Secure FTP

Client user guide

Author: Steria A/S
Version: 2.2
Date: 20 January 2010
Document SecureFtpClientUserguideV2_2.doc

Preface

Versioning

Intermediate versions of the document and possible attachments.

Version	Date	Name	Comment
0.8	2008-08-22	Mark Gjøl	Initial document
0.9	2008-09-16	Carsten L. Birn	Layout changes
0.91	2008-09-17	Jesper B. Henriksen	1. revision
0.92	2008-10-01	Jesper B. Henriksen	2. revision. Based on input from SKAT, Terkel Tolstrup, 2008-10-01
1.0	2008-11-04	Jesper B. Henriksen	Version update – phase 2 delivery
1.9	2009-09-28	Jesper B. Henriksen	Updated document with changes caused by new alternative solution.
1.91	2009-10-01	John Hansen	1. Revision
2.0	2009-10-01	Jesper B. Henriksen	Version update – alternative solution delivery
2.1	2009-12-04	Jesper B. Henriksen	Added additional connectivity information in Appendix B.
2.2	2010-01-20	Jesper B. Henriksen	Added information on status files

Author references

Name	Email
Jesper B. Henriksen	jbh@steria.dk
Carsten L. Birn	clb@steria.dk
Mark Gjøl	mgj@steria.dk

Table of Contents

1. Purpose of this document

This document describes the client side of the Secure FTP solution. It contains both prerequisites and guidelines on how to use it.

1.1. Prerequisites

In order to connect to the Secure FTP Solution, some prerequisites must be in place:

- An FTP client which supports explicit FTPS and user certificates.
  SmartFTP is a functional client, which Steria has used during the implementation and test phases. The configuration of this client will be explained in detail in appendix A.
- A valid OCES certificate issued by DanID, which can either be a personal certificate, an employee certificate or a company certificate.

1.2. Conventions

The following conventions are used:

- File- and path names are written in **bold**
- Other names are written in *italic*

2. Generic configuration

- The protocol of the client should be set to use FTP over SSL, Explicit mode.
- An OCES certificate should be chosen as the used login credentials.
- As the username and password are not used, any will do. Note here, that anonymous login is fine, but not sending the information will result in an error.

3. Usage

3.1. Inbound files for a Backend System / Business Service

- Connect to the server using the generic configuration description from section 2 and login informations from Appendix B – Connection and login information.
- Change directory (cd) to relevant Backend System / Business Service.
- In this directory, either
  - Upload the file for the Backend System / Business Service. The filename must be unique, as it will be used as your transaction ID (FTPTransactionID).
    Note that as soon as the upload has finished, the file will be moved for processing. This might yield an error if the client tries to check the file size, but this error can safely be ignored.

  or

  - create a directory corresponding to your transaction ID (FTPTransactionsID).

  - In this directory, create a directory called **in**.
  - Upload the file for the Backend System / Business Service to the in directory. See note above about uploading a file.
- Shortly hereafter, you can find a status file in the **/out** directory (in the root folder, which can be found one step out (cd ..) from your login directory if you're using a employee or company certificate – or in your login folder if you're using a personal certificate). This **/out** directory will contain a file called status_<requested service>_<FTPTransactionID>.xml which contains information on whether the file was successfully delivered to the Backend System / Business Service or an error occurred. A status file will be exposed for download in these three scenarios:
  - File has been sent to requested Backend System / Business Service.
  - Requested Backend System / Business Service has successfully accepted the file.
  - An error has occurred.
- The **/out** directory should be polled regularly for further responses from the Backend System / Business Service. These will likewise be accompanied by a status file.

3.2. Outbound files from a Backend System / Business Service

When a Backend System / Business Service sends outbound files, these will also be placed in **/out**. It should be noted that for company- and employee certificates these files will then be available for all certificates of that company. Due to this fact, extra care should be taken when deleting files, as these company messages will be deleted for all other certificate holders within that company as well.

