	JPK / SAF-T Transfer Administrator Installation Manual	
		Version: 2018-04-24 (2.0/010)

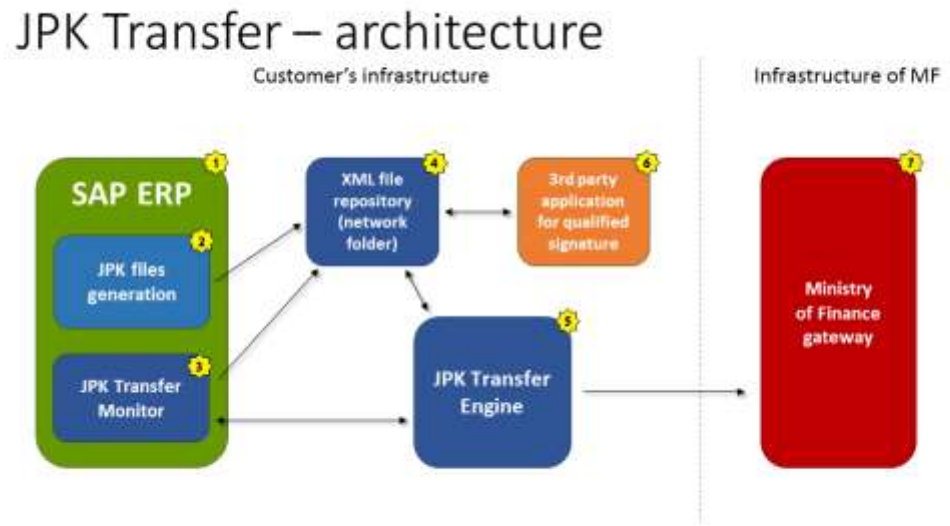
Table of contents

1. JPK Transfer installation description 2
1.1. Alternative landscapes of JPK Transfer solution 3
1.2. Installation steps 4
2. Installation of JPK Transfer Engine as a scheduled task 16
3. Security of JPK / SAF-T Transfer 17
4. Authorizations of SAP users in JPK / SAF-T Transfer 18
5. JPK Transfer update description 21
6. JPK Transfer XSD version configuration 22
7. JPK Transfer Engine local paths 22
8. Signing tools start for local user configuration 22
9. JPK Transfer Engine shutdown 23
10. Certificates required for connection with external HTTPS services 23
11. More information 23

1. JPK Transfer installation description

PRODUCT ID (Capital letters, max 9 characters):	JPKT
Product name	JPK Transfer – Sending JPK/ SAF-T files to the Ministry of Finance Gateway

JPK/ SAF-T Transfer extends the functionality of JPK/ SAF-T file preparation product. JPK / SAF-T Transfer encrypts and transforms the JPK/SAF-T files and sends them to the Ministry of Finance.



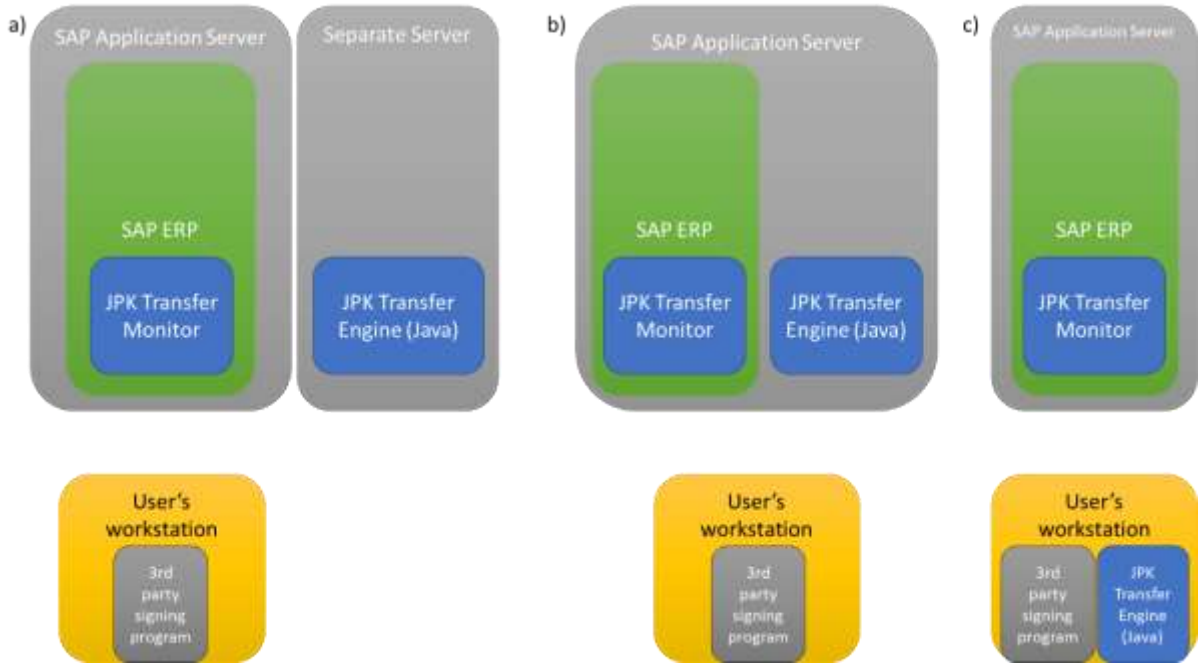
Transaction ID	Transaction description
/BCC/JPT	**JPK Transfer Monitor**
/BCC/JPTC or /BCC/JPT_CUST	JPK Transfer – Basic configuration
/BCC/JPT_XSD	JPK Transfer – XSD version settings (checking XML)
/BCC/JPT_LEP	JPK Transfer – Paths to local JPK Transfer Engine (only optionally used)
/BCC/JPT_STP	JPK Transfer – Paths and settings of local signing tool (optionally used)
/BCC/JPT_SHUTDOWN	JPK Transfer – JPK Transfer Engine shutdown

1.1. Alternative landscapes of JPK Transfer solution

JPK Transfer solution can be installed in several alternative ways depending on JPK Transfer Engine (JAVA) element positioning and depending on XML files repository access.

