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

Date
5th of December 2012
Your date

Our reference
STY 2012-240
Your reference

Developers, suppliers of systems supporting EDI to Swedish Customs

Version 2.0 - 4th of January 2012 – Security concept based on PKI and update
Version 2.1 - 9th of January 2012. – Adjustment of technical method and correction
Version 2.2 - 19th of March 2012 - Translation and for publication
Version 2.3 – 5th of December – notification of local clearance import and export

Guidelines for system description EDI permit

Introduction

A system description or reference to a system description that has been approved following assessment must be appended to an application for a permit for electronic information submission, or at the latest before a decision about a production permit can be made.

This document is directed at suppliers of standard systems or for systems unique to a company. These guidelines are aimed at detailing what must be described regarding a system intended to submit and/or receive electronic documents to and from Swedish Customs in order for the description to be approved.

With these guidelines for system descriptions, Customs will receive the same format and information for all systems, which facilitates checking, comparing and assessing descriptions from various suppliers on a competition-neutral basis.

First we check whether the system description entirely complies with these guidelines in terms of format and information; if not, we provide suggestions for adjustment or supplement in a new document version.

When a system description complies with these guidelines, Customs makes an assessment whether the system description can be approved. In this assessment, we also consider whether the limitations or differences reported can be accepted. If not, certain parts of the system may need to be improved in order to be approved.

Once the system description has been approved, the system owner is notified of this. A company applying for a permit does thereafter not have to attach the system description to an application if reference is made to an approved document version of the system description.

A supplier of a standard system can also be subjected to a more in-depth assessment of the system for a group of messages (technical regulatory framework) in order to get the system approved for the technical regulatory framework in question. Such systems are published on Customs' website www.tullverket.se. Companies applying for a permit for messages within this regulatory framework with an "Approved X System" do not have to carry out the final tests normally required, but will instead receive a production permit following a simple procedure for safeguarding that the company can go into production.

In conjunction with an assessment of a system description, or at a later stage, Customs may have reason to compare the system in production with the system description submitted. If the description does not correspond to the

system in production, the company's permit for electronic submission of information and the system supplier's system status of "Approved" may be reassessed.

These guidelines are not static, but will change in the light of new experience, changes in technical development or Customs' methods and continued development of electronic messages. In the event of significant changes of these guidelines, the system suppliers will be granted a transition period during which to adapt their systems and descriptions.

Purposes of guidelines and approval of system description

- Basis for ensuring fundamental requirements that safety, certain functions and qualities will be ensured before electronic documents are exchanged between companies and Customs.
- Basis for decision about production approval of permit.
- Competition-neutral design of and contents of system description.
- Competition-neutral assessment of system description.
- Reduces error and administrative burden related to external systems.
- Basis for the permit holder (information provider) to facilitate understanding and an opportunity to monitor compliance with Customs' guidelines on:
  - own maintenance of function and security according to system description
  - system and description corresponding in relation to fundamental requirements, including after production approval
  - the extent to which the system supports requirements and wishes from Customs.

At the same time, they form the basis for Customs to increase their knowledge about external systems for:

- Customs' issuing of permits (in the design of tests, final tests and the design and contents of system descriptions),
- Customs' monitoring (that fundamental requirements are complied with once a production permit has been issued),
- Customs' support function (for facilitating support for the effects on external system),
- Customs' technical and functional managers (during maintenance of Customs' internal system and communication about effects on external systems),
- Customs' development projects (in their effects on external systems, communications and data messages).

Who is responsible for ensuring the system documentation is drawn up, is correct and is maintained?

Systems that are to communicate with Customs may be developed, compiled, sold, receive support and training and also maintained in many different ways and by various actors.

Standard systems
So-called standard systems make up a very large proportion and are characterised by containing general system functions that are marketed to companies in general. The system owner who develops a standard system usually owns the source code, but sells licences for the right to use the system, often with a time limit. This system owner also ultimately decides on any measures to be undertaken in the system.

The purchaser (permit holder) of a standard system is therefore dependent on his system owner in order to receive system functions, corrections, maintenance and development. The system owner of a standard system is therefore the person Customs in the first instance considers to be the most suitable to draw up and maintain system documentation for a standard system.

