 27.11.2002PD

Kundens PLDistribusjonslisteSign.datoDraft  Kunde A/S

FTP-GW

Client User Guide

|  |  |
| --- | --- |
| **Author:** | Steria A/S |
| **Version:** | 3.2 |
| **Date:** | 09-03-2015 |
| **Document** | FTP-GW Client User Guide v3.1.docx |

Purpose

This document describes the client side of the FTP-GW solution, i.e. how you as a user can upload files to SKAT or receive files from SKAT using FTP-GW’s facilities for secure file transport via the FTPS protocol.

Document history

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Name** | **Comment** |
| 0.8 | 2008-08-22 | MGJ | Initial document |
| 0.9 | 2008-09-16 | CLB | Layout changes |
| 0.91 | 2008-09-17 | JBH | 1. revision |
| 0.92 | 2008-10-01 | JBH | 2. revision. Based on input from SKAT, Terkel Tolstrup, 2008-10-01 |
| 1.0 | 2008-11-04 | JBH | Version update – phase 2 delivery |
| 1.9 | 2009-09-28 | JBH | Updated document with changes caused by new alternative solution. |
| 1.91 | 2009-10-01 | JHA | 1. Revision |
| 2.0 | 2009-10-01 | JBH | Version update – alternative solution delivery |
| 2.1 | 2009-12-04 | JBH | Added additional connectivity information in Appendix B. |
| 2.2 | 2010-01-20 | JBH | Added information on status files. |
| 2.3 | 2010-10-05 | JBH | Corrected connectivity information in Appendix B. |
| 2.4 | 2010-10-26 | JBH | Minor clarifications |
| 2.5 | 2011-07-22 | LAH | Minor changes to reflect some changes |
| 2.6 | 2011-09-22 | HUT | Appendix updates |
| 2.7 | 2011-10-24 | Various | Updated after feedback from SKAT |
| 2.8 | 2012-08-15 | EUH | Updated with description of login limitations |
| 2.9 | 2013-06-20 | TBU | Users should use their company email address as username, and new recommendation regarding file length |
| 3.0 | 2014-05-15 | MNY, CNI | Major updates and clarifications. |
| 3.1 | 2015-03-09 | JHA | SIT-environment added to appendix B |
| 3.2 | 2015-04-22 | JHA | Cosmetic changes |

**Table of Contents**

[1. Introduction 4](#_Toc477525578)

[2. Document Conventions 5](#_Toc477525579)

[2.1. Terminology 5](#_Toc477525580)

[3. General Usage 6](#_Toc477525581)

[3.1. Prerequisites 6](#_Toc477525582)

[3.2. FTP Client Configuration 6](#_Toc477525583)

[3.3. Login Limitation 6](#_Toc477525584)

[4. File Flows 7](#_Toc477525585)

[4.1. Inbound Files for a Backend System or Business Service 7](#_Toc477525586)

[4.2. Outbound Files from a Backend System or Business Service 7](#_Toc477525587)

[4.3. Status Files 8](#_Toc477525588)

[4.4. Delayed status files (eKapital only) 9](#_Toc477525589)

[5. Appendix A – SmartFTP Configuration 11](#_Toc477525590)

[6. Appendix B – Connection and Login Information 16](#_Toc477525591)

[7. Appendix C – Status File Examples 18](#_Toc477525592)

[8. Appendix D – Error Codes 20](#_Toc477525593)

[8.1. General error codes 20](#_Toc477525594)

[8.2. Error codes specific for eKapital systems 22](#_Toc477525595)

# Introduction

FTP-GW provides a facility for a managed and secure file flow between SKAT’s customers and SKAT’s backend systems.

This document gives a practical description of how SKAT’s customers can use FTP-GW to transfer files to and from SKAT systems in sections 3 – *General Usage* and 4 – *File Flows*.

Examples and other reference material is provided in the appendices.

