, the delegation of working tasks and powers of authority can lead to responsibility for the person to whom the tasks or powers are delegated. In such cases, the responsibility is determined based on the circumstances in the specific case.

1.5 Categories of electronic documents

In the security concept, two categories of electronic documents are defined for EDI communication between a company and Swedish Customs. Each EDI authorisation contains information on the category in which a specific electronic document falls.

Category 1 – no requirement for the identification of a natural person

This refers to electronic documents not covered by requirements that an authorised user approves the data before they are submitted, and where the sender does not have to identify an authorised natural person – neither when the information is submitted, nor subsequently.

Thus, this category of electronic documents can be created and submitted automatically in a computerised system.

Category 2 – with requirement for the identification of a natural person

This refers to electronic documents covered by requirements that an authorised user must approve the data before they are submitted, and where Swedish Customs shall be able to get information about the identity of the person that approved the data – not during the transmission, but at a later stage.

The method used for identification of authorised user, access control and logging related to the user and data in the electronic document must fulfil the requirements from Swedish Customs.

The data must be locked during the process when the data are reviewed and approved by a natural person whose responsibility is linked to the data being transmitted in the electronic document. Thus, this category of electronic documents cannot be created and transmitted automatically in a computerised system.

1.6 Terminology used

	Description
Authorised signatory	The authorised signatory, e.g. the Chief Executive has the primary responsibility. The company registration certificate states who has the power to sign on behalf of the company. The authorised signatory can delegate specific responsibilities. The person appointed responsibility for customs matters are sometimes called the Customs Manager. In this document, the Customs Manager will be considered an authorised signatory.
Authorised user	A person who has the authority to approve (electronically sign) electronic documents before they are submitted.
Contact person for signature certificates	The person, who orders, receives and manages the signature certificates for EDI data interchange.
Electronic document	By an electronic document in this context, we refer to the contents of the document from an business point of view, and do not focus on its technical format (EDIFACT, XML etc.). In reality, however, it is the technical format that is signed.

2 Brief description of the security concept

From the PKI-based security concept follows that the exchange of information between Swedish Customs and the companies is always made by signed electronic documents. For the flow of information from the company to Swedish Customs a signature certificate issued for the company is used to create an electronic signature. For information flow in the reverse direction a signature certificate issued for Swedish Customs is used.

Traditionally, secure EDI communication requires that:

1. the electronic document cannot be changed without this being detected
2. no one shall be able to send the electronic document in someone else’s name – deliberately or by mistake – without this being detected
3. the sender shall not be able to deny having produced and sent the electronic document
4. the recipient shall not be able to deny having received the electronic document
5. no unauthorised person shall be able to read the electronic document.

Items 1-3 are ensured by the PKI-based security concept, item 4 by the requirement for signed receipt messages, and item 5 by the requirement for encrypted communication.

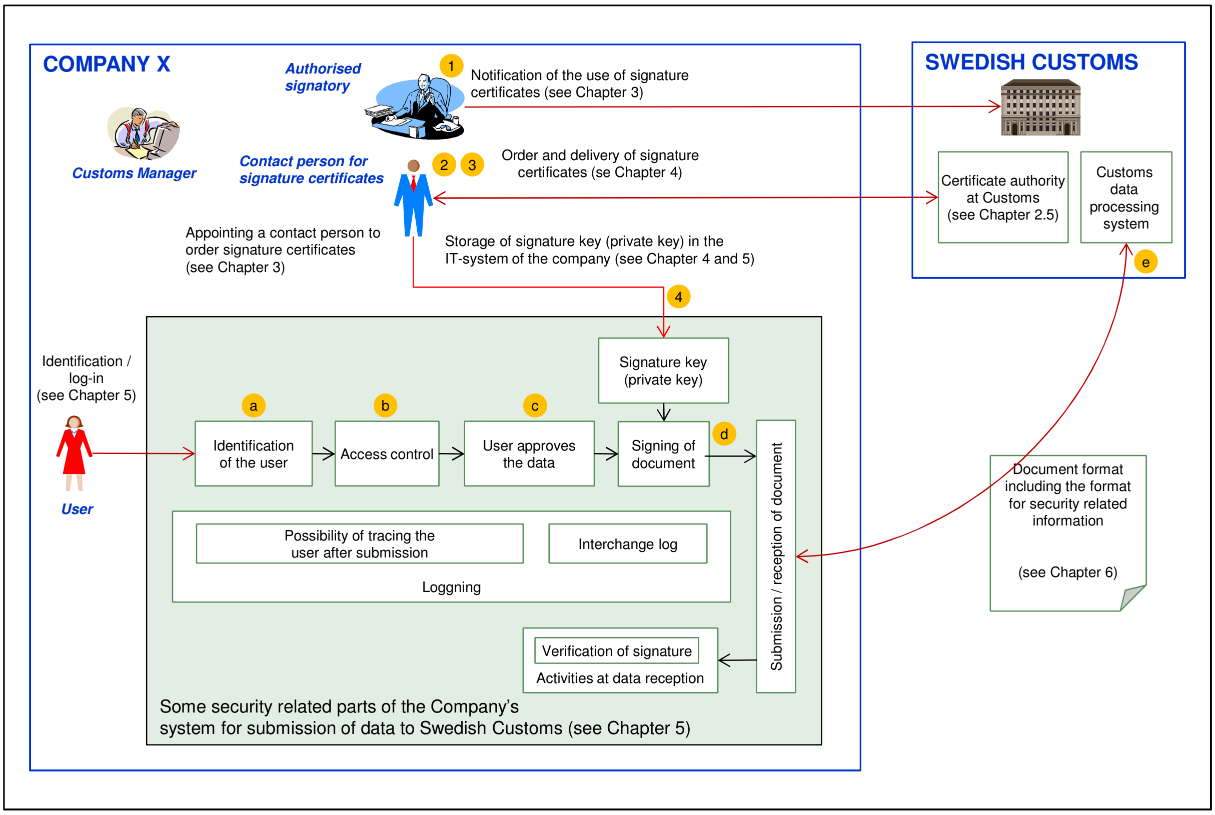
In addition to these general EDI requirements, Swedish Customs requires the possibility to identify a natural person for electronic documents of Category 2.

2.1 Description of the concept

The example below illustrates some important points of the security concept for data interchange of electronic documents of Category 2. For documents of Category 1 there are some simplifications since no identification of a natural person is needed.

In the example, the company wants to send import or export declarations electronically to Customs and has applied for authorisation to do so. However, to start the electronic submission of information, they need a signature certificate.

The process can be divided into an administrative part, covering the management of signature certificates, and an operational part, covering the use of signature certificates in the data interchange with Customs.


COMPANY X
Customs Manager
Authorised signatory
1
Notification of the use of signature certificates (see Chapter 3)
Contact person for signature certificates
2
3
Order and delivery of signature certificates (se Chapter 4)
Appointing a contact person to order signature certificates (see Chapter 3)
Storage of signature key (private key) in the IT-system of the company (see Chapter 4 and 5)
4
SWEDISH CUSTOMS
Certificate authority at Customs (see Chapter 2.5)
Customs data processing system
e
Identification / log-in (see Chapter 5)
User
a
Identification of the user
b
Access control
c
User approves the data
Signature key (private key)
Signing of document
d
Submission / reception of document
Possibility of tracing the user after submission
Interchange log
Loggning
Verification of signature
Activities at data reception
Document format including the format for security related information
(see Chapter 6)
Some security related parts of the Company's system for submission of data to Swedish Customs (see Chapter 5)

2.1.1 Administrative management of signature certificates

To start the electronic submission of information, the company needs access to a signature certificate, which can be obtained by sending a notification to Swedish Customs.