According to the foregoing, it emerges that a retailer of a standard system normally cannot be qualified to draw up and maintain system documentation, unless it is clearly shown who the actual system owner is, and that the retailer is producing the system documentation on behalf of the system owner.

For the same reason, a wholly or partly owned subsidiary or affiliated company of the company that owns the right to the source cannot draw up and maintain system documentation, unless it is clearly shown who the actual system owner is and that the group company is producing the system documentation on behalf of the system owner.

Some standard systems are supplied with various system functions and services from several suppliers. In some cases, there is an agreement that the subcontractor becomes a part supplier that invoices its services direct to the permit holder. If these system functions impinge on the functions requested by Customs in this system documentation, the interfaces between the systems shall be described and each supplier describe its system functions separately.

Systems unique to a company
A smaller proportion of systems are so-called in-house development systems or systems unique to a company. For these systems, it is the purchaser (permit holder) who decides on and pays for any changes. In-house development systems are characterised by being developed or adapted

specially for a company or group of companies. The system as a whole may be developed using the company's own resources, or may be a compilation of various purchased system functions and consultancy services.

This system category also includes standard systems that have been changed so significantly that they are no longer included in the system supplier's normal agreement regarding undertaking maintenance, support and further development; instead, this is only done following an order from the permit holder, and on the permit holder's behalf.

The purchaser (permit holder) of an in-house development of a standard system is therefore the person Customs in the first instance considers to be the most suitable to draw up and maintain system documentation for an in-house development system.

Because there are so many different actors, in this documentation we have consistently used the designation:

- The "system owner" is 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.

.

Design and contents of a system description

General instructions

The system description should initially be sent by email to *edi.tillstand@tullverket.se* for checking and assessment. *The system description shall be attached in Word or pdf format.*

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

Each new documentation of the system description shall therefore have its own unique version number and date. A unique document version makes it possible for Customs, the system supplier or permit holder to refer to the correct version that is being checked, assessed or has been approved.

Only after approval has been notified to the system owner shall the system description be printed out as an original on the supplier's letterhead paper, signed by an authorised signatory for the company and sent by post to Swedish Customs.

In its final version, the system description shall be in Swedish. Exemptions may be granted after special assessment, in the first instance for systems unique to a company.

A system description shall consist of the following chapter arrangement in order to be assessed and approved. There is reason for each chapter to be described separately; if you feel that a description would be repeated, this is not our intention – please contact us for clarification.

Please do not refer to any other chapter, instead provide an exhaustive answer or example of user interface within the chapter in question.

This instruction is based on a standard system. For in-house development systems in particular, certain chapters may be entirely irrelevant; if so, please state "not applicable". This may also apply to specialised systems, such as system support for Entry Summary Declaration, SID.

Chapter 1-5 are intended to provide Customs with an overall understanding. Please keep these chapters factual and brief. Please avoid any sales argument in the description of the system, but focus on the information you deem to be of interest to Customs. If necessary, we will ask you to supplement or clarify the information.

All systems change over time with updates made for various reasons. Only when changes are made that impinge on the approved system description

may there be a need to update this as well. Please contact us if you have any doubts. Just because a system in production may have a higher system version than that shown in the system description there is no reason to update it with a new document version.

1. System owner

1.1. **Company**
Describe the company, its operation, history, organisation and any affiliation to a group of companies.

1.2. **Customs competence**
Describe the personnel with customs competence, their training or corresponding experience.

1.3. **Contacts**
State the means of contact, such as postal address, telephone and email of:
1.3.1. System manager (overall)
1.3.2. Support manager (vis-a-vis the permit holder)
1.3.3. Training manager (vis-a-vis the permit holder)
1.3.4. Maintenance manager
(Customs system/EDIFACT/communication
1.3.5. Development manager
(Customs system/EDIFACT/communication)
that Customs can contact or refer users to.

2. System

2.1. **Version**
2.1.1. What is the system called, the customs module?
2.1.2. What version is used for the system description?
2.1.3. How is the version being used shown to the user? See Chapter 16 index instruction - a).