# Document Conventions

The following conventions are used:

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

## Terminology

Throughout this document specific acronyms and terms are used. Some of them are shortly explained here.

|  |  |
| --- | --- |
| Authenticate | The process of identifying and verifying the identity of a user. In FTP-GW authentication is based on OCES Certificates. |
| Authorize | To verify that an (authenticated) user has been granted the permission required in order to perform an action or access a resource. In FTP-GW authorization is based on SKAT’s security system DCS. |
| Backend System | A Backend System, a so-called “Classic System”, does not use a service-oriented architecture. Instead it uses only files to communicate with the Gateway.  Authorization of clients communicating with a Backend System is handled by a local authorization-scheme in the FTP-GW solution.  The solution for Backend Systems was originally implemented for “eKapital” systems. |
| Business Service | A Business Service uses a service-oriented architecture, more specifically it uses the StyretFiloverførsel design (managed file transfer) to communicate with the Gateway.  Authorization of clients communicating with a Business Service is handled in DCS. |
| DCS | SKAT security system responsible for authenticating and authorizing clients using the FTPS-entrance. Since any client with a valid OCES Certificate can access the Gateway, it must be verified that the user is known to SKAT and have privileges to send files to a certain Business Service. |
| ESB | Enterprise Service Bus |
| Gateway | Synchrony Gateway from Axway |
| Inbound and outbound | Always think of the terms inbound and outbound as seen from SKAT’s point of view. I.e. inbound files originate from customers and FTP-GW manages the transfer **in** to SKAT’s systems, and outbound files originate from SKAT’s systems and FTP-GW controls the transfer and delivery **out** to customers. |
| Integrator | Synchrony Integrator from Axway |
| MBC | Message Builder Component  A component in Integrator that has a specific purpose. It is written in the Message Builder language. |
| Outbound | See ‘Inbound and outbound’ |
| Secure Relay / SSR | Synchrony Secure Relay from Axway |
| WLS | Weblogic Server |

# General Usage

## Prerequisites

In order to connect to FTP-GW, some prerequisites must be in place:

* You must have an FTP client which support explicit FTPS and user certificates.   
  SmartFTP is a functional client, which Sopra Steria has used during the implementation and test phases. The configuration of this client will be explained in detail in appendix A as an example.
* You must have a valid OCES certificate issued by DanID, which can either be a personal certificate, an employee certificate or a company certificate.
* You must be registered in Skats security system DCS. For further details please refer to Appendix E *– Getting Authorized* .

## FTP Client Configuration

* The protocol should be set to use FTP over SSL, Explicit mode.
* An OCES certificate should be chosen as the used login credentials.
* For login we recommend users to use their company email address and leave the password field empty.
* The maximum length of a filename is 17 characters*.*
* If line lengths exceed 2048 characters, Binary mode *must* be used.
* If files are uploaded to SKAT’s eKapital systems, ASCII mode *must* be used.

## Login Limitation

To avoid excessive use of system resources it is strongly recommended to login to check for responses and status updates at most once per minute.

The number of successive logins within a time frame is limited, e.g. 10 login attempts within 30 seconds. If the limit is reached, it is not possible to login with a given certificate for a certain time, typically 1 or 2 minutes.

The actual values vary depending on which environment is being accessed.

The values at the time of writing can be found in Appendix B, but is subject to change without updates to this guide.

# File Flows

FTP-GW implements two versions of both ingoing and outgoing file flows. First file-flows were implemented specifically for eKapital, and later the more generic IP flows were added. From a client perspective, eKapital and IP flows are identical, except:

* The eKapital flow implements a retry feature, which may delay the delivery of status files. For further details regarding examples following the format of these files, please refer to Appendix C – *Status File* Examples.
* The eKapital flow uses the same error codes as the IP flow, but eKapital furthermore uses some specific error codes. For further details please refer to Appendix D – *Error Codes*.

