Swedish Customs
Managing the Trade
Lars-Gunnar Nilsson
Ph. +46 31 63 35 27
lars-gunnar.nilsson@tullverket.se

Date
19 March 2012
Your date

Our reference
STY 2012-240
Your reference

Developers, suppliers or Authorisation holders of a customs system with EDI to Swedish Customs

Version 2.0 - 4th of January 2012 – New security concept and update
Version 2.1 – 19th of January 2012 - Adjustment two component solution
Version 2.2 - 19th of March 2012 - Translation and for publishing

Guidelines for "Certificate of Security Handling during Information Exchange via EDI"

Introduction

Because so many different concepts exist, in this documentation we have consistently used the designation:

- The "system owner" for the legal entity that is normally drawing up a system description. This indicates who owns or controls the source code or in some other way is the entity best suited to drawing up a system description.
- The "permit holder" indicates the legal entity that uses a system in order to draw up customs declarations and determines which individuals among the personnel that are allowed to issue and sign an electronic document on behalf of the company.

A system description, or reference made to one already approved, and also a certificate of the permit holder's security handling must be appended to an application for a permit for electronic information submission, or at the latest before Swedish Customs can issue a production permit.

The system description is normally drawn up by the system owner of a standard system, or a system unique to the company, which is to submit or receive electronic documents to or from Customs. The system owner has the best competence to describe how the system and functions satisfy the requirements of Customs. Special guidelines to perform a system description are provided separately.

A permit holder who wishes to be granted a production permit must submit a **"Certificate of Security Handling during Information Exchange via EDI"** to Customs. This is suitably done once training and tests have been carried out, so that the company can handle the system and is competent to submit electronic documents to Customs.

The permit holder is the most competent person to draw this up, as the person responsible to Customs for knowing, complying with and maintaining the security instructions in accordance with **"Guidelines and Instructions relating to Security during Information Exchange via EDI"**. Following the issue of a production permit, changes may be made both to the system and to the Customs regulatory framework or guidelines. In this event, an updated certificate constitutes a confirmation to Customs that the permit holder is about to carry out or has carried out the change.

The authorised signatory/-ies for the permit holder must appoint a contact for security for the information exchange with Customs. We call this person the security contact person, SKP. The SKP must become familiar with the rules and functions for protecting the company's information with the aid of the customs system and shall be prepared to assist Customs on these issues. The SKP is the person who is responsible vis-a-vis Customs for the handling of

the two-component solution for the users who are authorised to submit electronic documents in notices of security category 2. The SKP is also the person that Customs will ask if necessary about the user identity for submitted electronic documents.

In conjunction with Customs introducing a new security concept based on PKI certificates, a new concept was also introduced: one or several contacts that have been granted authority to handle signing certificates, CKP. The CKP can be the same or another person than the SKP, but the responsibility and the contacts relate to different purposes and we often use different concepts for the roles. It is the Customs IT Department that communicates with CKP.

The system owner can supply the permit holder with a template text for the certificate that is adapted to the prerequisites of the system, or else the permit holder can draw up the certificate him-/herself.

These guidelines for the drawing up and contents of the certificate are intended to make it easier for the permit holder and for Customs to check, compare and assess certificates from various permit holders with the same system in a more uniform and competition-neutral basis.

Design and contents of a "Certificate of Security Handling during Information Exchange via EDI"

General instructions
If the certificate does not comply with these guidelines, one or several adjustment or supplementation cycles may be necessary before the certificate can be assessed for approval.

In its final version, the certificate shall normally be in Swedish, but certificates in English may be approved, after individual assessment, for foreign permit holders.

A permit holder may use one or several customs systems for submitting electronic documents to Customs. A permit holder can also submit electronic documents to Customs using various communication channels connected to Customs' clearing-house function, TMF. The technical appendix/-ces to the permit shows the communication channels the company uses. For each technical appendix, the permit holder needs to provide a certificate, as the systems and terms may differ.

*See also our document "**Guidelines and instructions relating to security during information exchange via EDI**" at www.tullverket.se/Innehåll A-Ö/Säkerhet vid informationsutbyte via EDI.*

Customs places great emphasis on this document and certificate providing satisfactory protection, both from a legal and a technical point of view, for the company and the individual issuing an electronic document.

The security in this instance relates to processes, both manual and computerised, for the handling of:

- *so-called signing certificates,*
- *the technical method for reinforced authority and identity control,*

relating to how security is complied with by both the system owner (system supplier/manufacturer) and the company (permit holder).

Below follow instructions that facilitate the drawing up of a "Certificate of Security Handling during Information Exchange via EDI".

"Certificate of Security Handling during Information Exchange via EDI"

The "Certificate of Security Handling during Information Exchange via EDI" shall be issued on the permit holder's letterhead paper.

The certificate shall start with:

- The permit holder's registered name
- Corporate identity number or the corresponding registration identity
- The EORI number
- The registration number of the permit
- The permit's technical appendix (number) to which the certificate relates (the permit may have several technical appendices)
- The system name
- Version
- System owner.

Handling of signing certificates

- You and either confirm that you will handle the signing certificate using support from the customs system, in accordance with Chapter 10.2.1.1-10.2.1.2 in the system description, or you can confirm that the handling will be carried out without support from the customs system.

Handling of reinforced authority and identity control

This applies in case you are handling a message of security category 2 in accordance with the **"Guidelines and instructions relating to security during information exchange via EDI".**

- You should either confirm that the technical method for reinforced authority control is handled according to the system description, Chapter 10.2.2.2, or
  you can replace the current Chapter 10.2.2.2 with your description how the adaptation has been done and how the handling with the technical method chosen by you satisfies the requirements.

- Describe how you as SKP introduce the administrator to:
  - the customs system's function for authority and identity control,
  - how the user in a secure way is allocated the two components for identification in the system,
  - how to protect the issuer identity.

Special adaptations

If there is integration between other systems where data from these system is used in customs declarations, this shall be briefly described here.

If so, describe whether this data is checked (validated according to the terms and conditions for customs declarations) in the other systems or in conjunction with the declaration being drawn up in the system the certificate relates to.

It may be necessary to describe the information transferred to the customs system and, if requested, clarify this with a file description, for example.

The permit holder's contact and means of contact

Please state the name, postal address, telephone and email of the contacts at the company, to which Customs may address any questions.

- Customs manager (contact for issues relating to the permit)
- System manager (contact for issues relating to system use)
- Security contact (contact for issues relating to authority control and provision of identity information according to Section 5.1 requirement 4 in **"Guidelines and Instructions relating to Security during Information Exchange via EDI"**)

Certification and signature

The company's security contact shall certify that:

- they have read the entire system description from system owner X, on date YYMMDD, document version X – relating to system X, system version X,
- the system description corresponds to the system installed,
- they will be submitting a new "Certificate of Security Handling during Information Exchange via EDI" if any changes are to be introduced that affect this certificate,
- they will notify Customs when a new security contact is appointed (certified by authorised signatory),
- they will notify Customs when other contacts or means of contact change.

The "Certificate of Security Handling during Information Exchange via EDI" shall be signed by the permit holder through the security contact appointed by the authorised signatory together with name in block letters and date.

The original of the "Certificate of Security Handling" shall be submitted by post to Tullverket, EDI-tillstånd, Box 12854, SE-112 98 Stockholm, Sweden.