1) In the notification, one or more contact persons are appointed for future contacts with Swedish Customs regarding signature certificates.

2) The contact person orders signature certificates from the Certificate authority at Swedish Customs.

3) The contact person initiates that a private (secret) key is generated by the company and is linked to the certificate (see Section 4).

4) The private key is stored in a secure way in the company's IT system.

To provide reliability, the total security of the company's customs management system must be sufficient. This includes i.a. a secure handling and storage of private keys linked to the signature certificates.

It is also important that the system offers traceability through log files (Category 2) so that the user signing an electronic document always can be identified with sufficient reliability (see Section 5).

2.1.2 The use of signature certificates in the data interchange

The way information is submitted differs between electronic documents of Category 1, without requirements for the identification of a natural person, and Category 2, with such requirements.

Requirements for electronic documents of Category 2:

a) initial identification of the person

b) check, based on the identity, that the person is authorised

c) the electronic document must be approved by the authorised user before it is signed.

Requirements for both categories of electronic documents:

d) the electronic document is signed using the company’s signature certificate

e) the signature is verified when received by Swedish Customs.

When Swedish Customs send a signed electronic document to the company, the signature must be verified by the company.

2.2 Electronic signature

The significance of a handwritten signature varies depending on the document that is signed. At its simplest form, the signature only indicates that the person has read a document. In other contexts, for example in a real estate purchase contract, the significance of the signature is considerably higher with regard to non-repudiation. Non-repudiation means that the person cannot deny having approved a transaction etc. by signing it.

The electronic signature is the electronic-world equivalent of a handwritten signature. Like the handwritten signature, the electronic equivalent can mean different things depending on the demands put on the electronic document. An electronic signature can also be called a digital signature.

Characteristic of the signature used in Swedish Customs PKI-based security concept is that it is only linked to the company. In other words, it has no direct link to the person approving the data. However, for electronic documents of Category 2, the company must always be able to account for the natural person having approved the data and, when Customs so demand, provide information on the identity of this person.

2.3 PKI

The acronym PKI in Swedish Customs PKI-based security concept, means Public Key Infrastructure. A basic feature of a PKI-based security concept is that, to verify the signature, the receiving party does not need access to the key that the sender uses to sign the electronic document. To handle this, each party participating in the data interchange has a unique pair of keys, with a *private key* that must be kept secret and a *public key* that can be distributed to all parties.

There is a strong mathematic relation between the private key and the public key. This relation enables the recipient of an electronic document to use the public key to verify whether the signature of the electronic document is created by use of the corresponding private key.

2.4 Signature certificates

The meaning of ‘certificate’ in this context is defined by the international standard X.509. The certificate links the public key of the company (see 2.3) to the company name and other identification data. The connection is made by the certificate authority (see 2.5). To ensure that the connection is not subsequently changed, the certificate authority locks the certificate with a signature.

When the company sends a signed electronic document, Swedish Customs can use the public key of the company to verify that the signature is created by use of the corresponding private (secret) key. If this is the case, Swedish Customs can use the public key of the company and the linked identification data in the certificate for reliable identification of the company that produced the electronic document. This enables non-repudiation for data interchange where this is required. In the same way, the company can verify electronic documents sent from Customs by verifying Customs’ signature.

A signature certificate used for data interchange between a company and Swedish Customs is not linked to an individual person. The signature certificate is only linked to the company and is thus an organisation-oriented certificate.

2.5 Certificate Authority (CA)

Initially, Swedish Customs will be the certificate authority (CA) of the PKI-based security concept. One reason for this is that currently, the market cannot meet the needs to provide certificates to all companies with required functionality. The certificates provided by Swedish Customs are only intended for the signing of electronic documents in the data interchange with Customs.

As mentioned in Section 2.4 above, an important task for the certificate authority is to link the public key of the company to the company name and other identification data and to lock this information with a signature.

To archive reliability, the certificate authority must also ensure that the information in the certificate is correct. In the Swedish Customs PKI-based security concept for EDI, the company provides the certificate authority with this information. However, the certificate authority must ensure that the information can be traced to an authorised person (authorised signatory) and that it reaches the certificate authority unaltered together with information on the public key of the company.

3 Appointing a contact person for signature certificates

A company intending to use the PKI-based security concept needs access to signature certificates to sign electronic documents before sending them to Customs. By notifying Swedish Customs, the company can appoint one or more contact persons within the company and authorise them to order and administer signature certificates. The ordering of signature certificates is covered by Section 4.

To obtain a signature certificate, the company must be authorised to submit certain types of electronic information to Customs, or apply for such authorisation.

A notification form is available for download from the website of Swedish Customs. The notification shall include information on the contact persons authorised to order and administer signature certificates. You can also use the form to add new contact persons or remove previously reported contact persons.

The form shall be signed by an authorised signatory or a person to whom the signing authority has been delegated. Customs may verify the information against the registers of the Swedish Companies Registration Office or equivalent foreign registers, or by other means ensure that the signatory is entitled to sign on behalf of the company.

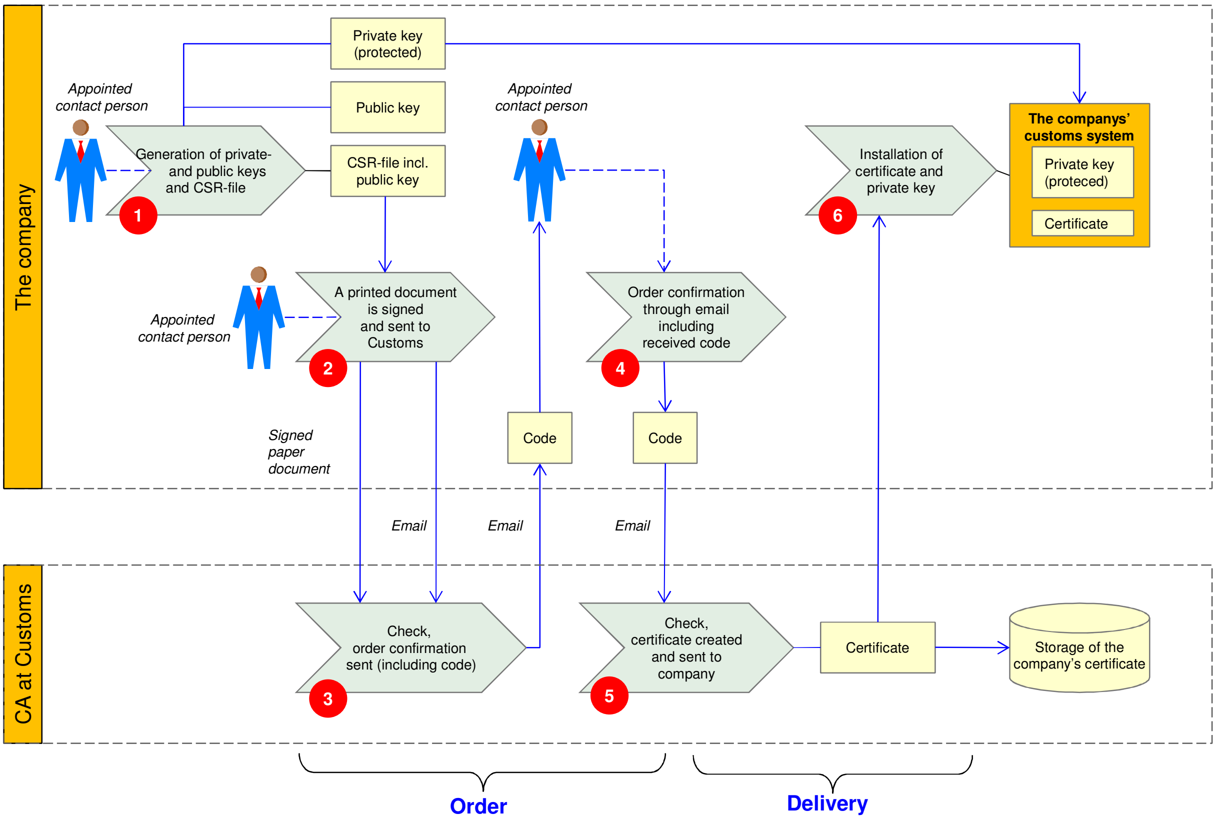
After having handled the application, Swedish Customs sends an acknowledgement receipt to the company, confirming that the notification has been received and handled.

