2015-08-28
version 1.1 EN

Please note that if there are differences between this FAQ and the technical specifications, the technical specifications shall apply

Where do I find documentation for the OFTP2 communication concept?

RFC5024 contains documentation on OFTP2 communication.

Swedish Customs is using session level encryption by using Transport Layer Security (TLS). TLS provides data confidentiality by encryption of all protocol commands and data exchanged between Swedish Customs and our partners. This will provide enough security, preventing a third party from extracting any useful information from the transmission. Swedish Customs does not use OFTP2-functionality for file encryption or signing.

Do we need a separate certificate for the OFTP2 communication or is it possible to use the certificate we will receive for the EDIFACT AUTACK signature handling?

As you will be initiating the OFTP-connections to send and receive files there is no need for any extra certificate.
The certificate for the EDIFACT AUTACK signature handling is not used for communication.

TLS works the same way for OFTP2 as for https. This means that Customs OFTP using a standard web server certificate. It is usually required to install this server certificates or CA-certificate for your software to allow this access. This corresponds to the approved CA certificate that is placed on your browser.

Where do I find the Swedish customs server certificate used for OFTP2?

The currently used certificate is issued by Verisign. Root and CA certificates can be downloaded from

Root certificate (Root 3 VeriSign Class 3 Primary CA - G5)**:**
https://www.symantec.com/content/en/us/enterprise/verisign/roots/VeriSign-Class%203-Public-Primary-Certification-Authority-G5.pem

Intermediate certificates (VeriSign Class 3 Secure Server CA - G3)**:**
https://knowledge.symantec.com/support/ssl-certificates-support/index?page=content&actp=CROSSLINK&id=INFO2108

Information
Licensing and Use of Root Certificates:
https://www.symantec.com/page.jsp?id=roots

Repository:
https://www.symantec.com/about/profile/policies/repository.jsp?tab=Tab3

If necessary, import the root and intermediate CA certificates into your EDI System.

What OFTP parameters is used?

OFTP – Parameters

SSID (ODETTE-Code):	*O094200002021000969PRDINT*
SFID	*O094200002021000969PRDINT*
DNS Name:	*tmf01.tullverket.se*
Port:	*6619*

Below you find an example of OFTP2 parameters that we recommend you to use:

OFTPCODE	O09420000123456781012345 6	Your EDI code “Example: O09420000ORGNUMMBERV6TEKN”.
FILEDIR	B	File direction
FORMAT	U	File format
CHANNELSIN	1	Number of incoming OFTP channels.
CHANNELSOUT	1	Number of incoming OFTP channels
PORT	6619	Port
Oftp Maximum Protocol Version	2.0	Oftp Protocol Version
Oftp Maximum Window Size	7	Oftp Window Size
Oftp Maximum Buffer Size	2048	Oftp Buffer Size
Use TLS for OFTP2	Y	Use TLS for OFTP2

Important:
Use format “U” Unstructured, when sending files to *Swedish Customs.*
All files sent from Swedish Customs has format fixed and record size 80.

How can I verify that the OFTP connection works?

If a normal OFTP connection with your OFTP software is connecting and disconnecting with status “ normal session termination” your connection including TLS works properly.

I can’t connect on OFTP level, how can I verify that the TLS connection works?

To check the connection you can use Openssl.

OBS! The check has to be performed from the same machine as the OFTP is going to communicate from.
openssl s_client -connect tmf01.tullverket.se:6619 –showcerts

When you receive “ODETTE FTP READY” the connection works properly.