The following sub-sections are equally applicable for IP- and eKapital flows.

## Inbound Files for a Backend System or Business Service

* Connect to the server using the generic configuration description from section 3.2 and login information 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 and no longer than 17 characters, as it will be used as your transaction ID (FTPTransactionID).  
  Note that 5 seconds after the upload has finished, the file will be moved for processing. This delay should suffice for the FTP clients that tries to check the file size after upload.

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.

As the uploaded file is processed, status files are written to the **/out** directory (in your root folder, which can be found one step out (cd ..) from your login directory, if you’re using an employee, company or EORI certificate – or in your login folder, if you’re using a personal certificate).

The /**out** directory should be polled regularly for status files generated by the FTP-GW solution and possibly responses from the Backend System / Business Service. These files are described in the following chapters.

Status files are described in detail in section 4.3 *Status Files.*

## Outbound Files from a Backend System or 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. An outbound file is accompanied by a status-3 file, but no status 1 or 2 files, as these describe a file transfer from the client to the Backend, which doesn’t happen in the case of an outbound file.

There is no uniform naming standard as the outbound files are named by the Backend System / Business Service.

## Status Files

The purpose of the status file is to inform what has occurred to the uploaded file. If you or your client software has performed an action that was unexpected by FTP-GW, the status file will hold information about 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, you will be informed accordingly. Furthermore, you 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.

Status files are named **status\_<requested service>\_<FTPTransactionID>\_<statuscode>.xml, where**

* <requested service> is the service that the file was delivered to. This corresponds to the folder in which the file was placed.
* <FTPTransactionID> is the FTP transaction ID. This is either the full path of the file or a custom ID. See paragraph 4.1 for details.
* <statuscode> is either 0, 1, 2 or 3.

There are four possible status codes:

* **Status 1 (File delivered)**  
  This file is generated when the file has been sent to the Backend System/Business Service
* **Status 2 (File Accepted)**  
  This file is generated when the file has been validated and accepted by the Backend System/Business Service.
* **Status 3 (File exposed)**  
  This file is generated when a file has been sent from the Backend System/Business Service to the client. A file is sent either as a response to a file sent from the client (as described in paragraph 4.1) or as an unprovoked outbound flow (as described in paragraph 4.2). In case of a response, the status file will contain the response.Filename, which will not exist in case of an outbound flow.
* **Status 0 (Error)**  
  This status file is generated when an error or unexpected action occurs in the course of a file flow. A status 0 file will be generated in the clients **/out** directory when an inbound OR outbound flow fails. This means that, in addition to receiving a status-0 file when failing to send a file (inbound), the client will also receive a status-0 file in cases where a Backend System/Business Service fails to send a message to the client, regardless of the file being a response to a client file or an unprovoked flow.  
  The result of a status 0 should be – unless special agreements have been set up between client and backend system – a re-shipment of the file.

It is important to note that the FTP-GW in no way validates the content of the files being sent from client to Business Service (and vice versa). All validations on file contents are done by the Backend System/Business Service or client.

The gateway only generates status\_0 files if the flow itself fails, either because of an internal error or because the backend did not accept the file. If the backend returns a response document containing an error, the transfer of the file was successful, and no errors occurred from FTP-GW’s perspective; FTP-GW does not read or validate transferred files.

Depending on how the backend service has implemented the FTP-GW protocol, the service may reject a file based on the content, once it has been received by the service. In this case the error will be reported as a status\_0 file, as the backend rejected the transferred file.

Example:

Consider a service that receives an XML document with phone numbers and returns an XML document with addresses based on the phone numbers.

* If an error occurs internally in the FTP-GW, a status\_0 file will be generated in **/out**.
* If a validation fails, for example if the client does not have the rights in DCS to call the service, a status\_0 file will be generated in **/out**.
* If the file is transferred to the backend, but the backend rejects the file, a status\_1(File delivered) followed by a status\_0 will be generated in **/out**.
* If the file is transferred to the backend, and the backend accepts the file but fails afterwards (i.e. a simple validation error in the backend system occurs), a status\_1(File delivered), status\_2(File accepted), status\_3(File exposed), along with a response document from the backend service containing the error will be generated in **/out**.