2.2. **Type of system**
2.2.1. **Category**
Describe the type of system, for example:
- a standard system,
- a system core with a requirement for company adjustment,
- a system support developed or compiled in-house for a certain company or group of companies, or
- a system or program module that mechanically processes and supplies data to and from other systems.

2.2.2. **Conditions**
Describe if the permit holder has any conditions for where and how the system is installed, or where information is processed, for example:

- The permit holder can freely choose the computer and location where the system is installed and is himself responsible for all day-to-day operating procedures.

- The permit holder has certain limitations on choosing the computer and location where the system is installed or where information is processed.

  Describe the reason. For example, a condition for use requires that certain services are carried out by the system owner or that information supply is processed in other systems.

- The permit holder has no opportunity to choose the computer or location where the system is installed, and the system owner is responsible for operation.

  Describe why. For example, an ASP solution (Application Service Provider).

- The permit holder shall summarise information and this is transferred to a so-called IT Service Provider, who converts the information to message format, signs it and transfers it according to Customs' regulatory framework.

2.3. System support

2.3.1. Area of use

Describe briefly the main scope of the system and the customs areas the system supports (import, export, transit, etc.). If information is not entirely created within the system, describe the interaction with other systems.

2.3.2. Electronic transfer

Give an overall description of the way in which the system processes electronic information exchange between the permit holder and Customs; from the position where the user requests information to be sent until a response message has been received and the information has been processed.

2.3.3. Modules

Attach a summary diagram of the system's compilation of modules and /or connections that facilitates the understanding of the system's construction.

If the system support, for the customs area, in turn is divided up into several modules, for example export, import or transit,

please specify what modules the system offers and their functions in brief.

3. System components

3.1. **Computer environment**
Describe the environment/s the system is intended to be used in, mini computer and operating system, PC server, PC stand-alone, Citrix, etc.

3.2. **System configuration**
Attach a schematic summary diagram of a normal configuration consisting of the components (see also 3.3) that are needed in total for submission of information, the system, the user and communication with Customs' clearing-house function TMF.

3.3. **Components**
Explain the components included in the summary diagram, including those that may be outside the system licence but which are a prerequisite. For example, for communication with TMF: EDIFACT program, file transfer protocol, network service to VAN/TMF, application for signature and technical methods for reinforced authority or identity control.

3.4. **External components**
Describe which of these components for which the system owner does not have complete operational, support or maintenance responsibility, or the cost of which is offset direct vis-a-vis the permit holder.

4. Maintenance, support and training

Describe conditions, availability and limitations for the permit holder in relation to:
4.1. support,
4.2. maintenance and
4.3. training for the system.

For example, is each service included within certain limits against an annual fee, against a fee for time spent or period only against quotation? Please describe clearly enough that it is shown where or when the system owner's responsibility converts into a paid service.

If any of these services are not carried out or offered by the system owner, it is important to describe who carries out the service.

5. Updates and means of distribution

Describe in detail how the system is updated with changes to the program and database respectively. For example:

- The program package is made available on the system owner's resource of type central server or website. The system installed at the permit holder's checks automatically if any system changes have occurred and, if so, downloads and installs both program and database. The entire process normally occurs without any need for participation from either the permit holder or the system owner.

- A program packet with changes is notified to the permit holder, who is encouraged to carry out the update by downloading it from a central server or website, or distributed electronically or on a medium of type CD. Installation is carried out via an installation program that is handled independently by the permit holder, normally without any need for interaction with the system owner.

- Program changes are distributed as above, but changes in the database may only be carried out by the system owner and are usually done remotely via a link to the permit holder's installation.

- Program and database changes may only be carried out by the system owner. The changes are always made on location.

6. Handling of tests and final tests

The permit holder must have the opportunity to send messages to Customs' company testing environment instead of the production environment. This is in order to carry out own testing, final tests for messages and for training purposes. Such messages shall include an indicator that it is a test message.

An indicator in a message states that the transfer is a test, and it is then processed in Customs' company testing environment and not in the production environment. In the same way, the indicator is returned in a response message to enable the permit holder's system to process a production message differently from a test message.