4. Table of figures

5. Appendix A – SmartFTP configuration

The SmartFTP client can be downloaded from http://www.smartftp.com. A default installation should be performed.

Configuration in SmartFTP:

- Go to the *Favorites/Edit Favorites window*.

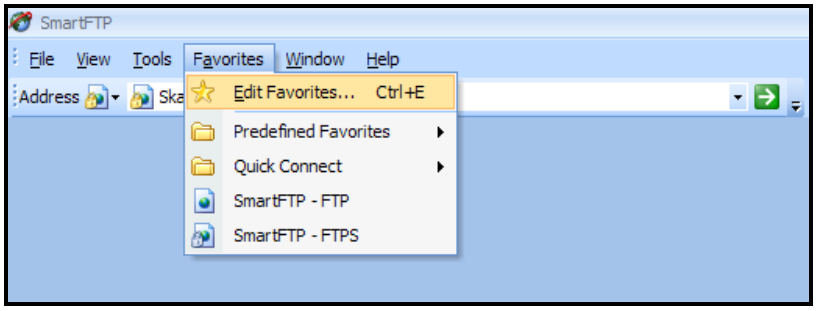

Figure 1 Edit favorites

- Click *Favorite/New/Favorite*.

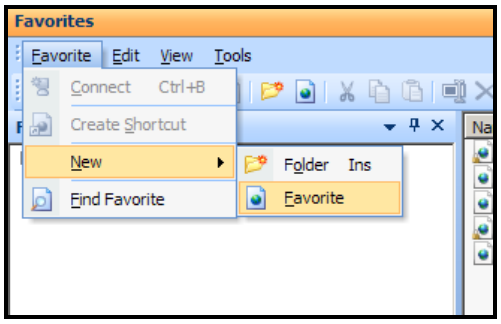

Figure 2 Create new favorite

- Under *General* specify a favorite connection. The connection will be identified by what is written in *Name*. It is important to choose *FTP over SSL Explicit* as *Protocol*, and to choose *Anonymous* as *Login Type*.