It is important always to check for the existence of a status-0 file, as this indicates an error in the flow. In rare cases, a status-0 file can even be generated along with a status-3 file. When both a status-3 and status-0 file exists for a flow, the status-0 file takes precedence and the flow should be seen as failed.

The elements in the status files are:

|  |  |  |
| --- | --- | --- |
| Filename | | Name of the file uploaded by the client. 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 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 |

For a list of possible error codes, please refer to Appendix D – *Error Codes*.

Examples of status files can be found in Appendix C – *Status File Examples*.

## Delayed status files (eKapital only)

When sending files to the eKapital Services, there may be a delay before any status files are generated. This is due to a resend feature that is in place towards these services. In case of the upload from FTP-GW to the eKapital service, FTP-GW will attempt to resend the file after 5 minutes, 9 hours and 37 hours. This delay will only happen in case of an upload error to the backend system. Any other cases will result in an immediate status-0 file.

# Appendix A – SmartFTP Configuration

This appendix has been included for inspiration on the configuration described in Chapter 3.2. It is based on SmartFTP version 4.1 and changes must be expected in later releases (for our purpose, version 4.0 and 4.1 are identical except for the naming of the TLS protocol: 4.0 calls it *SSL/TLS* and 4.1 calls it *TLS*).

The SmartFTP client can be downloaded from <http://www.smartftp.com>.

A default installation should be performed.

In the following steps, connection information is added as an example. The actual information according to the target environment (Test or Production) can be found in appendix B.

**Configuration in SmartFTP:**

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

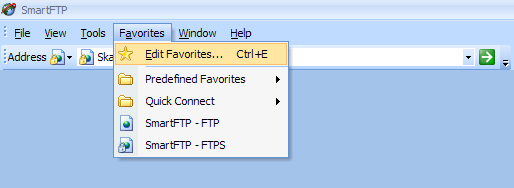


Figure 1 Edit favorites

* Click *Favorite/New/Favorite*.

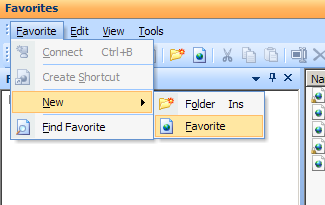


Figure 2 Create new favorite

* Under *General* specify a favorite connection. The connection will be identified by what is written in *Name*. It is important to choose *FTPS (Explicit)* as *Protocol* and to use the user’s company email address as username.

