TULLI
TULL·CUSTOMS

Data Management

Message Exchange

Direct Message Exchange

Most common problem situations in direct message exchange

v. 1.0, 11.8.2014

Most common problem situations in direct message exchange

This checklist is targeted at customers and software suppliers who are developing solutions for direct message exchange with Customs. This document contains a list of the most common error situations in direct message exchange and related error messages, as well as the solutions to the errors. More comprehensive guidance is available in the Technical Guide, which is available on the Customs website at:
http://www.tulli.fi/fi/yrityksille/sahkoinenasiointi/edi/sanomapohjainen_asiointi_tekninen_opas.pdf.

 The explanation of the error codes can also be found there.

Having problems with the server certificate?

The figure below illustrates the process of acquiring the required server certificate.
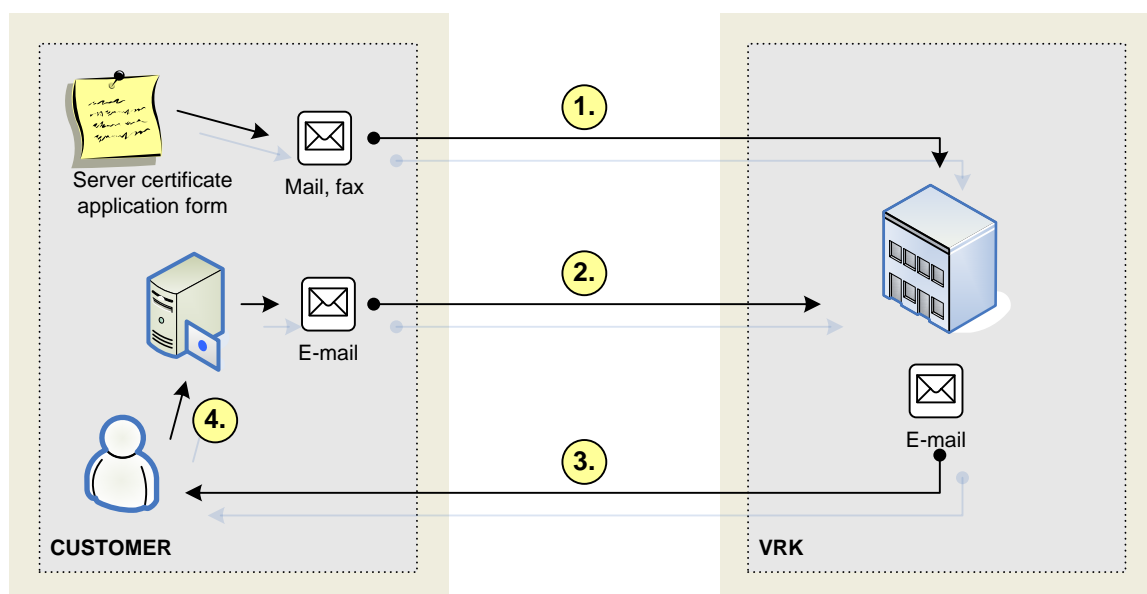
ACQUIRING A CERTIFICATE:

1. Fill in and send the server certificate application form to VRK
http://www.fineid.fi/default.aspx?id=587

2. Create the certificate request file on server and send it to VRK

3. VRK sends back the server certificate

4. Install the VRK delivered server certificate on the server

Ensure that the certificate has been installed correctly for use by the software. The installation of the server certificate varies according to the software. If necessary, the customer should contact the software supplier. As a troubleshooting tool you can use the freeware WIRESHARK.

Ensure that you are using HTTP version 1.1 or 1.2 and note that only the HTTP POST method is allowed. Supported versions of the encryption protocols are TLS version 1 (recommended) and SSL version 3.

- **Error codes: 450**

Are you experiencing problems after renewing the server certificate?

When renewing the server certificate, you need to ensure that the new certificate pair is implemented everywhere as defined in the software.
- If, after the expiry of the old certificate, only the retrieval of message lists and messages succeeds, it is likely that the new certificate pair has not been implemented in the message signature function.