4 Order, delivery and blocking of signature certificates

The certificates provided by Swedish Customs are only intended for the signing of electronic documents in the data interchange with Customs.

The signature certificate is valid for a limited period of time. It is the responsibility of the company to order a new certificate in good time before a certificate expires. Overlapping periods of validity is permitted and recommended. The procedure described below is applicable both to initial orders of certificates and to renewals.

4.1 Order and delivery


The company
CA at Customs
Private key (protected)
Public key
CSR-file incl. public key
Appointed contact person
Generation of private- and public keys and CSR-file
1
Appointed contact person
Installation of certificate and private key
6
The companys' customs system
Private key (proteced)
Certificate
Appointed contact person
A printed document is signed and sent to Customs
2
Order confirmation through email including received code
4
Signed paper document
Code
Code
Email
Email
Email
Check, order confirmation sent (including code)
3
Check, certificate created and sent to company
5
Certificate
Storage of the company's certificate
Order
Delivery

Step 1
The appointed contact person at the company generates a key pair, a private and a public key, using appropriate software. The private key must be handled in accordance with the security requirements listed in Section 5.

In connection with the generation of the keys, a CSR (Certificate Signing Request) file is also generated. This file includes the public key and other necessary data.

Step 2

The contact person at the company shall copy the entire plain text from the CSR file into an email message and send it to edi.certifikat@tullverket.se. Company name and EORI number shall be specified in the email subject line.

The content of the CSR file in plain text shall be copied into a document with the title "Ordering of signature certificate" and the company name and EORI-number shall be specified. A printout of the document shall be signed by the contact person (including name spelled out) and sent by postal mail to:

Swedish Customs, IT department
EDI Certificate
Aurorum 3
SE-977 75 Luleå
SWEDEN

The signed letter is necessary to legally associate the contact person to the issued signature certificate.

Step 3

Swedish Customs checks the order against previous notification of the use of signature certificates. The receipt of the order is confirmed via email to the contact person by use of the email address previously provided in the notification. In the receipt message Swedish Customs provides a code that the company shall use to confirm the order.

Step 4

The company contact person referred to in the order, confirms the order in an email by including the code received from Customs.

Step 5

When Swedish Customs has received an accurate order confirmation from the company contact person, Customs issues and signs an X.509 certificate valid 14 months from the time it is issued, based on the information received in the CSR file. The certificate is stored at the CA at Swedish Customs and sent by email to the company contact person by use of the email address provided in the notification.

Step 6

The company installs the received certificate and their private key using a process that meets the requirements listed in Section 5.

4.2 Creating a CSR file

When placing an order for a signature certificate, as described in the previous section, the company shall provide Swedish Customs with correct identification information through a “Certificate Signing Request” stored in a CSR file. The creation of a CSR file follows common standard (RFC 2986) and is implemented in development tools for various computing environments such as Windows, Java etc. Based on the CSR file, Customs issues the signature certificate to the company. The signature certificate is stored at Swedish Customs and sent to the company.

When creating the CSR file, the company also generates their public and private keys. The signature keys must be generated in a way that protects the private signature key against unauthorised access (see Section 5).

The customs management system at the company should provide a user-friendly interface for creating and sending CSR files to enable the contact person to handle this task without having deep technological knowledge.

The CSR file shall contain the following information regarding the identity of the company (subject):

Attribute	Maximum length	Note
countryName	2	Country Code for the company
organizationName	64	Company Name
organizationalUnitName	64	Unit within the company (optional)
serialNumber[9]	64	The EORI number of the company
commonName	64	Company name in a shorter version (optional)

In addition to these data, the public key of the company is included. See Appendix A and B for further information and some examples.

[9] Note that the 'serialNumber' in the table above does not refer to the certificate's serial number but is a part of the description of the organization for which the certificate is issued (the subject). See RFC 5280, Section 4.1.2.4, for further description of 'serialNumber'. In specification X.520 is 'serialNumber' defined by object identifier 2.5.4.5 and is of type "Printable String" (unlike the certificate's serial number which is of type "Integer").

4.3 Revocation

The signature certificates can be revoked.

4.3.1 Revocation initiated by the company

Should the company know or suspect that someone who is not an authorised user has access to the company's private key, a revocation of the certificate must be requested without delay.

A revocation request can be made by

- email
- fax
- telephone
- letter

Contact information to Swedish Customs can be found on our website www.tullverket.se. Before a certificate is revoked, Customs contacts the company to verify the revocation request.

4.3.2 Revocation initiated by Swedish Customs

Swedish Customs has the right to revoke a certificate issued by Customs to a company.

The motive for revocation may be e.g. suspected inaccuracies or the fact that other authorisations, mandatory for electronic data interchange, is withdrawn.

4.3.3 Publication of revoked certificates

Swedish Customs will publish lists of revoked certificates issued by Swedish Customs. The lists will include both certificates issued to Customs and to companies.

5 Requirements on the company's customs management system

The company shall use an implementation of the PKI-based security concept for their customs management system to ensure a high level of total security. This includes i.a. that the system shall meet the requirements listed below. The requirements are applicable to the submission of information to Customs as well as the reception of information from Customs.

The requirements set out for the customs management system vary according to the category of the documents submitted. In the boxes below, the symbols ❶ (Category 1) and ❷ (Category 2) are used to indicate to which category/categories the specific requirement applies. The categories are defined in Section 1.5.

5.1 Management of signature key

De signature of the electronic document is the basis for document security as well as for a reliable identification of the company.

Requirement 1 ❶ ❷	The signature keys must be generated and used in a way that protects the private signature key against unauthorised access. New signature keys must be generated for each new certificate and created by parameters that meet requirements on the quality of the keys. Key length for RSA keys shall be in accordance with Appendix A.