Alternative landscapes for JPK Transfer Engine:

a) JPK Transfer Engine installed on a separate server
b) JPK Transfer installed on SAP Application Server
c) JPK Transfer installed on User's Workstation



Solution a) is the most complex because:
- it allows having JAVA environment independent on JAVA environment on SAP Application Server
- it allows JPK Transfer Engine access internet independently of firewalls on SAP Application Server (see chapter 2 of this manual)
- it allows continuous running of JPK Transfer Engine and being used by many users.

Solution b) is an intermediate solution (medium complexity) of configuration that still can be used in quite huge deployments.

Solution c) is usually most simple to configure, but recommended only for small implementation, where JPK Transfer will be used by 1-2 persons.

Important! JPK Transfer Engine should be created in so many copies, as there are SAP system/ clients on which JPK Transfer solution will be used. If more than one copy of JPK Transfer Engine is to run, then for each copy in the *jpk.properties* file one should set different program ID (parameter JCO_PROGID=*your_new_program_ID,* default value is JPK_ENGINE)!

Possible file access settings

For XML file access usually one prepares shared *JPK network folder* (e.g.: \\office\bcc\JPK\ ). This network folder should be visible from:
- SAP Application Server
- JPK Transfer Engine
- User's Workstation (option)

In case of Solution a) and c) the URL of *JPK folder* „seen" from SAP Application Server should be, if possible, the same as „seen" from JPK Transfer Engine (not always possible when different OSs).

In case of Solutions a) and b) it is possible not to make the *JPK Folder* accessible from user's workstation. If this is the case one should use the configuration parameters (**TOSIGN_S_COPY_LOCAL**, AUTO_COPY_SIGNED (or AUTOCOPY), AUTO_START_SIGN_TOOL) allowing copying the files to be signed, to user's workstation (while starting signing tool) and copying afterwards the signed file back to the SAP Application Server (during file sending).

In case of Solution b) when using Windows server, it is recommended to map additionally the network folder as a Windows Drive letter. This allows using parameter AUTO_START_ENGINE_AS, allowing starting JPK Transfer Engine automatically.

1.2. Installation steps

Step 1. Network location for storing generated JPK files

The network folder will be used between application that generates JPK files, JPK Transfer Monitor, JPK Transfer Engine and application used for qualified signature.

1. Assign at least 200 GB (recommended 500 GB) network space (shared folder) where generated JPK files will be stored.
    a. The network space has be to accessible from both SAP (where JPK file generation [in the case of customers who purchased the solution] and JPK Transfer Monitor will be running) and a machine where JPK Transfer Engine (Java application working outside SAP) is installed.
    b. JPK Transfer Engine needs write access.
2. On the network folder unzip jpk-network-folder-structure.zip file. A new folder called JPK should be created. Inside the JPK folder, XML subfolder should be visible. **The XML folder is the one where generated JPK files must be stored** (directly in the XML folder, and not in any subfolders of the XML folder). The other folders in the JPK folder are used by JPK Transfer Engine (described below).
3. The network folder has to be available without any password

Step 2. Installation of application for qualified signature

JPK files must be signed with qualified signature solution. You may use the one you already have or if you do not have any application for qualified signature yet, please order one and install it on any computer that will have an access to the JPK folder mentioned in step 1.

Sample vendors:

- KIR: http://www.elektronicznypodpis.pl/
- Asseco / Certum: https://sklep.certum.pl/uslugi-kwalifikowane/zestawy-do-podpisu-elektronicznego/certum-mini.html
- PWPW / Sigillum: http://sigillum.pl

Step 3. Installation of *JPK Transfer Engine*

JPK Transfer Engine is an application that runs outside of SAP but it communicates with SAP via RFC interface. It can be installed on other server than the one where JPK files are stored but it has to have an access to the JPK files.

Important! It is recommended to run JPK Transfer Engine on a separate server and schedule it to start automatically (see also 2. Installation of JPK Transfer Engine as a scheduled task), so that it is always on. The JPK Transfer Engine can be alternatively run on the application server or on the user's workstation.

When the Java Transfer Engine is installed on application server, then it is possible to start it automatically when the user is using JPK Transfer transaction /BCC/JPT– see AUTO_START_ENGINE_AS setting (in configuration table /BCC/JPT_DB_TCU, transaction /BCC/JPT_CUST)

When the Java Transfer Engine is installed on user's workstation (which is not the recommended approach but is also supported), then it is possible to start it automatically when the user is using JPK Transfer transaction /BCC/JPT– see AUTO_START_ENGINE_LC setting (in configuration table /BCC/JPT_DB_TCU, transaction /BCC/JPT_CUST)

If the JPK Transfer is to work in several SAP systems/ several clients on one SAP system one should set up several instances of JPK Transfer Engine server (several copies with different properties file, other RFC connections e.g. JPK_JCO1 and JPK_JCO2 and different engine server program IDs e.g. JPK_ENGINE1 and JPK_ENGINE2).