To avoid any mix-up, the system must also show the user very clearly the difference between customs transactions and messages in testing or production.

6.1. Describe in detail how a test indicator is applied in outgoing messages, and how it is handled in incoming answers. How are tests carried out, in parallel operation with both production and testing,

with production shut down, or does testing require separate systems or environments from production?

6.2. Describe carefully with examples how the user sends a test message in the system. Describe and exemplify with a screen shot, how the user is shown if the customs transaction or message, and also Customs' answer, is a production or testing message.

7. Communication with Customs (via TMF)

7.1. Describe the communication process – step by step – from the position where the system has been approved for sending information up to and including the position where the latest message in the exchange has been downloaded from TMF and processed in the system.

In the process steps, refer to the relevant component – described in the system configuration in Chapter 3.2. – with which each process step occurs. Attach a schematic summary diagram of the process with references.

7.2. Is a direct communication from the permit holder's installation of the system to TMF created, or are intermediaries, such as a VAN operator, used, and if so, what is carried out there?

7.3. At what intervals is there communication with TMF, and can users influence this interval? Can the interval be changed by intermediaries or by a VAN operator?

7.4. Describe the system's handling on receipt of electronic transfers from Customs regarding checking of message, signing, logging and creating receipts stating correct or incorrect.

8. General and TDR/SCTS-specific functions

The various Customs Data Regulatory Frameworks (TDR) and Swedish Customs Technical Specifications (SCTS) state the prerequisites for designing electronic documents that are technically correct.

In addition to these prerequisites, Customs also sets a number of requirements and wishes for functions in the systems developed by the system owner in order for the system description to be approved.

These requirements and wishes are aimed at ensuring that the system's design of or lack of functions does not create serious quality failings or additional work for Customs, and that they reduce unnecessary support for the permit holder and for Customs.

If certain regulatory frameworks are not applicable to the system, please state "Not included in the system support".

8.1. Requirements

8.1.1. Irrespective of regulatory framework

8.1.1.1. Status during indirect communication

If the system does not have direct communication with TMF, describe the codes that may be used to describe where and the status of the message when it is being handled by intermediaries, i.e. outside the system but before it reaches TMF.

8.1.1.2. EDIFACT control

Describe how an authorised person can check that entered information corresponds to the contents of the EDIFACT message before or after it has been sent.

8.1.2. TDR050 (Import and Export)

8.1.2.1. Status codes

See Chapter 16 index instruction - a)
See Chapter 16 index instruction - b)
Define what constitutes a Customs transaction for the system.

8.1.2.2. Error codes

See Chapter 16 index instruction - a)
See Chapter 16 index instruction - c)

8.1.2.3. Error handling

See Chapter 16 index instruction - d)

8.1.2.4. Monitoring of transactions in progress

See Chapter 16 index instruction - a)
See Chapter 16 index instruction - c)

8.1.2.5. Merging and sorting of goods items

Describe how the system
- handles merging of goods items in relation to duplicates (same content of criteria) and
- whether sorting of goods item occurs, and if so
- in falling or rising order.

Specify as necessary the criteria for summary and sorting separately for export and for import.

8.1.2.6. Indicators

Describe how the system handles setting the correct indicator

in electronic documents. Describe if each indicator is set with a value pre-set by the system, or if users are forced to state a value for:

8.1.2.6.1. Agent relationship/quality assured transaction (GIS=ZKS)

8.1.2.6.2. Call me code (GIS=Z11) combined with code relating to restrictions
See Chapter 16 index instruction - a)

8.1.2.6.3. *The sub-chapter is no longer current.*

8.1.2.7. **Pending transactions**

Describe the support the system has for only monitoring so-called pending transactions, i.e. customs transactions that have been started but are not yet cleared and released (for example UNU, HNU and DNU). Exemplify with a screen shot

Describe how the system handles CUSRESU-IEMD in these cases.

8.1.2.8. **Goods value**

Describe if, and if so how, the system supports calculation of:

- Customs value
- Statistical value
- Invoice value

8.1.2.9. **Fall-back procedure**

See Chapter 16 index instruction - i).