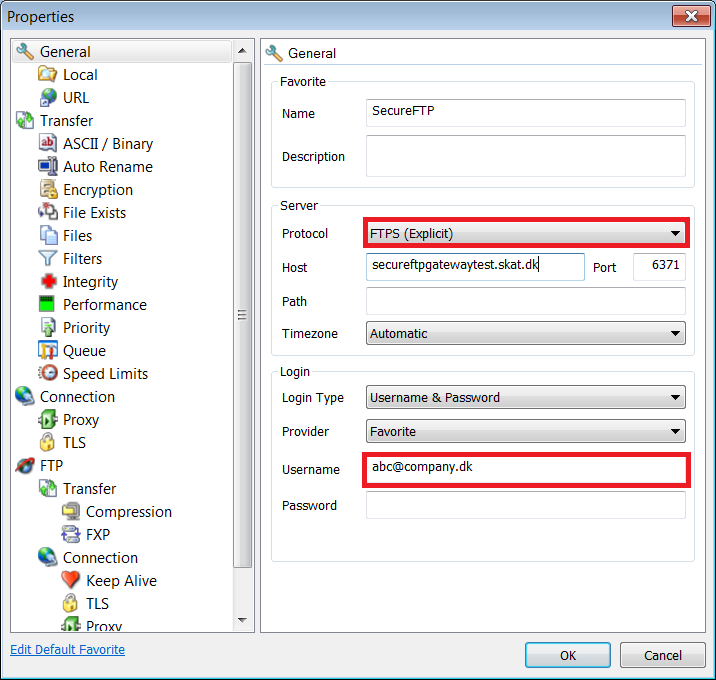


Figure 3 SmartFTP favorites settings

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

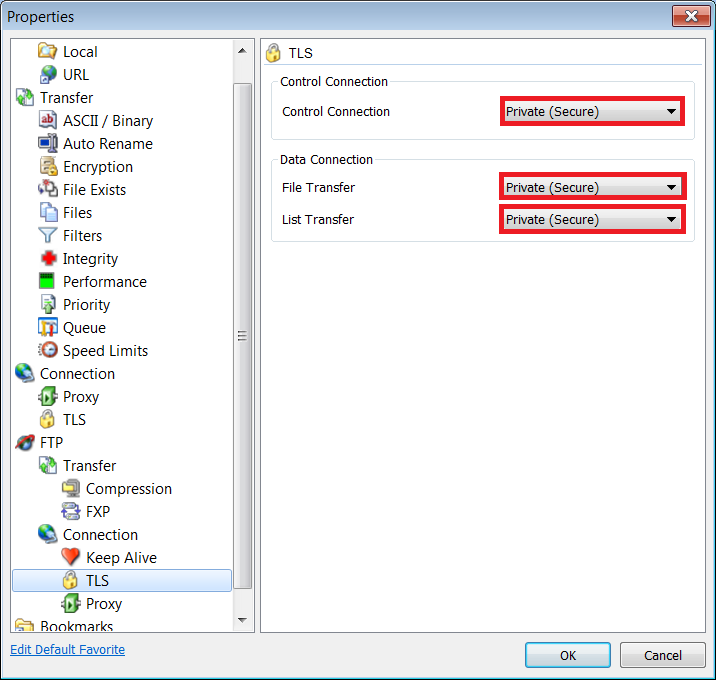


Figure 4 SmartFTP TLS setting

* Now go to *Connection/TLS* and set the options as shown in figure 5.
* Note that *Show server cert warning* should be set to *enable* in a production system.

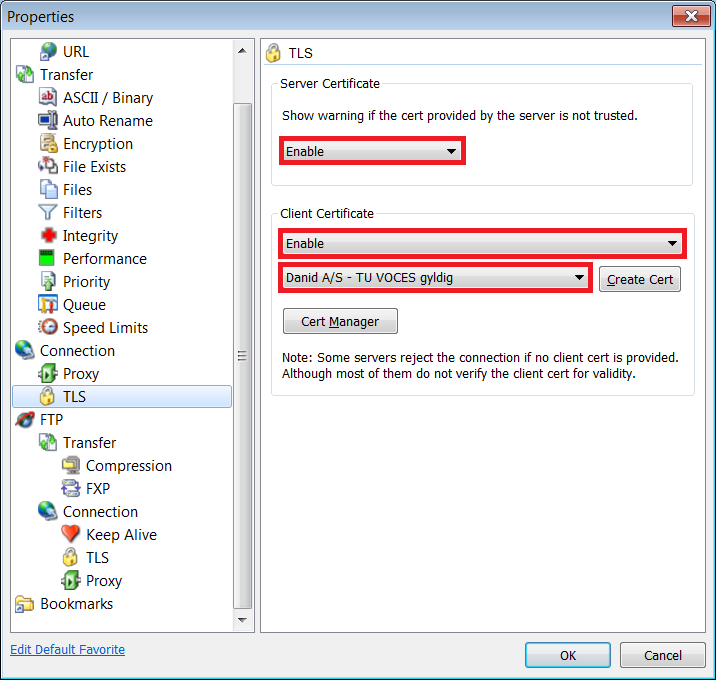


Figure 5 SmartFTP certificate setup

* 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.