5.2 User identification and access control

As long as the Customs' requirements are met, the company can choose their own secure solution for identification of users approving data to be signed. Identification is a prerequisite for access control as well as for the possibility to trace the user at a later stage.

Identification

Requirement 2 ❷	A user approving data must be identified in the company's customs management system with a high level of security, which requires at least a two-factor solution[10]

[10] Factors to choose between are: Something you know (e.g. a password), something you own (e.g. a card or a security token), something you are (e.g. a fingerprint). "Something you own" refers to something which is difficult to copy and that only the user disposes and carries with him. Magnetic cards, IP addresses and reproducible list of one-time password does not meet this requirement. A two-factor solution means that you choose two different factors.

Requirement 3 ❷	To guarantee the identity of the user approving data to be signed, a new identification (in accordance with Requirement 2) has to be carried out after a certain time of inactivity. This time of inactivity should be relatively short to maintain a high level of security.
Requirement 4 ❷	After the submission, the company shall provide information of the identity of the authorised user who has approved the electronic document to be signed, if Customs so require. The EDI authorisation includes information on how long after the submission of the document this information must be accessible.

Access control

Requirement 5 ❷	The customs management system must be covered by an access control system, to ensure that only authorised users can approve data to be signed.
Requirement 6 ❷	Only specifically appointed officials shall have the power to authorise access to the system.

5.3 Approving and signing the data interchange

Prior to the submission to Customs, the user approves the data in the electronic document. As a result of the approval, a signature should be added to the transaction, locking the information and enabling the recipient to securely identify the sender. The document can either be signed directly when the data is approved or at a later stage.

Requirement 7 ❷	Prior to the approval of the electronic document, the user must be able to review all the information in a user-friendly way.
Requirement 8 ❷	The customs management system shall ensure that the information that is to be sent to Customs cannot be changed by other users while the user reviews the information before approving it.
Requirement 9 ❷	The approval of the data must require a deliberate action from the user (such as pressing a key) and the user must be made aware that this action equals a handwritten signature.
Requirement 10 ❷	If the signature is not created directly when the user approves the information, the information must be protected against change until the document is signed.

5.4 Signature verification at reception

Generally, all electronic documents from Swedish Customs contain a signature. At the reception of these documents, the company must verify this signature.

Requirement 11 ❶ ❷	In accordance with the technical specification for the type of electronic document, an acknowledgment receipt must be sent to Swedish Customs for all electronic documents received from Customs, to confirm that they have been received.
Requirement 12 ❶ ❷	The recipient shall verify the signature of all the electronic documents where a signature is mandatory according to the technical specification for the type of electronic document.
Requirement 13 ❶ ❷	If the signature is erroneous or missing, when it is mandatory according to the technical specification for the type of electronic document, an error message must be returned.

6 Security implementation for the EDIFACT format

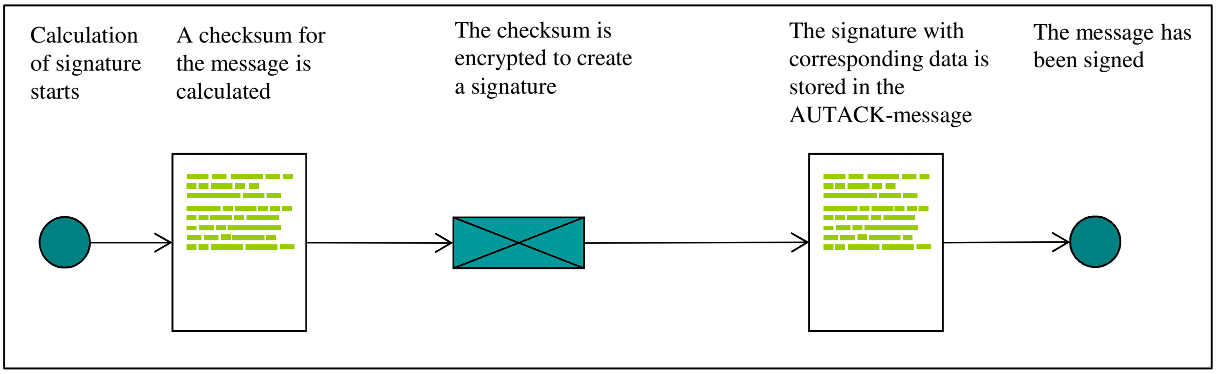
For the EDIFACT format, the AUTACK message is used to package signature-related information.

The ***SCTS-SC*** technical specification, which is available at Swedish Customs website, describes more in detail how the signature-related information is handled and stored in the AUTACK message.

Since the security concept is based on commonly supported standard security algorithms, all computer environments generally offer good support for implementation of electronic signatures. However, the implementation can differ between different development tools.

6.1 The Signing Process

6.1.1 Creating a signature for an electronic document (to Swedish Customs)


Calculation of signature starts
A checksum for the message is calculated
The checksum is encrypted to create a signature
The signature with corresponding data is stored in the AUTACK-message
The message has been signed

Before the signature process starts, the electronic document must be converted into an EDIFACT message.

The EDIFACT interchange consists of EDIFACT messages for the electronic documents included and an AUTACK message for the security information.

Firstly, a checksum is calculated based on the EDIFACT representation of the electronic document. The checksum is calculated for the whole message including all information, i.e. also EDIFACT control data like separator characters and segment name, by use of an algorithm in accordance with Section 6.2, see also the SCTS-SC technical specification that can be found on the website of Swedish Customs.

Next step is encryption of the checksum[11] through an algorithm for electronic signatures in accordance with Section 6.2. This encryption is performed by use of the company’s current

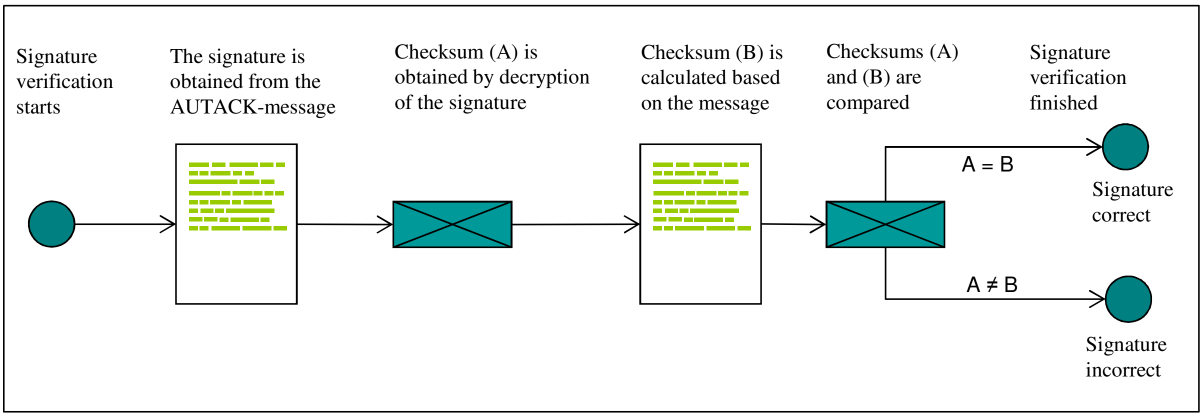
[11] Before encryption the checksum is complemented, see Section 6.2

signature key (private key) linked to the signature certificate. The encrypted checksum is the signature of the electronic document.