8.1.3. **TDR310 (DDNTA 4.0 - Transit)**

8.1.3.1. **Status codes**

See Chapter 16 index instruction - a)
See Chapter 16 index instruction - b)

8.1.3.2. **Error codes**

See Chapter 16 index instruction - a)
See Chapter 16 index instruction - c)

8.1.3.3. **Error handling**

See Chapter 16 index instruction - d)

8.1.3.4. **Monitoring of transactions in progress**

See Chapter 16 index instruction - a)
See Chapter 16 index instruction - e)

8.1.3.5. **Fall-back procedure**

See Chapter 16 index instruction - i).

8.1.4. TDR007 (Outgoing import and export)

8.1.4.1. UTL

See Chapter 16 index instruction - a)
See Chapter 16 index instruction - f)
See Chapter 16 index instruction - g)
See Chapter 16 index instruction - h)
Describe any status, monitoring procedures and integration with import transaction, customs diary.

8.1.4.2. ZKH

See Chapter 16 index instruction - a)
See Chapter 16 index instruction - f)
See Chapter 16 index instruction - g)
See Chapter 16 index instruction - h)
Describe any status, monitoring procedures and integration with drawing up or reconciling against supplementary customs declaration.

8.1.4.3. ZKB

See Chapter 16 index instruction - a)
See Chapter 16 index instruction - f)
See Chapter 16 index instruction - g)
See Chapter 16 index instruction - h)

8.1.5. SCTS-AIS (Entry Summary Declaration)

See Chapter 16 index instruction - a).
See Chapter 16 index instruction - f)
See Chapter 16 index instruction - g)
See Chapter 16 index instruction - h)
See Chapter 16 index instruction - i).

8.1.6. SCTS-NP

8.1.6.1. Notification of Local Clearance - ALE, ALI

Describe if, the system supports EIR and the ability to accumulate several EIR to one notification ALE/ALI.

Describe if, integration exists with Declarant business system to exchange information of EIR or notification ALE/ALI.

8.1.6.1.1. Status codes

See Chapter 16 index instruction - a)
See Chapter 16 index instruction - b)

8.1.6.1.2. **Error codes**

See Chapter 16 index instruction - a)
See Chapter 16 index instruction - c)

8.1.6.1.3. **Error handling**

See Chapter 16 index instruction - d)

8.1.6.1.4. **Monitoring of transactions in progress**

See Chapter 16 index instruction - a)
See Chapter 16 index instruction - e)

Describe if, ability to monitor if EIR / Notification have been or has to be completed in a UFF/TQN.

8.1.6.2. **Release for export ZKL**

See Chapter 16 index instruction - a)
See Chapter 16 index instruction - f)
See Chapter 16 index instruction - g)
See Chapter 16 index instruction - h)

8.2. Wishes

8.2.1. Describe the way/s the system supports quality requirements according to AEO Guidelines: for example traceability, correct classification and charges, checks whether values are reasonable or are updated.

8.2.2. Describe the support the system provides for checking and quality of customs declaration, type validation of values against the support registries provided by Customs.

- Integrated TARIC customs tariff; describe the source and the updating frequency, the TARIC scope in the system in relation to:
  - commodity code,
  - measures,
  - additional codes,
  - texts,
  - history (for example 3 calendar years back), and
  - if so, how is an unbroken history safeguarded in the history,
- customer and permit registers,
- exchange rates,
- other code registers.

8.2.3. Describe whether, and if so which user support the system offers to enable the user to understand the information to be submitted,

for example field heading, help text, reference to ED field number and customs value guidance.

8.2.4. Describe whether, and if so how the system supports validation of mandatory fields in relation to the message to be transferred for the transaction.

9. EDIFACT message and any limitations

Scope of messages
Each regulatory framework includes a number of EDIFACT messages of both functional and technical character that are to be exchanged between permit holders and Customs. According to the regulatory framework, the system shall handle both foundation messages and the associated receipt message for each one.

Customs recommends that complete support for all messages within each regulatory framework shall be developed for each system.