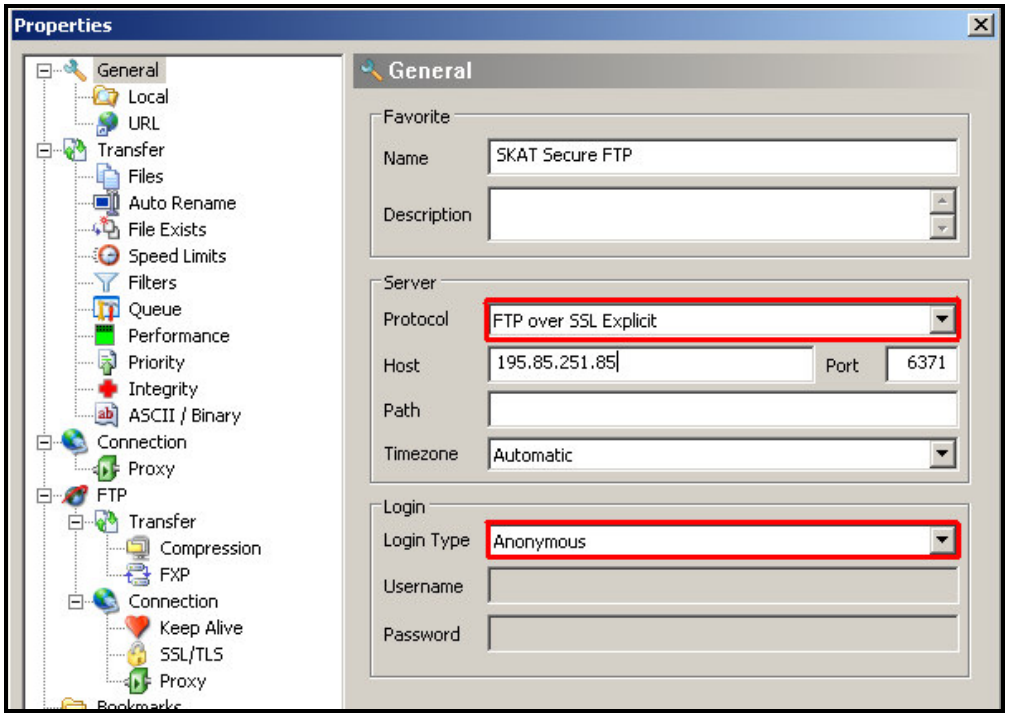

Figure 3 SmartFTP favorites settings

- Go to *FTP/Connection/SSL/TLS*. Make sure that the following options are set:

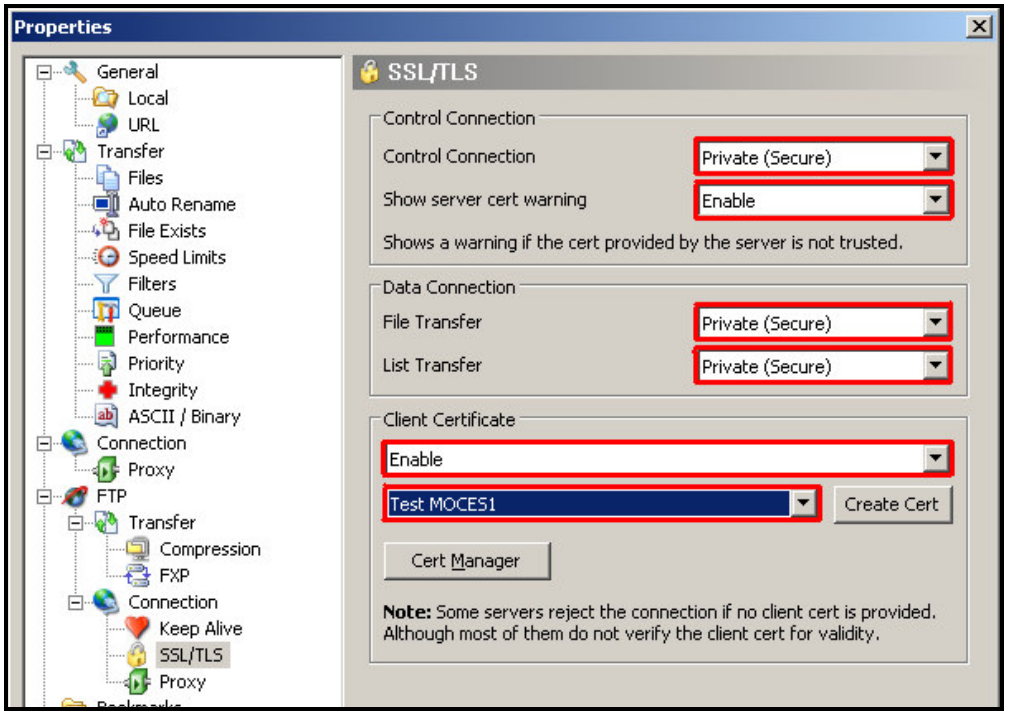

Figure 4 SmartFTP certificate setup

- Note that *Show server cert warning* should be set to *enable* in a production system.

- Click the *Cert Manager* button to manage certificates in SmartFTP.
- If no valid DanID OCES certificate exists in the manager, click *Import…*.
- Follow the guide, choosing your own DanID OCES certificate.
- When the certificate is imported successfully, it should appear in the Personal tab. Close the certificate manager and choose the OCES certificate next to the *Create Cert* button.