- If, after the certificate has been changed, the attempts to send messages result in an SSL handshake-related error message "certificate expired", a likely reason for the error is that the so-called server certificate pair used for creating the https connection has not been changed.

If there are problems with implementing the certificate, contact Customs only after the https connection to the Customs integration layer has been successfully created. Only at that stage the Customs systems will identify the customer and we can help solve the problem. If problems occur in earlier stages, you can try to capture your Ethernet packets concerning the connection attempt e.g. by using tcpdump or Wireshark and try to solve the problems through them.

Are you sending the messages to the correct environment?

Check that the following settings related to the environment are correct:
TEST URL: https://ws-customertest.tulli.fi/services/DirectMessageExchange
PRODUCTION URL: https://ws.tulli.fi/services/DirectMessageExchange

Value of Environment XML sub-element (ApplicationRequest.xml)
Test: <appl:Environment>TEST</appl:Environment>
Production: <appl:Environment>PRODUCTION</appl:Environment>

Value of the test indicator in the Message block of Arex application messages
Test: <wco:test>1</wco:test>
Production: <wco:test>0</wco:test>

If a message expected from Customs is not available for retrieval, you need to ensure that DownloadList and Download requests have been sent to the appropriate environment. If you try to retrieve a message from the wrong environment error code ERR 700 'Invalid request' or 453 ' Wrong target environment for DownloadRequest will be displayed.

If the optional application identifier given in the DownloadList request is not valid, the error code 472 'Invalid Application specified' is generated.

- **Error codes: 453, 468, 472, 700**

Have the parties been granted authorisations and access rights?

In direct message exchange, both the declarant and the intermediary must obtain from Customs an authorisation for message exchange. If the declarant does not send and retrieve own messages, the declarant must authorise a service provider for generating and transmitting messages. Ensure that Customs has granted the permits and given the necessary authorisations.

- **Error codes: 461, 465, 466, 467**

Are the parties identified correctly in the messages?

The XML elements in web service requests identify the involved parties as follows:

- IntermediaryBusinessId   = message declarant or service provider
- MessageBuilderBusinessId = message declarant or service provider
- DeclarantBusinessId   = message declarant

For a company registered in Finland, the country code and Finnish business ID (e.g. FI2244567-8) is used as the identifier.

For a company registered abroad, the VAT number with country code (e.g. SE12346789) is used as the value of IntermediaryBusinessId and MessageBuilderBusinessId. The EORI number with country code issued to the company is used as the value of DeclarantBusinessId.

The **Sender** element of the application message and the **DeclarantBusinessId** element of the frame message must contain the same data.

- **Error codes: 460, 463, 464, 465, 466, 467, 502**

Have you observed restrictions on message exchange set by Customs?

The frequency of sending service requests is restricted. Customers can submit requests under the following restrictions:

- **One (1)** Upload message **at one-second intervals**
- **Five(5)** Download messages **at one-second intervals**
- **One (1)** DownloadList message **at five-minute intervals** (ERR 457)

Please note: The time limit is calculated from the end of the previous message operation to the beginning of the next operation.

The maximum size of an application message is 512 kilobytes for ELEX and ITU messages and 1024 kilobytes for AREX, EMCS, ALA, NCTS and INSTAT messages.

The interchange identifier must be unique per each Customs target system. If the message is resent, the interchange identifier must be changed. The interchange identifier is in the XML element 'Reference', and it consists of an abbreviated name of the company (5 characters) and a consecutive number (1-9 characters). (ERR 458, ERR 500)

If the application message contains an interchange identifier, it must be identical to the interchange identifier of the web service request. (ERR 501)

The message must not contain well-known SQL keywords such as DESC. (ERR456)

The message list cannot be requested for messages older than 14 days. (ERR 600).

- **Error codes: 456, 457, 500, 501, 600**

Are the errors related to message validation?

Validation errors can occur relating to the:

1. SOAP request (ERR 451)
2. Application request document (ERR 452, 470)
3. Application message (ERR 471)

If you receive an error message indicating a validation error, validate the message before resending it. Many tools exist for this purpose, e.g. the tool "Syntax-Check Your XML" available at: http://www.w3schools.com/XML/xml_validator.asp. Using the selected tool, ensure that the message is well formed and conforming to the required XML schema.