In this chapter, the system owner shall either verify the foregoing, or specify exactly which messages the system supports and give an explanation why the system does not support missing messages.

Limitations in messages
The regulatory frameworks also state what information each message is capable of transferring. For various reasons, a system owner can develop limitations in his handling of messages in relation to what is possible or permitted within the regulatory frameworks. For example, this may be about the system limiting the number of characters for certain data fields, or the ability to repeat certain data in relation to what the regulatory framework permits.

In this chapter, the system owner shall either verify that there are no limitations, or describe what limitations the system has for each message.

Limitations are generally not accepted if they contravene legal or technical principles, if they may cause additional work for Customs or for any other sender or recipient of messages. The description shall also show clearly to the permit holder that it is the system that sets the limitation, and not Customs.

A system owner who wishes to have his system tested as a so-called "Approved System" for certain technical regulatory frameworks must also carry out technical final tests for the regulatory frameworks that include such final tests.

These technical final tests and, as applicable, documents for reporting are available from Customs' website or by contacting edi.test@tullverket.se. A specification/s shall be attached as an appendix to the system description.

Differences between user interface and message
For various reasons, a system owner may also develop differences in the system's user interface in relation to what the system's electronic message communicates. In this way, the user can enter more or less information than the message can communicate to Customs, and, conversely, the user can see less of the information, data fields or repetitions received.

In this chapter, the system owner shall either verify that there are no differences, or describe the differences that exist. But if so, the system owner must also describe in which way the system notifies the user of these differences and how the user can compensate for the difference.

For individual permit holders, limitations or differences may be accepted as a unique company adaptation if the permit holder can show that their operation does not need the information and that the permit holder would otherwise be forced to do unnecessary extra work.

9.1. TDR050 (Import and Export)

9.1.1. Scope of messages
See Chapter 16 index instruction - j).

9.1.2. Limitations in messages
See Chapter 16 index instruction - k).

9.1.3. Differences between user interface and message
See Chapter 16 index instruction - l).

9.2. TDR310 (DDNTA 4.0 - Transit)

9.2.1. Scope of messages
See Chapter 16 index instruction - j).

9.2.2. Limitations
See Chapter 16 index instruction - k).

9.2.3. Differences between user interface and message
See Chapter 16 index instruction - k).

9.3. TDR007 (Outgoing import and export)

9.3.1. Scope of messages
See Chapter 16 index instruction - j).

9.3.2. Limitations
See Chapter 16 index instruction - k).

9.3.3. Differences between user interface and message
See Chapter 16 index instruction - l).

9.4. **SCTS-AIS (Entry Summary Declaration)**

9.4.1. Scope of messages
See Chapter 16 index instruction - j).

9.4.2. Limitations
See Chapter 16 index instruction - k).

9.4.3. Differences between user interface and message
See Chapter 16 index instruction - l).

9.5. **SCTS-NP**

9.5.1. Scope of messages
See Chapter 16 index instruction - j).

9.5.2. Limitations
See Chapter 16 index instruction - k).

9.5.3. Differences between user interface and message
See Chapter 16 index instruction - l).

10. Security during information exchange via EDI

During 2011, Swedish Customs introduced a new PKI-based security concept for the electronic information exchange via EDI. The PKI-based security concept shall completely replace the old solution (Nexus Elektroniska Sigill - "Nexus Electronic Seal") which may be used in parallel with the new security concept during a transitional period.

In this version of guidelines for system description, both security concepts are therefore included during this transitional period. After 1 April 2012, the guidelines for the old security concept are only current when updating previously approved system descriptions for those systems that have not yet been adapted to the new security concept.

Customs places special emphasis on this part of the description being convincing from a legal and technical point of view, so that the system offers satisfactory security handling in the information exchange via EDI.

Customs must always be able to ensure
*a) which **company** is submitting electronic information,*
*b) for certain messages, also the identity of the **individual issuer** of the electronic document.*

The recipient of the information must be able to ensure

c) that it is Customs that is submitting electronic information.

This is safeguarded in different ways in the old and the new security concepts.