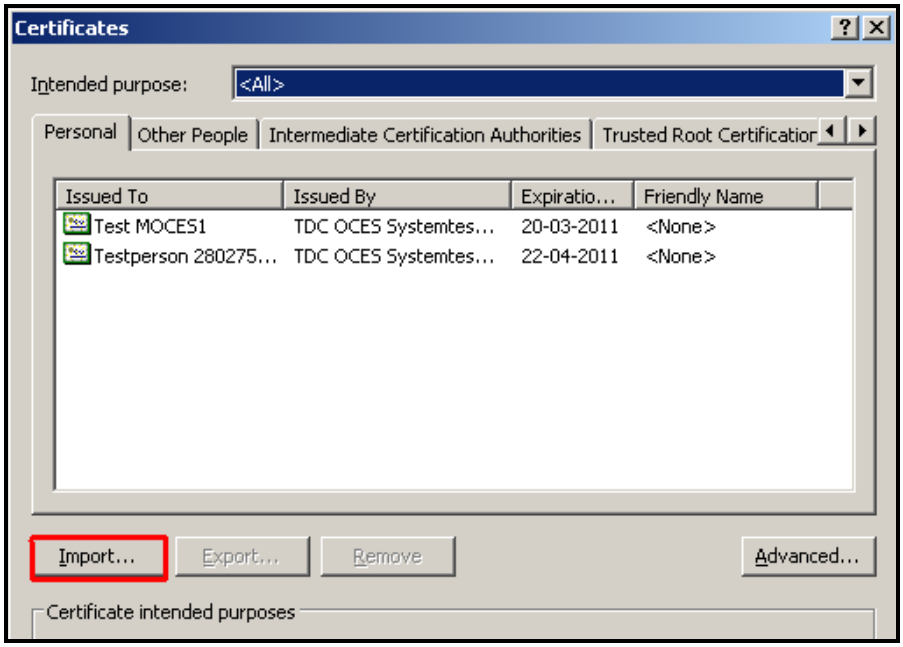

Figure 5 Installed certificates

Click *OK* to close the *properties* dialog.

6. Appendix B – Connection and login information

Test system (until 1. of January 2010):

IP address of the Gateway server:
secureftpgatewaytest.skat.dk (195.85.251.85)

Port number on the Gateway server for inbound FTP connections:
6371

Port range on the Gateway server for inbound FTP data connections:
35000 - 35010

Login:
Any username/password or anonymous.

Certificate:
Use a valid OCES certificate; either personal, employee or company.

Production system (from 1. of January 2010):

IP address of the Gateway server:
secureftpgateway.skat.dk (195.85.251.102)

Port number on the Gateway server for inbound FTP connections:
6371

Port range on the Gateway server for inbound FTP data connections:
35000 - 35100

Login:
Any username/password or anonymous.

Certificate:
Use a valid OCES certificate; either personal, employee or company.

7. Appendix C – Description of status file

One purpose of the status file is to inform what has occurred to the uploaded file. If the client has made a mistake, the status file will hold information of the error and what action needs to be taken to resolve it. Likewise, if a system error occurs or if the file flow has completed successfully, the client will be informed accordingly. Secondly, the client will receive a status file whenever a Business Service has finished a file transfer, containing details on whether this is a reply or not, and which files have been made available.

The status file contains information identifying the specific transaction to the client:
The called service, the selected transaction ID, the uploaded file name, the SKAT transaction ID and the time of the status file. The format of the status file is detailed in the appropriate XSD [status_file.xsd].

The elements in the status files are:

filename		Name of the uploaded file by the client. Can in theory be omitted if status file is for an outbound file that is not a response to a previously uploaded file.
FTPTransaktionsId		Unique transaction ID as specified by the client
SKATTransaktionsId		Unique transaction ID generated by the system
timestamp		Timestamp of the status file
status.code		Status code. Can either be **OK** or **ERROR**
service		Requested backend system
response	filename	List of files exposed to the client. This will only be be included if status file is for one or more outbound files.
error	error.code	Unique code for a specific error
	error.message	Description of the error
	error.resolution	Description of a possible solution