In order for the recipient to uniquely identify the certificate used, a reference shall be stored in the AUTACK message, with the certificate serial number (*serialNumber*) and a reference to the certificate authority (*authorityKeyIdentifier[keyIdentifier]*), see Appendix A.

The *serialNumber* and the *authorityKeyIdentifier[keyIdentifier]* of the certificate shall be stored in Base64 format in the *certificate reference* and *key name* data elements of the AUTACK message, see Appendix C.

6.1.2 Verifying a signature for an electronic document (from Swedish Customs)


Signature verification starts
The signature is obtained from the AUTACK-message
Checksum (A) is obtained by decryption of the signature
Checksum (B) is calculated based on the message
Checksums (A) and (B) are compared
Signature verification finished
A = B
Signature correct
A ≠ B
Signature incorrect

The EDIFACT interchange consists of EDIFACT messages for the electronic documents included and an AUTACK message for the security information.

The public key of the sender is obtained from the sender’s (Swedish Customs’) certificate. The certificate is published by Swedish Customs, but is not included in the EDIFACT transmission. More than one certificate can be valid at the same time, for example in connection with replacement of a certificate. To determine which certificate has been used, the data elements *key name* and *certificate reference* from the AUTACK message must be used, see the SCTS-SC technical specification.

The electronic signature is obtained from the AUTACK message. Through the public key of the sender and the algorithm for electronic signatures in accordance with Section 6.2, the signature received is decrypted and the checksum[12] is obtained (checksum A in the figure). A new checksum[13] is calculated for the received EDIFACT message (checksum B in the figure). The calculation is made in the same way as when a message is signed. After that, the

[12] The complemented checksum, see Section 6.2

[13] Checksum is complemented according to Section 6.2 before comparison is made

checksums A and B are compared and they should be identical to confirm that the signature is correct. The signature verification also includes generally recognised checks that the certificate is correct, i.e. check against lists of revoked certificates, check of the period of validity, check of root certificate including certificate chains, etc.

If the signature is incorrect, an error message is sent to Swedish Customs in accordance with current regulation.

6.2 Algorithms for checksum and electronic signature

Checksum	SHA-256 shall be used as checksum algorithm.
Electronic signature	RSA shall be used as encryption/decryption algorithm for electronic signature, see RFC 3447, RSASSA-PKCS1-v1_5. Key length for RSA keys shall be in accordance with Appendix A.

Before the checksum is encrypted, it is supplemented with data on checksum algorithm and padding bytes to achieve the same length as the encryption key. *Note that this functionality usually is included in the standard software functions used for signing.*

6.3 Important to remember when using binary numbers

Storage in the data element 'Key name' in AUTACK

The certificate field *authorityKeyIdentifier[keyIdentifier],* containing verification data used to identify the issuer certificate of the certificate authority (Swedish Customs), is stored in the data element *key name* in AUTACK*,* see Appendix A and the SCTS-SC technical specification. Before the data is stored, it has to be Base64 encoded, see Appendix C.

Storage in the data element 'Certificate reference' in AUTACK

The certificate field *serialNumber,* containing the certificate serial number, is stored in the data element *certificate reference* in AUTACK, see Appendix A and the SCTS-SC technical specification. Before the data is stored, it has to be Base64 encoded, see Appendix C.

Storage in the data element 'Validation value' in AUTACK

The calculated checksum and the electronic signature are stored in the data element *validation value* in AUTACK, see Appendix A and the SCTS-SC technical specification. Before the data is stored, the values have to be converted into hexadecimal code, see Appendix C.

Byte order in API calls of security functions

When making the technical implementation of the security concept, it is important to pay attention to the fact that different computer environments (Windows, Java etc.), may require different byte order for binary numbers in API calls of security functions (big endian or little endian).

7 Appendix A: Certificates – a technical description

7.1 Certificate Hierarchy

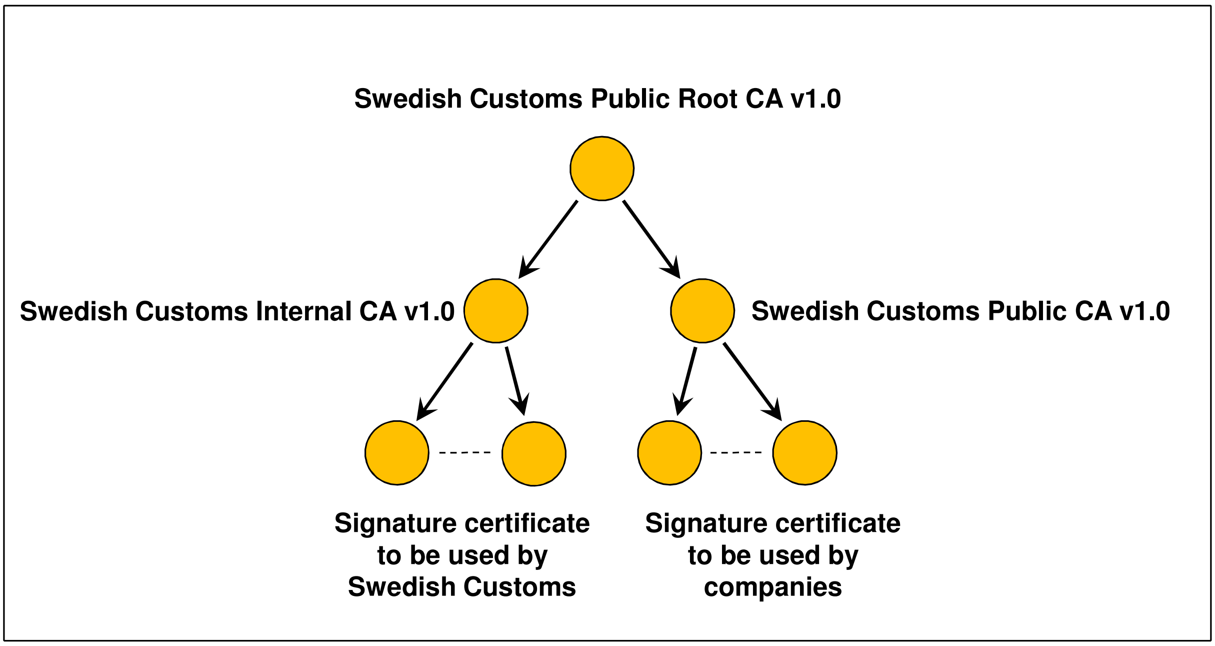
Swedish Customs PKI-based security concept for EDI has a certificate hierarchy of three levels.

On the lowest level is the signature certificates used for secure electronic data interchange (EDI) by companies and Swedish Customs. These signature certificates are signed by intermediate CA certificates.

On the intermediate level there are intermediate CA certificates with a maximum period of validity of 10 years, signed by the root certificate. Two types of intermediate CA certificates are used, one for signing company's signature certificates and the other for signing Swedish Customs own signature certificates.

At the top level is Swedish Customs root certificate with a maximum period of validity of 20 years, used only for the issuing of intermediate CA certificates.

Root- and intermediate CA certificates are published on www.tullverket.se.