10.1. Older solution based on SÄKdata/Nexus Elektroniska Sigill

Handling of seal keys, authority controls, sealing formats and associated processes shall be described in particular detail and be exemplified using screen shots, for example, in order to enable prior assessment and subsequent checking of the protection.

10.1.1. What sealing formats and authority attributes does the system use? For example:

- Stand-alone sealing, authority control of individual issuer, document and personal seal is done per transaction and carried out using a smartcard in a stand-alone (only connected to the electricity network) sealer.
- Built-in sealing with a single-use password, authority control of individual issuer (new required after 30 minutes' inactivity) is carried out using a smartcard in a stand-alone sealer. Document and personal sealing is done immediately or later with the aid of encrypted seal keys and sealing software in a program loop that cannot be interfered with and offers no opportunity to detect seal keys.
- Built-in sealing as above, but with built-in or integrated card reader.
- Other method.

10.1.2. Describe security procedures (preferably with screen shot sequences) for:

10.1.2.1. Authority and security for handling new seal keys, encryption function and where and how seal keys are stored.

10.1.2.2. Authority control of user during login in the system handling the completion of customs declaration.

10.1.2.3. Function/s for the issuer to check the information in the transaction that will be sent to TDS, saving (waiting), restarting and marking for sending electronic document, change mind before transfer is effected.

10.1.2.4. Function for marking several transactions to send created by several users and the principle for whose issuer seal will be used for the transactions marked.

10.1.2.5. The reinforced authority control system and protection procedures for the person who is the issuer of electronic documents. Describe the process how and where the the seal key is handled in conjunction with the handling of a smartcard, customs sealer or corresponding solution for authority control. Describe in steps where encrypted seal keys are collected, where they are unencrypted, calculated and when and how unencrypted seal keys are erased. Please clarify with a schematic summary diagram and describe clearly how this process has been protected from human interference and detection of unencrypted seal keys.

Describe in particular the handling of:

10.1.2.5.1. Initial controls. What activates the authority control for issuers, or when?

10.1.2.5.2. Inactivity controls. How is inactivity defined, and when is it checked?

10.1.2.5.3. Within what time interval? Adjustable interval or a fixed value in program code?

10.1.2.5.4. Reset functions in the event of inactivity and logout respectively?

10.1.2.5.5. Handling of seal key when sealing EDIFACT message? Whether this does not occur in direct and fixed conjunction with the authority control, for example, only at the time of transfer?

10.2. New solution based on PKI certificate

*See 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. References to sections below relate to this document.*

10.2.1. PKI certificate and private signing keys

10.2.1.1. Ordering a signing certificate

Describe whether, and if so in what way the system has integrated the administrative handling by generating signing certificates in accordance with Section 4 in the document **"Guidelines....EDI".**

10.2.1.2. **Maintenance of a signing certificate**

Describe if, and if so in what way the system has additional functions, such as monitoring the validity period of certificates, ordering new certificates, blocking certificates (for example due to an authorised signatory no longer being employed) and logging functions for events.

If the validity period of a signing certificate expires, all messages will be declined, which can have serious consequences for the permit holder. Customs is not responsible for monitoring and renewing signing certificates. When monitoring, the permit holder should also take into consideration the lead time for getting a renewed signing certificate into production.

10.2.1.3. **Handling of signing key on reception**

Describe how requirements 1 and 11-13 respectively are satisfied in the system in relation to Section 5 in the document **"Guidelines...EDI"**

10.2.2. **Authority control**

10.2.2.1. **General authority control for the customs system**

10.2.2.1.1. User authority

Describe if a function exists for registration of users and what authorities they have in the customs system.
See Chapter 16 index instruction - a).

10.2.2.1.2. Login and access to the customs system

Describe if there is any function for login and access to the customs system, for example user identity + password. Describe the security requirements the system sets for these two concepts (minimum character number, a/n, validity period, repeat input). See Chapter 16 index instruction - a).