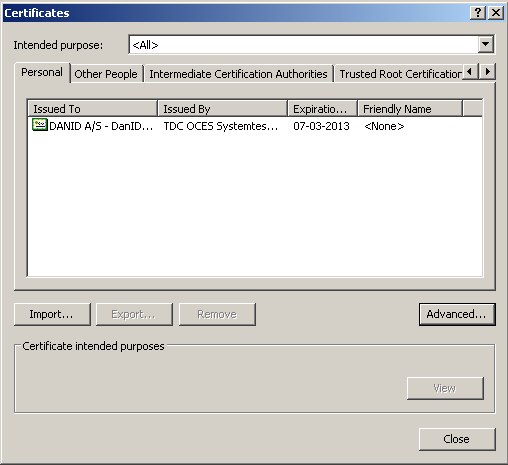


Figure 6 Installed certificates

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

# Appendix B – Connection and Login Information

**Test System ‘System Integration Test’ (SIT):**

**Host name of the Gateway server:**

secureftpgatewaysit.skat.dk

**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:**

username[@company.dk](mailto:@company.dk), and any password.

**Certificate:**

Use a valid Test OCES certificate; either employee or company.

**Login restrictions:**

No more than 10 logins every 30 seconds for each user.

**Test System ‘Test For Erhvervslivet’ (TFE):**

**Host name of the Gateway server:**

secureftpgatewaytest.skat.dk

**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:**

username[@company.dk](mailto:@company.dk), and any password.

**Certificate:**

Use a valid OCES certificate; either employee or company.

**Login restrictions:**

No more than 20 logins every 30 seconds for each user.

**Production System:**

**Host name of the Gateway server:**

secureftpgateway.skat.dk

**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:**

username[@company.dk](mailto:@company.dk), and any password.

**Certificate:**

Use a valid OCES certificate; either employee or company.

**Login restrictions:**

No more than 10 logins every 30 seconds for each user.

# Appendix C – Status File Examples

Status 0 (error):

status\_ Manifest.MidlertidigOpbevaringOpret \_ EORI-DK88216512,FILENO-174002.xml \_0.xml

<?xml version="1.0" encoding="UTF-8"?>

<status>

<file>

<filename>/CVR\_20621117/UID\_24269534/CheckUdbetalingListeSend/ EORI-DK88216512,FILENO-174002.xml </filename>

<FTPTransaktionsId>EORI-DK88216512,FILENO-174002.xml</FTPTransaktionsId>

<SKATTransactionId>lpar3-jiwxkem8-cn21-jfgy-dbsq-2ytlnzjjh21p\_LgIdlogger\_4254\_0000000000425108</SKATTransactionId>

<timestamp>20140612120349</timestamp>

<status.code>Error</status.code>

<service> Manifest.MidlertidigOpbevaringOpret </service>

<error>

<error.code>AUTHORIZATION\_TIMED\_OUT</error.code>

<error.message>The security system does not respond</error.message>

<error.resolution>Please try again or contact SKAT customer service if the problem continues</error.resolution>

</error>

</file>

</status>

Status 1 (File delivered):

status\_ Manifest.MidlertidigOpbevaringOpret \_ EORI-DK88216512,FILENO-174002.xml \_1.xml

<?xml version="1.0" encoding="UTF-8"?>

<status>

<file>

<filename>/CVR\_20621117/UID\_24269534/ CheckUdbetalingListeSend / EORI-DK88216512,FILENO-174002.xml </filename>

<FTPTransaktionsId> EORI-DK88216512,FILENO-174002.xml </FTPTransaktionsId>

<SKATTransactionId>lpar3-hmoizs2u-spjd-rutn-rkjj-aln1fgpinvqs\_LgIdlogger\_4254\_0000000000007006</SKATTransactionId>