Swedish Customs Public Root CA v1.0
Swedish Customs Internal CA v1.0
Swedish Customs Public CA v1.0
Signature certificate to be used by Swedish Customs
Signature certificate to be used by companies

7.2 Root certificate

Key length and validity period

RSA-key with a length of 2048 bits.
Period of validity: 20 years.

Certificate fields

Certificate fields	Comments
version	X.509 version 3 (value = 2)
serialNumber	Unique number for each certificate issued by the CA (Issuer)
signatureAlgorithm	sha1WithRSAEncryption
issuer	Issuer. For the root certificate, issuer and subject are the same
validity	See RFC 5280
subject	Organisation for which the certificate is issued. C = SE, O = Tullverket, OU = Swedish Customs, OU = Root Certificate Authority, SERIALNUMBER = SE2021000969, CN = Swedish Customs Public Root CA 1.0
subjectPublicKeyInfo	Signature algorithm and public key encoded according to RFC 5280
authorityKeyIdentifier	non-critical, see Section 7.5 and RFC 5280
subjectKeyIdentifier	non-critical, see RFC 5280
keyUsage	critical. The following bits must be set: *keyCertSign, cRLSign*
basicConstraints	critical. The field has two subfields: `cA`= TRUE; pathLenConstraint not specified

7.3 CA certificate

Key length and validity period
RSA-key with a length of 2048 bits.
Period of validity: 10 years.

Certificate fields

Certificate fields	Comments
version	X.509 version 3 (value = 2)
serialNumber	Unique number for each certificate issued by the CA (Issuer)
signatureAlgorithm	sha1WithRSAEncryption
issuer	Issuer is the same as subject in the root certificate
validity	See RFC 5280
subject	Organisation for which the certificate is issued. Used for signing companies signature certificates: C = SE, O = Tullverket, OU = Swedish Customs, OU = Public Intermediate Certificate Authority, OU = Only for authorized use, SERIALNUMBER = SE2021000969, CN = Swedish Customs Public CA 1.0 Used for signing the Swedish Custom's signature certificates: C = SE, O = Tullverket, OU = Swedish Customs, OU = Internal Intermediate Certificate Authority, OU = Only for authorized use, SERIALNUMBER = SE2021000969, CN = Swedish Customs Internal CA 1.0
subjectPublicKeyInfo	Signature algorithm and public key encoded according to RFC 5280
authorityKeyIdentifier	non-critical, see Section 7.5 and RFC 5280
subjectKeyIdentifier	non-critical, see RFC 5280
keyUsage	critical. The following bits must be set: *keyCertSign, cRLSign*
certificatePolicies	non-critical. OID which identify the certificate policy used for the certificate.
basicConstraints	critical. The field has two subfields: cA= TRUE; pathLenConstraint = 0

7.4 Signature certificate

Key length and validity period
RSA-key with a length of 2048 bits.
Period of validity: 14 month.

Certificate fields

Certificate fields	Comments
version	X.509 version 3 (value = 2)
serialNumber	Unique number for each certificate issued by the CA (Issuer)
signatureAlgorithm	sha1WithRSAEncryption
issuer	Issuer is the same as subject in the intermediate CA certificate
validity	Se RFC 5280
subject	Organisation for which the certificate is issued. Example for signature certificate for a company: C = SE, O = Example import and export, OU = IT department, SERIALNUMBER = SE1122334455, CN = Eximpexp Example for signature certificate for Swedish Customs: SERIALNUMBER=SE2021000969, O=Tullverket, C=SE, OU=Swedish Customs, CN=Tullverket EDI
subjectPublicKeyInfo	Signature algorithm and public key encoded according to RFC 5280
authorityKeyIdentifier	non-critical, see Section 7.5 and RFC 5280
subjectKeyIdentifier	non-critical, see RFC 5280
keyUsage	critical. The following bit must be set: *nonRepudiation*
certificatePolicies	non-critical. OID which identify the certificate policy used for the certificate.
basicConstraints	critical. The field has two subfields: cA= FALSE; pathLenConstraint ej angivet
cRLDistributionPoints	non-critical. This field contains a pointer to the CRL

7.5 authorityKeyIdentifier

One step in the control of a document's signature is to verify that the certificate used to create the signature is correct. This also includes validation of the certification path above the signature certificate up to the root certificate.

The certificate field *authorityKeyIdentifier* is used to uniquely identify the parent certificate used to sign a certificate. This field is divided into the following subfields (see RFC 5280):

Subfield	Comments
keyIdentifier	Contains a checksum of the parent certificate’s public key.
authorityCertIssuer	Issuer of the parent certificate
authorityCertSerialNumber	Certificate serial number for parent certificate

The subfield *keyIdentifier* is used for signature certificates issued by Swedish Customs.

To verify the signature, the recipient must have access to the sender's signature certificate. In the Swedish Customs' implementation of the EDIFACT format, no signature certificate is included in the AUTACK message (see Section 6) but must be downloaded. However, the AUTACK message includes certificate serial number, *serialNumber*, and reference to the CA, *authorityKeyIdentifier [keyIdentifier]*. The fields *serialNumber* and *authorityKeyIdentifier [keyIdentifier]* uniquely identify the certificate used to sign the document which is necessarily to select the correct certificate.

Root certificate, intermediate CA certificates and Customs’ signature certificate can be downloaded from Swedish Customs' website, www.tullverket.se.

8 Appendix B: CSR file – description and examples

The purpose of the examples below is to show some different ways to create a CSR. The section is at a relatively deep technical level and is therefore primarily targeted at technical professionals who will implement the management of CSR files in its system. *Information in the section should be seen as guidance and not as precise instructions for the implementation.*

In the examples the following company information are used:

countryName	SE
organizationName	Example import and export
organizationalUnitName	IT-department
serialNumber	SE1122334455
commonName	Eximpexp

The CSR is a text file. The following is an example, created from the information above:

```
-----BEGIN CERTIFICATE REQUEST-----
MIICuDCCAaACAQAwczELMAkGA1UEBhMCU0UxIjAgBgNVBAoTGUV4YW1wbGUgaW1w
b3J0IGFuZCBleHBvcnQxFjAUBgNVBAsTDUlUIGRlcGFydG1lbnQxFTATBgNVBAUT
DFNFMTEyMjMzNDQ1NTERMA8GA1UEAxMIRXhpbXBleHAwggEiMA0GCSqGSIb3DQEB
AQUAA4IBDwAwggEKAoIBAQD5iVkD/dcGo3Vy9L9hT4FH4e400+2wma8CJ+0dmT2k
FsHzuwfWnUD8R433BemmxIs+3aglkgbMr8yV74xtBMldW63NUADYOPwJ87o07UGw
JSq6Ql9iIK//srPDbIpvJCv/Ns9GKM54HuI3zLGN8FGPKDpN9rxoD5gAx7rhK7oj
ANZPemGydaRtIlDSFfiGnZcjvK9tz/XzvOKTgGaqBydSnWaUhul+2noy9fkjcn7d
bxHbwqMZfyEPEO+Hxxu8bSrxtodSJDzLRBrhYM/bF0oTwF7AnrXafl3vYzvClWT5
B8ylKmZl/MP4csQ+nn1eUQe9lILR9tt+EA+xdxMqCStzAgMBAAGgADANBgkqhkiG
9w0BAQUFAAOCAQEAavdGqU8ToG+/NwrA0DyoR30zg9YQTfYcKgc5KztjelDdbovG
RbSyfKis05u7V2Re3VDe3Oy3fArnab+/1mavLkVuVTmhjEGAlaCbC5abI7tZewaU
NquTAKKVhYTBf3/XvHpNZJEzKEQ/yrytiyu6kdzZyvORLejhWoATzAOjudPlzy3/
kBqf3B/YafeJMJ6JMyHHjMFr5AF8vLFFe7PqjjALrSno1fr/TKNE80IGHxvEKvqh
8tgIvLF0CJSaOjKWiH7EdxLECksBN09k/3oDUQtExnUmtUQOqVhnpg4zj9EKcP6m
FJ2qb9gJtvTU+7MsF6mF0dEjTlr0/q8kV/RWaw==
-----END CERTIFICATE REQUEST-----
```