Requirements:

1. Server with at least 4 GB (recommended 16 GB) RAM memory and CPU with at least 4 cores.
2. Operating system: Windows 7 (or newer), Windows Server 2012 (or newer) or Linux 64-bit.
3. Java 7 (1.7.0) or newer. You can check it by typing in command line:
   `java -version`
4. Access to the JPK folder from Step 1. Its name should start with \\ (for Windows) or from / (for Linux).
5. The server should be made accessible via RFC from the SAP system (opened port 33XX, where XX is the SAP system number). JPK Transfer Engine will run in server mode using dedicated SAP user account.
6. On Windows machine, Visual Studio 2005 C/C++ runtime libraries (8.0.50727.4053 or newer version) are required – download from Microsoft website if you do not have them installed on your system.
7. Connection with SAP system (under Windows check if you have an entry for sapgwXX [XX is SAP system/instance number] in system `C:\WINDOWS\system32\drivers\etc\services` file; under Linux check `/etc/services`). For example:
   `sapgw01  3301/tcp`
   Do not forget to press ENTER at the end of the above line!

Step 4. Installation of JPK Transfer Engine

1. On the server prepared in the previous step uncompress `jpk-transfer-engine-<version>.zip` file.
2. Open command line and go to `jpk-transfer-engine` folder. Run `install.bat` under Windows or `install.sh` under Linux. Follow instructions on the screen. See **Step 5.3** below for the definition of JCO_USER.
3. Edit `jpk.properties` file for RFC / Java Connector (JCo) connection between SAP and JPK Transfer Engine. **The file contains detailed description of each setting.** Do not forget to set all mandatory fields.
   a. If SAP server uses 1 application server then you have to set the following variables:
      i. JCO_ASHOST
      ii. JCO_CLIENT
      iii. JCO_SYSNR
      iv. JCO_USER
      v. JCO_LANG
      vi. JCO_GWHOST
      vii. JCO_GWSERV

   b. If SAP server uses at least 2 application servers then you have to set the following variables:
      i. JCO_CLIENT
      ii. JCO_USER
      iii. JCO_PASSWD
      iv. JCO_LANG
      v. JCO_GWHOST
      vi. JCO_GWSERV
      vii. JCO_GROUP
      viii. JCO_MSHOST
      ix. JCO_MSSERV
      x. JCO_R3NAME
   c. If a server with JPK Transfer Engine uses **proxy** then you have to set HTTP_PROXY* and HTTPS_PROXY* variables. See also chapter about the Security of JPK / SAF-T Transfer.
4. Go to jpk-transfer-engine folder and run start.bat (if you use Windows) or start.sh (in case of Linux).
5. Wait until you will see Connected! message.

In a case of any issue open jpk-transfer-engine\log\log.html file in web browser (the file contains all messages displayed in the JPK Transfer Engine window) and check jpk-transfer-engine*.trc files.

Step 5. Installation of JPK Transfer Monitor in SAP

Action	Details
Loading the transport requests given in the folders (following the order) : 0. JPK Transfer & NIP Checker BASE (**import only with first installation of version 2.0**) 1. JPK Transfer Update (**import with every update**) 2. JPK Transfer Transaction & Programs (**import with every update**) 3. NIP Checker Update **(if using NIP Checker it is recommended to use newest NIP Checker installation package for installation/ upgrade)** 4. Authorization Role Z_JPT_JCO_REGISTRATION (for RFC user) **(import with first JPK Transfer installation, later it is recommended to adjust roles manually to the examples given in section 4)** 5. Authorization Roles Z_JPT_USER (for user) Z_JPT_ADMIN (for admin) (**import with first JPK Transfer installation, later it is recommended to adjust roles manually to the examples given in section 4)** Important! If present, set the following in transport options (checkboxes) **Overwrite originals** **Ignore Invalid Component Version.**	The transport requests contain below objects in the BCC reserved namespace /BCC/: Package R3TR DEVC /BCC/JPW Package R3TR DEVC /BCC/JPT Package R3TR DEVC /BCC/JPN Role: Z_JPT_JCO_REGISTRATION, Z_JPT_USER, Z_JPT_ADMIN

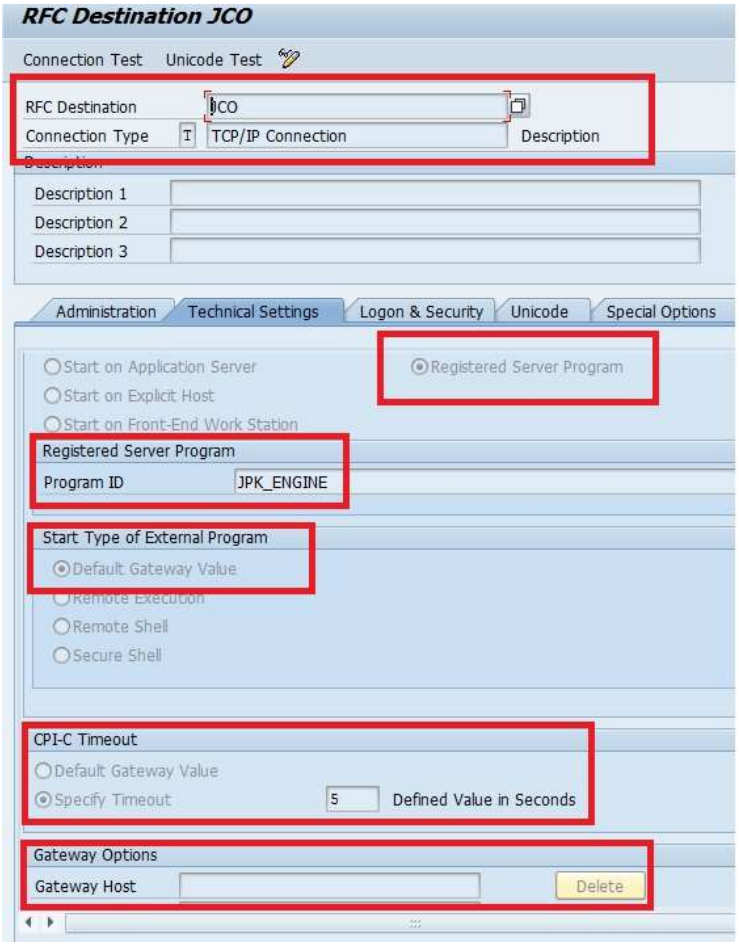
Installation steps:

Step 5.1. Load the transport requests (see numbers in the table above- column Action). You can find them in *transport*.zip* files.

Step 5.2. Create RFC connection:

Important! **If the JPK Transfer is to work in several SAP systems/ several clients on one SAP system, one should set up several instances of JPK Transfer Engine server (several copies with different properties file, other RFC connections e.g. JPK_JCO1 and JPK_JCO2 and different engine server program IDs e.g. JPK_ENGINE1 and JPK_ENGINE2).**

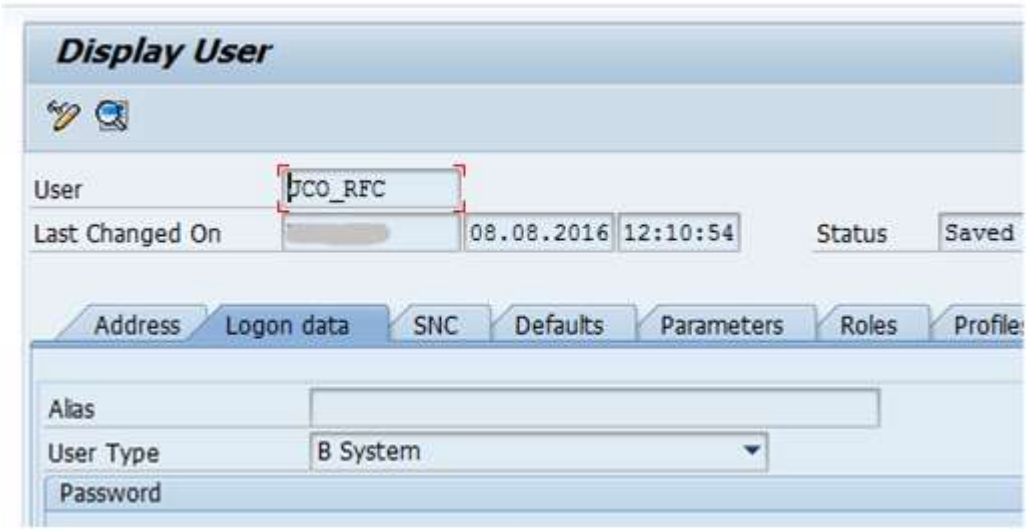
a. Go to SM59 and create new TCP/IP connection – fill in fields: RFC Destination, Activation Type, Program ID, CPI-C Timeout. Example:

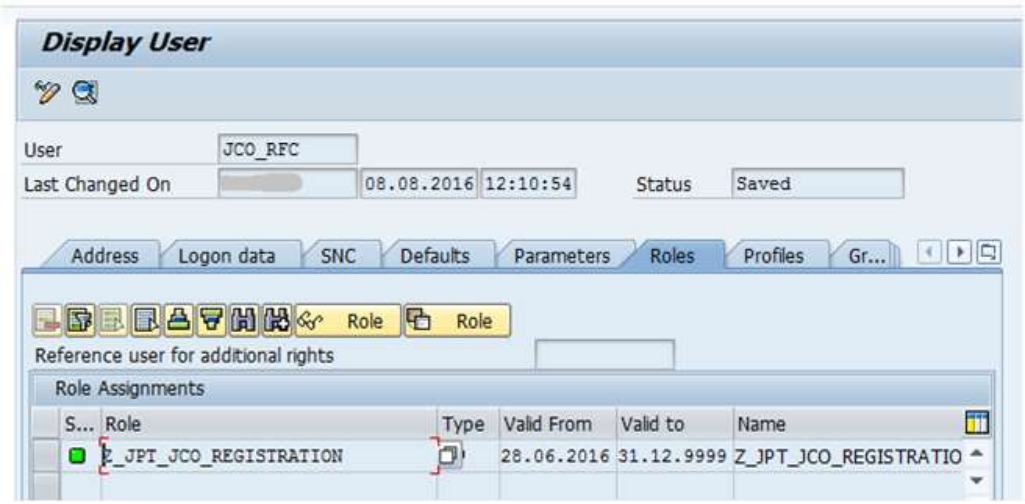


b. If you use **more than one SAP Application Server** (server group) you have to fill in the Gateway Host field (the same value as in **jpk-transfer-engine\jpk.properties** file). Otherwise the field can be empty.

c. If you want to use different Program ID you have to add a line:
JCO_PROGID=*your_new_Program_ID*
to **jpk-transfer-engine\jpk.properties** file.

