

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 Company signature certificate we will receive for the electronic document signature handling?

No, the Company Signature Certificate is only used for the electronic signatures of the EDI documents (XML files).

When connecting to the Swedish Customs OFTP2 server, no TLS client certificates are used. A public TLS server certificate is used, which must be trusted by your OFTP software in the same way as a web browser.

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

Information in English about used server certificates can be found at <https://www.tullverket.se/edicommunication>

Information in Swedish about used server certificates can be found at <https://www.tullverket.se/edikommunikation>

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

(continued on next page)

What communication/OFTP parameters are used?

Parameters	Example value
DNS Name:	tmf01.tullverket.se
Port:	6619
SSID (ODETTE-Code):	0094200002021000969PRDINT
SFID:	0094200002021000969PRDINT

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

Parameter	Value	Explanation
Port	6619	Port number
Protocol Version	2.0	OFTP Protocol Version
Incoming sessions	1	Number of incoming OFTP sessions.
Outgoing sessions	1	Number of outgoing OFTP sessions.
Use TLS for OFTP2	Y	Use Transport Layer Security (TLS) to tunnel the OFTP2 session.
SSIDCODE	0094200001234567810123456	Your OFTP EDI code "Ex: 0094200000RGNUMMBERV6TEKN".
SSIDSR	B	File direction
SSIDCRED	10	Credit, OFTP Maximum Credit Window Size
SSIDSDEB	8192	Data Exchange Buffer Size, Maximum
SFIDFMT	U	File format

Important:

For the OFTP File Format (SFIDFMT), the value 'U' (Unstructured) is used when sending/receiving files.

How can I verify that the OFTP connection works?

For an OFTP-connection the software will receive a positive End Session code (ESID '00' Normal session termination), meaning your OFTP-connection over 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 manually use OpenSSL.

Note! 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 and your OFTP software should be able to connect, if using the correct TLS protocol version and cipher suites.