The contact person at the company shall copy the entire plain text from the CSR file into an email message and send it to edi.certifikat@tullverket.se. Name and EORI number shall be specified in the email subject line.

The content of the CSR file in plain text shall be copied into a document with the title “Ordering of signature certificates” and the company name and EORI-number shall be specified. A printout of the document shall be signed by the contact person (including name spelled out) and sent by postal mail to:

Swedish Customs, IT department
EDI Certificate
Aurorum 3
SE-977 75 Luleå
SWEDEN

The signed letter is necessary to legally associate the contact person to the issued signature certificate.

8.1 OpenSSL

OpenSSL is available for many different computing environments and is open source. Documentation of OpenSLL can be downloaded from www.openssl.org.

Command line request to create a CSR:

```
openssl req -newkey rsa:2048 -keyout example.key -out example.csr
-subj "/countryName=SE/organizationName=Example import and export
/organizationalUnitName=IT department/serialNumber=SE1122334455/
commonName=Eximpexp"
```

When you run this command you will be asked to enter a password to protect the private key. In the command example above, the CSR is stored in the file *example.csr* and the private key in *example.key*.

OpenSSL can also be used to display the contents of a CSR:

```
openssl req -text -noout -in example.csr
```

Note that this presentation has limitations that make it hard to detect some errors in the subject field of the certificate.

Another utility in the openssl package is *asn1parse,* which can be used to show in detail the contents of the CSR. Through this, errors can be detected that are not detected via *req*.

```
openssl asn1parse -in example.csr.
```

Via "asn1parse" it is possible to check that the *serialNumber* is a separate object, see *OBJECT* in the example below.

The file *exemple.csr* is a correct CSR while the CSR *incorrect.csr* contains errors. The program *req* will however present the same content of *subject* for both these files. When *asn1parse* is used, the error in *incorrect.csr* can be identified, see below.

Output based on a correct CSR:

```
openssl asn1parse -in example.csr
    0:d=0  hl=4 l= 696 cons: SEQUENCE
    4:d=1  hl=4 l= 416 cons: SEQUENCE
    8:d=2  hl=2 l=   1 prim: INTEGER           :00
   11:d=2  hl=2 l= 115 cons: SEQUENCE
   13:d=3  hl=2 l=  11 cons: SET
   15:d=4  hl=2 l=   9 cons: SEQUENCE
   17:d=5  hl=2 l=   3 prim: OBJECT            :countryName
   22:d=5  hl=2 l=   2 prim: PRINTABLESTRING   :SE
   26:d=3  hl=2 l=  34 cons: SET
   28:d=4  hl=2 l=  32 cons: SEQUENCE
   30:d=5  hl=2 l=   3 prim: OBJECT            :organizationName
   35:d=5  hl=2 l=  25 prim: PRINTABLESTRING   :Example import and export
   62:d=3  hl=2 l=  22 cons: SET
   64:d=4  hl=2 l=  20 cons: SEQUENCE
   66:d=5  hl=2 l=   3 prim: OBJECT            :organizationalUnitName
   71:d=5  hl=2 l=  13 prim: PRINTABLESTRING   :IT department
   86:d=3  hl=2 l=  21 cons: SET
   88:d=4  hl=2 l=  19 cons: SEQUENCE
   90:d=5  hl=2 l=   3 prim: OBJECT            :serialNumber
   95:d=5  hl=2 l=  12 prim: PRINTABLESTRING   :SE1122334455
  109:d=3  hl=2 l=  17 cons: SET
  111:d=4  hl=2 l=  15 cons: SEQUENCE
  113:d=5  hl=2 l=   3 prim: OBJECT            :commonName
  118:d=5  hl=2 l=   8 prim: PRINTABLESTRING   :Eximpexp
  128:d=2  hl=4 l= 290 cons: SEQUENCE
  132:d=3  hl=2 l=  13 cons: SEQUENCE
  134:d=4  hl=2 l=   9 prim: OBJECT            :rsaEncryption
  145:d=4  hl=2 l=   0 prim: NULL
  147:d=3  hl=4 l= 271 prim: BIT STRING
  422:d=2  hl=2 l=   0 cons: cont [ 0 ]
  424:d=1  hl=2 l=  13 cons: SEQUENCE
  426:d=2  hl=2 l=   9 prim: OBJECT            :sha1WithRSAEncryption
  437:d=2  hl=2 l=   0 prim: NULL
  439:d=1  hl=4 l= 257 prim: BIT STRING
```

Output based on an erroneous CSR:

```
openssl asn1parse -in incorrect.csr
    0:d=0  hl=4 l= 699 cons: SEQUENCE
    4:d=1  hl=4 l= 419 cons: SEQUENCE
    8:d=2  hl=2 l=   1 prim: INTEGER           :00
   11:d=2  hl=2 l= 118 cons: SEQUENCE
   13:d=3  hl=2 l=  11 cons: SET
   15:d=4  hl=2 l=   9 cons: SEQUENCE
   17:d=5  hl=2 l=   3 prim: OBJECT            :countryName
   22:d=5  hl=2 l=   2 prim: PRINTABLESTRING   :SE
   26:d=3  hl=2 l=  34 cons: SET
   28:d=4  hl=2 l=  32 cons: SEQUENCE
   30:d=5  hl=2 l=   3 prim: OBJECT            :organizationName
   35:d=5  hl=2 l=  25 prim: PRINTABLESTRING   :Example import and export
```

```
    62:d=3  hl=2 l=  48 cons: SET
    64:d=4  hl=2 l=  46 cons: SEQUENCE
    66:d=5  hl=2 l=   3 prim: OBJECT            :organizationalUnitName
    71:d=5  hl=2 l=  39 prim: PRINTABLESTRING   :IT
 department/serialNumber=SE1122334455
   112:d=3  hl=2 l=  17 cons: SET
   114:d=4  hl=2 l=  15 cons: SEQUENCE
   116:d=5  hl=2 l=   3 prim: OBJECT            :commonName
   121:d=5  hl=2 l=   8 prim: PRINTABLESTRING   :Eximpexp
   131:d=2  hl=4 l= 290 cons: SEQUENCE
   135:d=3  hl=2 l=  13 cons: SEQUENCE
   137:d=4  hl=2 l=   9 prim: OBJECT            :rsaEncryption
   148:d=4  hl=2 l=   0 prim: NULL
   150:d=3  hl=4 l= 271 prim: BIT STRING
   425:d=2  hl=2 l=   0 cons: cont [ 0 ]
   427:d=1  hl=2 l=  13 cons: SEQUENCE
   429:d=2  hl=2 l=   9 prim: OBJECT            :sha1WithRSAEncryption
   440:d=2  hl=2 l=   0 prim: NULL
   442:d=1  hl=4 l= 257 prim: BIT STRING
```

8.2 Windows certreq

In a Windows environment, the program *certreq* can be used to create a CSR. Documentation can be found at http://technet.microsoft.com/en-us/library/cc725793(WS.10).aspx for Windows Server 2008 and at http://technet.microsoft.com/en-us/library/cc736326(WS.10).aspx for Windows Server 2003.