Step 5.3. Create RFC user of type “B System”. Assign role: Z_JPT_JCO_REGISTRATION for created user. The role is defined in a transport file for installation of JPK Transfer




Display User
User
JCO_RFC
Last Changed On
08.08.2016
12:10:54
Status
Saved
Address
Logon data
SNC
Defaults
Parameters
Roles
Profiles
Gr...
Role
Role
Reference user for additional rights
Role Assignments
S...
Role
Type
Valid From
Valid to
Name
Z_JPT_JCO_REGISTRATION
28.06.2016
31.12.9999
Z_JPT_JCO_REGISTRATIO

Step 5.4. Populate the configuration entries in table **/BCC/JPT_DB_TCU** for each SAP system in which JPK transfer is installed (transaction **/BCC/JPT_CUST**).

a) Example of JPK Transfer configuration with JPK Transfer Engine installed on a separate server, wher user's workstation cannot access the *JPK folder* and the files to be signed are copied from the SAP Application Server to user's workstation local folder C:\LocFiles\JPK\TOSIGN, and the signed file is copied back from the same local folder to the server SIGN folder and recognized via *.XAdES extension:

JPT - tabela konfiguracyjna

JG	JPK	Klucz konfiguracyjny	Wartość klucza konfiguracyjnego
		AUTHORIZATION_CHECK	X
		AUTO_COPY_SIGNED	C:\LocFiles\JPK\TOSIGN*.XAdES
		AUTO_START_ENGINE_AS	X
		AUTO_START_SIGN_TOOL	X
		PATH_TOSIGN_S	C:\LocFiles\JPK\TOSIGN
		PATH_XML	D:\JPK\XML
		PATH_XML_MANUAL	X
		PATH_XML_SAP	
		RFC_CONNECTION	JCO
		SAVE_SENT_XML	X
		TOSIGN_S_COPY_LOCAL	X

b) Example of JPK Transfer configuration with JPK Transfer Engine installed on the SAP application server:

JG	JPK	Klucz konfiguracyjny	Wartość klucza konfiguracyjnego
		AUTHORIZATION_CHECK	X
		AUTO_START_ENGINE_AS	X
		AUTO_START_SIGN_TOOL	X
		RFC_CONNECTION	JCO
		SAVE_SENT_XML	X
Y001		PATH_TOSIGN_S	\\sato\JPK\TOSIGN
Y001		PATH_XML	D:\JPK\XML
Y001		PATH_XML_SAP	X

c) Example of JPK Transfer Monitor configuration with JPK Transfer Engine installed locally:

JPT - configuration table

CoCd	JPK	Configuration key	Configuration key value
		AUTHORIZATION_CHECK	X
		AUTO_SHUT_ENGINE_LC	X
		AUTO_START_ENGINE_LC	X
		AUTO_START_SIGN_TOOL	X
		PATH_XML_SAP	
		RFC_CONNECTION	JCO
		SAVE_SENT_XML	X
*		PATH_XML	\\office\bcc\ProjektyWewnetrzne\JPK\XML
0001		PATH_XML	\\office\bcc\JPK\0001\XML
Z100		PATH_XML	\\office\bcc\JPK\Z100\XML

Obligatory keys:

- **PATH_XML** – Path to the default directory with JPK files. This parameter define the default value of the field "Folder with JPK file" on the selection screen of /bcc/jpt transaction. Important! This configuration parameter can be given on general level (CompCode = "*" and SAF-T(JPK) type = "*") or on detailed level (for any Company Code/ SAF-T type). The path has to end with \XML or /XML depending on operating system.
- **RFC_CONNECTION** – RFC connection created in sm59. Important! This configuration parameter can be given on general level (Company Code = "*" and SAF-T(JPK) type = "*") or on detailed level (for a given Company Code without specifying the SAF-T type).

  It is recommended to set also at least following optional parameters: PATH_XML_SAP, AUTO_START_SIGN_TOOL and AUTHORIZATION_CHECK (if there are more than one company code handled by different teams).

Optional keys:

- **PATH_XML_E** – Path to the default directory with JPK files visible from JPK Engine. This parameter should be used ONLY when JPK Transfer Engine must access JPK XML files from different path then the one visible by the SAP server(e.g. access via application SAP server on Linux and JPK Transfer engine located on Windows)! This configuration parameter can be given on general level (CompCode = "*" and SAF-T(JPK) type = "*") or on detailed level (for any Company Code/ SAF-T type). The path has to end with \XML or /XML depending on operating system.
- **PATH_XML_SAP** – defines whether the "Folder with the JPK file" will be accessed from the user workstation (SAP Folder = "") or from the application server (SAP Folder = "X"). It is recommended to customize access via application server. Important!)! This configuration parameter can be given on general level (CompCode = "*" and SAF-T(JPK) type = "*") or on detailed level (for any Company Code/ SAF-T type). There can be four values given for this parameter:

Parameter value	SAP Folder checkbox default value	SAP Folder checkbox editable by user
No entry in the configuration table		Yes (for backward comaptibility)
		No
X	X	No
1		Yes (for backward comaptibility)
2	X	Yes (for backward comaptibility)

  Important! If access via application server was chosen (SAP Folder = "X"), then instead of the workstation user, the access to the folder will be executed with the authorization of the user running SAP application server - **SAPServiceXYZ**, where XYZ is SAP system SID (SAP System Identifier). To make it working you need DOMAIN/SAPServiceXYZ user who will have an access to the network folder. **PATH_XML_MANUAL** – if any value (usually X) for this key was introduced, than user can enter the XML path on it's own. The path provided by the user overwrites the patch read from configuration table. Important! This configuration parameter can be given on general level (Company Code = "*" and SAF-T(JPK) type = "*") or on detailed level (for a given Company Code / SAF-T type).
- **PATH_TOSIGN_S** – Path to TOSIGN folder used by the signature tool (when AUTO_START_SIGN_TOOL parameter is used). Parameter PATH_TOSIGN_S should be used ONLY if the TOSIGN folder cannot be derived from PATH_XML parameter

(default behavior, when PATH_TOSIGN_S is not given or empty). This configuration parameter can be given on general level (CompCode = "*" and SAF-T(JPK) type = "*") or on detailed level (for any Company Code/ SAF-T type). The path has to end with \TOSIGN or /TOSIGN depending on operating system.