If the error code persists even after the above steps, check that:
- The message refers to the correct schema version. The valid schema versions are can be checked on the Customs website.
- The correct character encoding is used. Only UTF-8 is allowed.

- **Error codes: 451, 452, 459, 469, 470, 471**

Namespaces must be defined in accordance with the XML schema

Errors in defining namespaces are also typical validation errors.
We recommend using the practices listed below for defining namespaces:

- The namespaces are declared in the start tag of the root element
- Each namespace is given one and only one abbreviation (prefix), in the start tag of the root element
- The namespaces to which the elements contained in messages belong should be declared
- When using namespaces, each of the elements in the messages belongs to a specific namespace

A more comprehensive description of using namespaces is found in the Technical Guide.

- **Error codes: 451, 470**

Errors related to the XML signature

Ensure that you are using the following allowed algorithms for the XML signature:

- SignatureMethod → RSAwithSHA256
- DigestMethod → SHA256

The following utility can be used to validate the Base64-decoded ApplicationRequest:
http://www.aleksey.com/xmlsec/xmldsig-verifier.html

- **Error codes: 476, 477, 478, 479**

Data security checks of a message

The message you sent did not pass the data security checks of the content of the message. In the data security checks, the content of the message is analysed for malicious codes e.g. SQL injections. The error code of direct message exchange "456 Rejected by filter" is an error code generated by the component filtering SQL injection attacks.

In order to ensure that message will pass the data security check, it should not contain characters/character strings that might be interpreted as malicious codes. For reasons of data security, we cannot give any detailed description of characters/character strings that might be interpreted as malicious codes. Below you will find a link to the OWASP site where you can find more information and examples on this topic. This information might be useful when editing the contents of the message so that it will pass the data security control of Customs:

More information on SQL injection attacks, examples and links to additional information:
https://www.owasp.org/index.php/SQL_Injection
http://en.wikipedia.org/wiki/SQL_injection

Some XML Document Structure checks can also be classified as data security checks. These errors are shown by error codes "451 Schema validation error" , "452 Schema validation error in ApplicationRequest" or "471 Content validation failed".

- **Error codes: 451, 452, 456, 471**

Is your company using several software products that use the same Customs system:

This kind of situation might occur e.g. when a business is changing their customs clearance software. It is possible to use several software products, but the business must ensure that different software products comply with the message sending restrictions imposed by Customs and that the response messages received from Customs are directed to the correct software product.

From the point of view of the message sending restrictions it is recommended that the business would apply for an own server certificate from the Population Register Centre for both of the software products. When two server certificates are used both of the software products have own message sending restrictions and the synchronisation of message sending between the software products is not needed. In a temporary situation when the software product is changed, it is not necessary to apply for the second server certificate but the restriction must be taken into account.

When two software products or server certificates are used they can easily get mixed. The recipient of the response message when the business ID is used for identification (both of the server certificates have the same business ID). The customer must have in their software a logic component for choosing which one of the response messages should be retrieved for processing by the software product in question.

Especially during the implementation of the Message Notification Service it should be noted that the customs system submits all the message notifications addressed to the same business ID to the same URL.

Is your company using two server certificates with the same Business ID ?

In this case Customs processes the DownloadList requests separately and the five-minute search limit for the message list is set separately for both certificates. Two server certificates enable your two software products to search response messages from the same Customs application (e.g.. <v11:Application>AREX</v11:Application>) using the DownloadList request.

Companies must themselves separate the messages belonging to different software products. It is not recommended to retrieve messages belonging to other software because their status (message status) will change from not retrieved (NEW) to retrieved (OLD). After this, the details of the message will not be shown in the DownloadList response which the other software receives in response to its request.

Especially during the implementation of the Message Notification Service it should be noted the customs system submits all the message notifications addressed to the same business ID to the same URL.

No response messages from Customs after an Upload response indicating success

Contact EDI support at the Electronic Clearance Centre: edituki@tulli.fi