Create the configuration file (policy file) *example.inf* with contents as the following example:

```
 [NewRequest]
KeyLength=2048
RequestType=PKCS10
Subject="C=SE, O=Example import and export, OU=IT department,
serialNumber=SE1122334455, CN=Eximpexp"
Exportable = TRUE ; TRUE = Private key is exportable
SMIME = FALSE
```

Then run the following command to create a key pair and a CSR:

```
certreq -New example.inf example.csr
```

See also http://technet.microsoft.com/en-us/library/cc736326(WS.10).aspx for a description of *certreq* and its configuration file.

The command *certutil* can be used to check the CSR:

```
certutil -dump example.csr
```

Example of results from *certutil*:

```
PKCS10 Certificate Request:
Version: 1
Subject:
    C=SE
    O=Example import and export
    OU=IT department
    SERIALNUMBER=SE1122334455
    CN=Eximpexp
Public Key Algorithm:
    Algorithm ObjectId: 1.2.840.113549.1.1.1 RSA
    Algorithm Parameters:
    05 00
Public Key Length: 2048 bits
Public Key: UnusedBits = 0
    0000  30 82 01 0a 02 82 01 01  00 f5 36 cf c3 e4 a9 27
    0010  91 5b 4c 72 a4 45 81 39  ac 9c da f8 b4 93 af 6c
```

8.3 Java

Java *keytool* is available for many different computing environments.
Documentation of Java *keytool* can be downloaded from:
http://download.oracle.com/javase/6/docs/technotes/tools/index.html#security

Run the following command to create a key pair:

```
keytool -genkeypair -alias SE1122334455 -keyalg RSA -keystore
keystore.jks -keysize 2048 -dname "C=SE, O=Example import and export,
OU=IT department, serialNumber=SE1122334455, CN=Eximpexp"
```

Run the following command to create a CSR:

```
keytool -certreq -alias SE1122334455 -keystore keystore.jks
-file example.csr
```

Check of CSR can be made by e.g. *openssl req*, *openssl asn1parse* or Windows *cerutil –dump* (see 8.1 and 8.2).

9 Appendix C: Hexadecimal and Base64 encoding

9.1 Hexadecimal encoding

Hexadecimal encoding (also called Base16-encoding) is used to store binary data as alphanumeric characters.

The data is divided into groups of 4 bits. Each 4-bit group is converted to an alphanumeric character (0-9, A, B, C, D, E or F), representing the hexadecimal value. Each octet is thus represented by two alphanumeric characters.

In the EDIFACT encoding format, the 'Filterfunction 0505' is set to 2 to indicate that a hexadecimal filter is used for encoding.

Hexadecimal encoding is described in Section 8 of RFC 4648, "The Base16, Base32, and Base64 Data Encodings".

Example

The decimal number 31,420 corresponds to the binary 16-bit number 0111 1010 1011 1100. In hexadecimal encoding, this is represented by the four alphanumeric characters 7 A B C.

9.2 Base64 encoding

Base64 encoding is used to store binary data as alphanumeric characters. The Base64 encoding results in fewer alphanumeric characters than the hexadecimal encoding and is used instead of hexadecimal encoding when compression of the data is desired to save space.

In the EDIFACT encoding format, the 'Filterfunction 0505' is set to 7 to indicate that Base64 encoding has been used.

Base 64 encoding is described in Section 4 of RFC 4648, "The Base16, Base32, and Base64 Data Encodings".

Example

Firstly, the data is divided into groups of 24 bits (3 octets). If the binary number cannot be evenly divided into 24-bit groups, additional characters (padding) have to be added at the end.

The 24-bit groups are then divided into 4 x 6 bits. Each 6-bit group is assigned a character based on the table below.

Hex	Character	Hex	Character	Hex	Character	Hex	Character
0	A	10	Q	20	g	30	w
1	B	11	R	21	h	31	x
2	C	12	S	22	i	32	y
3	D	13	T	23	j	33	z
4	E	14	U	24	k	34	0
5	F	15	V	25	l	35	1
6	G	16	W	26	m	36	2
7	H	17	X	27	n	37	3
8	I	18	Y	28	o	38	4
9	J	19	Z	29	p	39	5
A	K	1A	a	2A	q	3A	6
B	L	1B	b	2B	r	3B	7
C	M	1C	c	2C	s	3C	8
D	N	1D	d	2D	t	3D	9
E	O	1E	e	2E	u	3E	+
F	P	1F	f	2F	v	3F	/

In the following example, we use a 160-bit binary number:
00:12:87:EC:A7:BD:25:20:2D:6D:2B:F5:5B:3D:1E:D7:86:07:BB:67
In the example, the colon (:) is used only to improve the readability.

Divided into groups of 3*8 = 24 bits:

```
00:12:87 =    0000 0000   0001 0010   1000 0111
EC:A7:BD =    1110 1100   1010 0111   1011 1101
25:20:2D =    0010 0101   0010 0000   0010 1101
6D:2B:F5 =    0110 1101   0010 1011   1111 0101
5B:3D:1E =    0101 1011   0011 1101   0001 1110
D7:86:07 =    1101 0111   1000 0110   0000 0111
BB:67:00 =    1011 1011   0110 0111   0000 0000
```

where the last 8 bits (00) in the last group are padding.

Regrouping into groups of 4*6 = 24 bits represented as hexadecimal numbers:

```
000000  000001  001010  000111 = 00:01:0A:07
111011  001010  011110  111101 = 3B:0A:1E:3D
001001  010010  000000  101101 = 09:12:00:2D
011011  010010  101111  110101 = 1B:12:2F:35
010110  110011  110100  011110 = 16:33:34:1E
110101  111000  011000  000111 = 35:38:18:07
101110  110110  011100  000000 = 2E:36:1C:00
```

Conversion of the 6-bit hexadecimal numbers into alphanumeric characters in accordance with the table:

```
00:01:0A:07 = ABKH
3B:0A:1E:3D = 7Ke9
09:12:00:2D = JSAt
1B:12:2F:35 = bSv1
16:33:34:1E = Wz0e
35:38:18:07 = 14YH
2E:36:1C:00 = u2c=
```

The result from the example is the following 28-character alphanumeric number:
ABKH7Ke9JSAtbSv1Wz0e14YHu2c=
(“=” in the end indicates that there is a padding character included).

Tullverket

Box 12854, 112 98 Stockholm
Telefon: 0771-520 520
tullverket.se