- **TOSIGN_S_COPY_LOCAL** – Can be used ONLY together with PATH_TOSIGN_S (or local TOSIGN) and AUTO_COPY_SIGNED (or local AUTOCOPY) parameters. Used when user's workstation cannot access JPK folders. When not empty ("X"), forces JPK Transfer Monitor to copy file from TOSIGN folder to local workstation folder (PATH_TOSIGN_S) before signing and to copy the signed file from local folder (either PATH_TOSIGN_S, or from AUTOCOPY) into SIGN folder on the server.
- **AUTHORIZATION_CHECK** – if any value (usually X) for this key was introduced, than authorization object /BCC/JPK01 is checked for the Company Code/ SAF-T Type. Important! This configuration parameter can be given only on general level (Company Code = "*" and SAF-T(JPK) type = "*").
- **SAVE_SENT_XML** – if any value (usually X) for this key was introduced, than, when UPO confirmation is read, the XML will be compressed and saved to the index database table /bcc/jpt_db_indx. It can be later downloaded from SAP via „Download archived XML" button. Important! The button appears on the ALV screen only if archived data for selected SAF-T files exist. Important! This configuration parameter can be given on general level (Company Code = "*" and SAF-T(JPK) type = "*") or on detailed level (for a given Company Code / SAF-T type).
- **AUTO_COPY_SIGNED** – Parameter that facilitates signing of the xml file, if the signing program does not have the functionality to copy the signature file to another folder (SIGN). If this parameter has the value X, then the solution before sending the file, checks if the .xades signature file is present in folders SIGN and TOSING. If the system finds the respective file in the folder TOSIGN and the file is missing in SIGN folder, than the system moves the signature file to „SIGN" folder. Important! When other signature file extensions are used or in Unix systems in which upper cases matter, one can put filter value for signature as AUTO_COPY_SIGNED parameter value, e.g.: "*. XAdES", instead of "X" value.

  Important! For proCertum SmartSign, when copying of signed files should be done to different folders for each Company Code or JPK Type, one can configure the SmartSign to archive the signed files in one folder (let us assume D:\JPK\SS) and then JPK Transfer could copy the signed files, from that folder to respective SIGN folders. For that to work one should put path and mask inside the AUTO_COPY_SIGNED parameter value, e.g.: "D:\JPK\SS*.xml".

  Important! When AUTO_START_SIGN_TOOL is set, then the copying property can be set locally (AUTOCOPY, ALV list menu Others> Set Signing Software). If for the signing tool for the given computer other, not-empty, value of AUTOCOPY parameter is set, than computer settings takes precedence over this general AUTO_COPY_SIGNED parameter. This configuration parameter can be given only on general level (Company Code = "*" and SAF-T(JPK) type = "*").
- **AUTO_START_ENGINE_LC** – Parameter that facilitates starting JPK Transfer Engine on user's workstation, when transaction JPK Transfer (/BCC/JPT) is started by the user. This parameter is used only, when JPK Transfer Engine is not installed on the separate served, but on user's workstation (not the recommended option). When any value for this parameter is entered (usually „X"), then when the user runs JPK Transfer transaction /BCC/JPT, the system searches for the JPK Transfer engine start file and path in the table /BCC/JPT_DB_TCU3. When the entry is found for respective user's workstation, then JPK Transfer Engine is being started. Each user can have JPK Transfer Engine installed in different folder, thus each user can select the path and file to start

(usually start.bat) from the JPK Transfer transaction. With the menu *Others > Set Engine file path* accessible on the ALV screen, one can set the JPK Transfer Engine starting file. Alternatively the paths for every computer can be set by the administrator in table /BCC/JPT_DB_TCU3. This configuration parameter can be given only on general level (Company Code = "*" and SAF-T(JPK) type = "*"). See also AUTO_SHUT_ENGINE_LC parameter.