<timestamp>20140612121614</timestamp>

<status.code>File delivered to requested Backend System</status.code>

<service> Manifest.MidlertidigOpbevaringOpret </service>

</file>

</status>

Status 2 (File Accepted):

status\_ Manifest.MidlertidigOpbevaringOpret \_ EORI-DK88216512,FILENO-174002.xml \_3.xml

<?xml version="1.0" encoding="UTF-8"?>

<status>

<file>

<filename>/CVR\_20621117/UID\_24269534/ CheckUdbetalingListeSend / EORI-DK88216512,FILENO-174002.xml </filename>

<FTPTransaktionsId> EORI-DK88216512,FILENO-174002.xml </FTPTransaktionsId>

<SKATTransactionId>lpar3-hmoizs2u-spjd-rutn-rkjj-aln1fgpinvqs\_LgIdlogger\_4254\_0000000000007006</SKATTransactionId>

<timestamp>20140612121629</timestamp>

<status.code>File accepted by Manifest.MidlertidigOpbevaringOpret </status.code>

<service> Manifest.MidlertidigOpbevaringOpret </service>

</file>

</status>

Status 3 (File exposed):

status\_ Manifest.MidlertidigOpbevaringOpret \_ EORI-DK88216512,FILENO-174002.xml \_3.xml

<?xml version="1.0" encoding="UTF-8"?>

<status>

<file>

<filename>/CVR\_20621117/UID\_24269534/ CheckUdbetalingListeSend / EORI-DK88216512,FILENO-174002.xml </filename>

<FTPTransaktionsId> EORI-DK88216512,FILENO-174002.xml </FTPTransaktionsId>

<SKATTransactionId>lpar3-hmoizs2u-spjd-rutn-rkjj-aln1fgpinvqs\_LgIdlogger\_4254\_0000000000007006</SKATTransactionId>

<timestamp>20140612121634</timestamp>

<status.code>File exposed</status.code>

<service> Manifest.MidlertidigOpbevaringOpret </service>

<response>

<filename>/out/ Manifest.MidlertidigOpbevaringOpret.EORI-DK88216512,FILENO-174002.xml </filename>

</response>

</file>

</status>

# Appendix D – Error Codes

If an error occurs during processing of a file, an error message will be returned to the user in a file named status\_<requested service>\_<ftp transaction id>\_0.xml.

The file contains various information about the error, including the fields error.code, error.message and error.resolution.

The following is a description of the errors that may be encountered and an explanation of the individual errors.

## General error codes

**Error code: INTERNAL\_SERVER\_ERROR**

Error message: An internal server error has occurred

Error resolution: Please contact customer service

This is a generic error that is thrown if the cause is not known. Contact customer service for further information about the resolution.

**Error code: BACKEND\_SYSTEM\_NOT\_AVAILABLE**

Error message: The requested Backend System does not answer

Error resolution: Please try again or contact SKAT customer service if the problem continues

The backend system cannot be reached. Please try again later or if the problem persist you can contact customer service for further information. The error usually occurs if there is some error in the infrastructure.

**Error code: OUTBOUND\_FILE\_ERROR**

Error message: An error occurred when exposing an outbound file

Error resolution: The originating Backend System has been notified and is responsible for resending the file

This error most often occurs when a file cannot be found. Check to see if the file is placed in the correct outbound folder and the name of the file is legal. Under certain circumstances this error can occur due to internal errors of the FTP-GW system.

**Error code: AUTHORIZATION\_TIMED\_OUT**

Error message: The security system does not respond

Error resolution: Please try again or contact SKAT customer service if the problem continues

This error will occur if the security system does not respond. Please contact SKAT customer service if the problem continues.

**Error code: SERVICE\_DOES\_NOT\_EXIST**

Error message: The requested service does not exist

Error resolution: Please contact SKAT customer service.