10.2.2.2. **Two factor solution**

*For certain messages to Customs, security category 2 is required, which means that in addition to signing, a two factor solution is required to create a reinforced authority and identity control in accordance with Sections 1.5 and 5.2 in the document "**Guidelines...EDI**".*

10.2.2.2.1. Technical description of product

Attach the supplier's description of the product and method for secure personal identification that the system owner has chosen to fulfil so-called two factor solution.

If the product in itself is not a two factor solution (PIN code or password + single use password) but only a one factor solution (single use password), it must be combined with another factor (in an integrated, secure and independent process) in order to constitute an acceptable two factor solution. Describe the other factor and its security requirements (see 10.2.2.1.2) and the process in the next chapter for requirement 2.

10.2.2.2.2. Use of two factor solution

Describe how each of the requirements 2-10 is satisfied in the system in relation to Section 5 in the document **"Guidelines...EDI"**. See Chapter 16 index instruction - a).

Requirement 3 – the maximum time that currently applies for inactivity is 30 minutes. Describe whether the customs system has a function for the user to protect against unauthorised used absences shorter than 30 minutes.

11. Use outside Sweden

Describe if, and if so which differences arise in the system or services if any part of the following occurs outside Sweden: installation of program, communication or use.

Customs shall be able to check systems and services against the system description and to follow up permits, which should normally be done in Sweden. Describe if, and if so how the system owner is made responsible in its agreement with the permit holder to assist in ensuring checks can be carried out in Sweden for system installations outside Sweden.

12. Printouts of electronic documents

Please attach copies of the printouts the system can produce for electronic documents based on final test transactions. This refers to such printouts as may be required for manual clearing "over the counter" in the event of exceptions from electronic information submission or during fall-back procedures in the event of operational stoppage in your system or the Customs' system.

13. Assistance during final testing

Describe the system owner's role and the services offered to the permit holder to carry out final tests for production approval for electronic messages.

14. Assistance in applying for permit

Describe the system owner's role and the services offered to the permit holder to complete an application for a permit or similar.

15. Certification and signature

System owner X certifies that:

- The system description corresponds to the system installed.
- Submit and await approval of a new document version before changes are made that affect the content of this document version.
- Notify if any contact or means of contact should change.
- Submit supplementary information at the request of Swedish Customs.
- Correct any failings in accordance with the requirements contained in this instruction voluntarily or at the request of Swedish Customs.

The system description shall be certified and signed by the authorised signatory of the system owner together with name in block letters and date.

The system description shall initially be sent via email to edi.tillstand@tullverket.se for suggestions or approval. The system description shall be attached in Word or pdf format.

After notice of approval, the system description shall be signed and the original sent by post to Tullverket, EDI-tillstånd, Box 12854, SE-112 98 Stockholm, Sweden.

16. Index of repeat instructions

a) Insert an example of a user interface.

b) Describe all status codes the system provides for the various stages at which a customs transaction may be and what condition triggers each status. For example, a table with columns: Status code – Description – Conditions – Comments.

c) Describe exactly what error codes are shown to the user, and how, and also any explanation.

d) Describe in what way an error message from Customs shall be handled by the user in order to correct or cancel the matter.

e) Describe how the system supports monitoring only of those customs transactions where handling is in progress, i.e. from the time the transaction has been approved for transfer to Customs until the time all messages sent about the transaction have received their last logical electronic answer. The scope is dependent on the definition of where a customs transaction is located in the system.

f) Describe the process and functions with system support.

g) Describe how the permit holder is notified that a message has been downloaded from Customs.

h) Describe how the user can partake of all the information in the message, for example attach a printout of an example of a screen shot.

i) Describe the system support for fall-back procedures.

j) Verify that all messages in the regulatory framework are handled by the system. If not, specify in a list of all messages in the regulatory framework and mark those message names that the system handles. Give a brief explanation why the messages in question are not covered by the system. State the date of coming into operation if a decision has been made to develop the message.

k) Verify that the system does not have any limitations for the regulatory framework's messages. If not, specify the limitations between each message and the regulatory framework and attach this list as an appendix to the system description. As necessary, use the document template on Customs' website.

l) Verify that the system does not have any such differences. If not, specify in a separate appendix the differences the system has in information between user interface and message.