- **AUTO_SHUT_ENGINE_LC** – parameter that can be used only together with AUTO_START_ENGINE_LC parameter. Setting this parameter will allow in future version of the program to switch off the JPK Transfer Engine (JAVA) on the workstation when leaving the JPK Transfer Monitor Transaction. It will work only if the Transfer Engine was started automatically when entering the transaction. This configuration parameter can be given only on general level (Company Code = "*" and SAF-T(JPK) type = "*").
- **AUTO_START_ENGINE_AS** – Parameter that facilitates starting JPK Transfer Engine on SAP application server, when transaction JPK Transfer (/BCC/JPT) is started by the user. This parameter is used only, when JPK Transfer Engine is installed on application server. When any value for this parameter is entered (usually „X"), then when the user runs JPK Transfer transaction /BCC/JPT, the system searches for external system command (defined in SM69 transaction) **ZJPT_ENGINE_ST_XXX (where XXX depicts SAP client number)** and tries to execute it.
  The example of such a command to call D:\JPK\start.bat:
  cmd /c "D: & CD \JPK\ & start.bat"
  lub
  powershell "D: ; CD \JPK\jpk-transfer-engine\ ; Start-Process start.bat"
  The parameter _AUTO_START_ENGINE_AS can have value X, or have value of the target host on which the JPK Engine should be started.
  This configuration parameter can be given only on general level (Company Code = "*" and SAF-T(JPK) type = "*").
- **AUTO_START_SIGN_TOOL** – Parameter switching on in JPK Transfer transaction (/BCC/JPT) additional icon that allows directly call the signing tool from SAP transaction. If the parameter has the value X, then in JPK Transfer Monitor new icon appears: *Start signature*, and new option appears also in the menu *Others > Set signing software.* Setting the signing software consist of:
  - setting the path to the file starting the signing tool
  - giving the command line parameters to pass to the program (string &FILE& will be replaced by full name of the file that should be signed)
  - if the transaction should copy the signed files from TOSIGN to SIGN folders, than file extension of the signed file should be given (e.g. *.xades) If the signing program has the option to move the signed file to a given folder, than it is recommended to set it in the signing program and left the extension in SAP empty. This configuration parameter can be given only on general level (Company Code = "*" and SAF-T(JPK) type = "*").
- **EXT_FILE_MASK** – used when external files (not produced with BCC JPK File product) are sent with JPK Transfer. With this parameter one can define a mask that will be used to retrieve file attributes from filename. Without using the mask, the attributes can be given manually, but since this approach is prone to user's mistakes it is recommend to use the mask when handling files from external source. In the mask following strings/characters have special meaning:
  ? – reflects exactly 1 character in the filename

* - reflects any number of character (from 0), asterisk can be placed inside the mask string or at its end. If asterisk is placed inside the mask string, then afterwards a normal character without any special meaning should be placed, e.g. *_)
&CC& - reflects company code (4 characters)
&TY& - reflects JPK Type (2 or 3 characters)
&YF& - reflects YEAR from (4 characters)
&yf& - reflects YEAR from (2 characters)
&MF& - reflects MONTH from (2 characters)
&DF& - reflects DAY of the month from (2 characters)
&YT& - reflects YEAR to (4 characters)
&yt& - reflects YEAR to (2 characters)
&MT& - reflects MONTH to (2 characters)
&DT& - reflects DAY of the month to (2 characters)
&VE& - reflects VERSION (1 or two digits)
Example:
mask: *&CC&_&TY&_&YF&&MF&&DF&_&YT&&MT&&DT&_&VE&*
filename: Y001_VAT_20170201_20170228_10 would result in retrieving:

- Company Code Y001 (string &CC&)
- JPK Type VAT (string &TY&)
- Date from 20170201 (three strings together *&YF& &MF& &DF&)*
- Date to 20170228 (three strings together *&YT& &MT& &DT&)*
- Version 10 (string &VE&)

This configuration parameter can be given only on general level (Company Code = "*" and SAF-T(JPK) type = "*").

- **EXT_FILE_MASK_AUTO**– used only together with EXT_FILE_MASK parameter. When this parameter is set ("X"), then if all file attributes are retrieved with the mask, the file is automatically saved (the user does not need to approve the attributes by pressing the save button). This configuration parameter can be given only on general level (Company Code = "*" and SAF-T(JPK) type = "*").
- **EXT_FILE_DISTINCT** – When this parameter is set ("X"), then only distinct values of file attributes are possible. This means the system will check whether a file with the same attributes already exist and if this is the case the version will be cleared giving the user possibility to adjust the version number. This configuration parameter can be given only on general level (Company Code = "*" and SAF-T(JPK) type = "*").
- **ONLY_TEST_MODE** – when set ("X"), then only test mode can be used. Use this parameters on test systems, where sending to production server of Ministry of Finance should not be allowed.

Important! Setting in configuration table the Company Code/ SAF-T type value to "*" is equal to setting empty value and means taking into consideration all Company Codes / SAF-T file types.
Important! The XML version configuration table (/BCC/JPT_DB_TCU2) should be changed via configuration transports given by BCC. Entry in this table should refer to respective xsd files in \JPK\XSD\ folder . In case of manual entry in this table, the relevant XSD version file should be added to \JPK\XSD\ folder.

Step 5.5. Adjust Gateway Security Files:
Please add the below line to the reginfo file, on the ABAP system (to enable connection between ABAP system and JPK_ENGINE program):

```
P TP=JPK_ENGINE HOST=* CANCEL=* ACCESS=*
```

and the following line to secinfo file:

```
P TP=JPK_ENGINE HOST=XX CANCEL=* ACCESS=*
```

where *XX* is the fully qualified domain name (FQDN) that runs JPK Transfer Engine.
Check if the first line in the secinfo/reginfo file is:
#VERSION=2

You can find the files in the subfolder “DATA” of the SAP instance folder.
Once the file is updated, please refresh GATEWAY configuration.
Tcode: SMGW – please choose from menu:
Goto -> Expert Functions -> External Security -> Reread.

2. Installation of JPK Transfer Engine as a scheduled task

The JPK Transfer engine can be installed:
- on a separate server, that can connect via RFC with SAP (recommended)
- on the SAP application server (see AUTO_START_ENGINE_AS config parameter)
- on user's workstation (see AUTO_START_ENGINE_LC, AUTO_SHUT_ENGINE_LC config parameters)

If the JPK Transfer engine is to be run on a separate server, than the administrator can add JPK Transfer Engine to Scheduled Task (Windows only). After saving the task and restarting computer, the JPK Transfer Engine should run in the background even if user in not logged in.