This error will occur if you have named your outbound folder with a name of a service that does not exist.

**Error code: UPLOAD\_PATH\_INVALID**

Error message: Files should be uploaded in correct folder structure

Error resolution: Upload the file in this structure: ~/[service] or in: ~/[service]/[FTPTransaktionsId]/in

The specified upload folder structure does not resemble the structure “~/[service]” or “~/[service]/[FTPTransaktionsId]/in“ . Check the folder structure.

**Error code: TRANSACTION\_ID\_UNDEFINED**

Error message: Uploaded files should be uploaded in a transaction ID folder if not directly under service

Error resolution: Upload the file in this structure: ~/[service]/[FTPTransaktionsId]/in or alternatively in: ~/[service]

The specified upload folder structure does not resemble the expected structure “~/[service]/[FTPTransaktionsId]/in“ . Check the folder structure.

**Error code: NESTED\_DIRECTORIES\_IN\_ARCHIVE**

Error message: The uploaded archive contains nested directories

Error resolution: Only upload flat archives without directories

The specified upload folder structure does not resemble the expected structure.

**Error code: GUID\_NOT\_FOUND**

Error message: The certificate ID does not correspond to a SKAT GUID

Error resolution: Please contact SKAT customer service

The client does not the required authorization. Check to see if you call the intended service or contact SKAT customer service. See also Appendix E – *Getting Authorized*.

**Error code: ROLE\_COULD\_NOT\_BE\_FOUND**

Error message: The role could not be verified for the certificate

Error resolution: Please contact SKAT customer service

This error will occur if the certificate attached to the client does not have the necessary rights to the requested Business Service/Backend system. Please contact SKAT customer service.

**Error code: HANDSHAKE\_TIMED\_OUT**

Error message: The requested Backend System has not acknowledged the send file within standard time frame

Error resolution: Please contact SKAT customer service

This error will occur if the time frame for acknowledging the file has been expired for the requested Backend System. Please try again or contact SKAT customer service.

**Error code: ZIP\_NOT\_ACCEPTED\_BY\_SERVICE**

Error message: The requested Backend System does not support zip files

Error resolution: Unzip file and upload it again

This error will occur if the client tries to upload a zip file. The Backend System does not support zip files. Unzip the file and try again.

## Error codes specific for eKapital systems

**Error code: CLIENT\_NO\_PERMISSION**

Error message: The used certificate does not have permission to access the requested service

Error resolution: Please contact SKAT for access to additional services

The FTP client does not have the permission to access the requested service. Check to see if you call the intended service or contact SKAT to get permission to access the service.

**Error code: FILE\_NOT\_UPLOADED\_IN\_ASCII\_MODE**

Error message: Files to the requested Backend System must be uploaded in ASCII mode

Error resolution: Upload file in ASCII mode

The backend System only support files uploaded in ASCII mode. Please upload the file in ASCII mode or contact customer service for further instructions.

**Error code: RECORD\_LENGTH\_INCORRECT**

Error message: The file does not conform with required format due to incorrect record length. Please see www.skat.dk/eKapital

Error resolution: Fix record length and upload file again

This error will occur to ensure that the record length has the correct length. Fix the record length and try to upload again. Please contact SKAT customer service if the problem continues.

**Error code: FIRST\_RECORD\_INCORRECT**

Error message: The file does not conform with required format due to incorrect start of first record. Please see www.skat.dk/eKapital

Error resolution: Fix first line and upload file again

This error will occur to ensure that the record length has the correct length. Fix the record length and try to upload again. Please contact SKAT customer service if the problem continues.

**Error code: LAST\_RECORD\_INCORRECT**

Error message: The file does not conform with required format due to incorrect start of last record. Please see www.skat.dk/eKapital

Error resolution: Fix last line and upload file again

This error will occur to ensure that the record length has the correct length. Fix the record length and try to upload again. Please contact SKAT customer service if the problem continues.