1. Open a command prompt. To open a command prompt, click **Start** , click **All Programs** , click **Accessories** , and then click **Command Prompt** . At the command prompt, type **Taskschd.msc.** Alternatively type **Taskschd.msc** in the windows search for the programs and files window and select the found program.
2. In the left window, on "Task Scheduler Library" with right mouse click from context menu select "New Folder…" and give it a name e.g. "JPK"
3. On the "JPK" Folder from the context menu select "Create basic task"…
    1. Name and description anything meaningful
    2. Trigger "When the computer starts"
    3. Action "Start a program" > Path (to the jpk-transfer-engine\start.bat) start in (path to jpk-transfer-engine\ folder)
    4. Finish (click Open the properties Panel when …)
    5. Task Properties:
        1. General tab: Check Run, whether the user is logged or not
        2. General tab: Check Run with highest privileges
        3. Conditions tab: Uncheck Start the task only if the computer is on AC power
        4. Conditions tab: Check Wake this computer to run this task
        5. Settings tab: Check Run task as soon as possible after the scheduled start is missed
        6. Settings tab: Check If the task fails, restart every
        7. Settings tab: Uncheck Stop the tasks if it runs longer that

3. Security of JPK / SAF-T Transfer

JPK Transfer Engine connects with SAP system (through RFC JCo connection) and with 3 external hosts:

1. e-dokumenty.mf.gov.pl (port SSL 443) – only in production mode of JPK Transfer Monitor
2. test-e-dokumenty.mf.gov.pl (port SSL 443) – only in test mode of JPK Transfer Monitor
3. *.blob.core.windows.net (port SSL 443) – group of servers (host name can be vary) used by JPK Transfer Monitor while sending files to the Ministry of Finance
4. crd.gov.pl (port HTTP 80) – used by JPK validation

4. Authorizations of SAP users in JPK / SAF-T Transfer

4.1. Authorizations for remote user (connection from/to JPK Engine)

This user should be entered in properties file of JPK Engine. The user should use role **Z_JPT_JCO_REGISTRATION** provided together with JPK Transfer installation files (one can use also a copy of this role).

Important: When upgrading from version lower than 2.0 either upload the new transport request with the updated role or if you maintain the role manually add the following authorization objects:

S_DATASET:
ACTVT 33
FILENAME *
PROGRAM /BCC/JPT_CL_UTILS==========CP

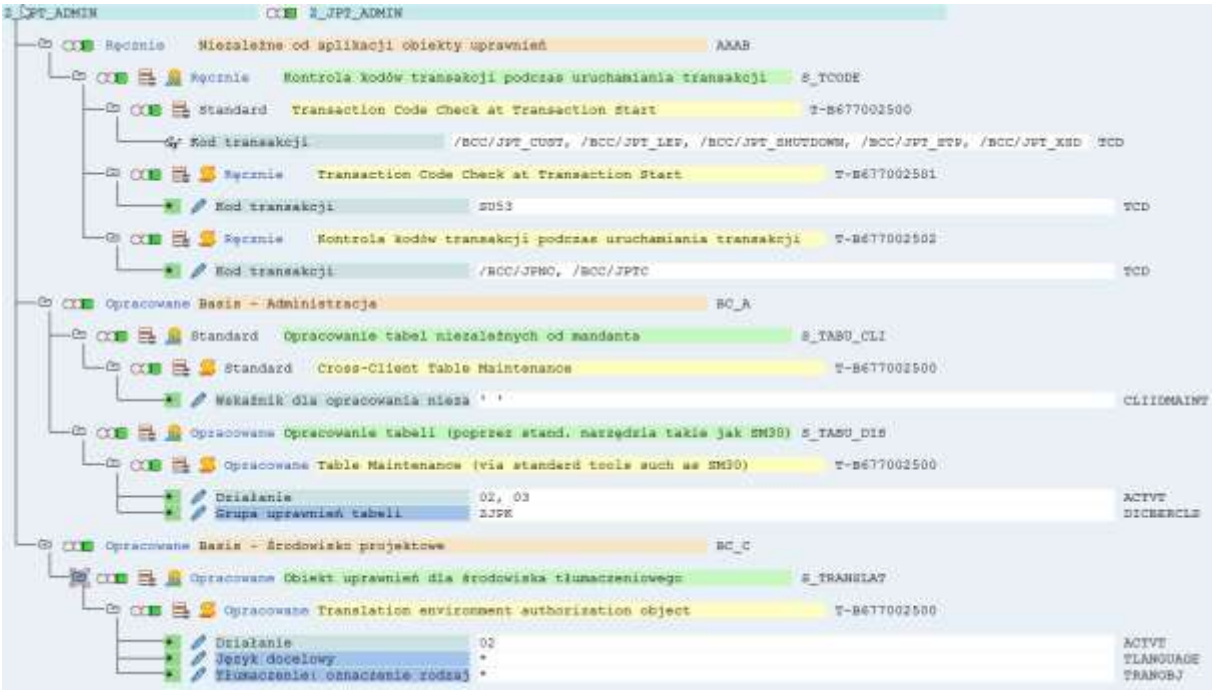
S_RFC
RFC_TYPE: FUGR
RFC_NAME: SDIFRUNTIME

4.2. Authorizations for end user sending files

User validating, preparing and sending XML files with JPK Transfer solution, should have at least following authorizations (object **/BCC/JPK01** can be adjusted to user organizational position and is used only when AUTHORIZATION_CHECK parameter is set in the configuration table):
Object S_DATASET is only needed when access to files is done via application server (SAP Folder switch). Objects S_DATASET filed FILENAME can be adjusted to the required JPK folder.
Object S_LOG_COM is only needed when automatic start of JPK Transfer Engine on application server is used (configuration parameter AUTO_START_ENGINE_AS).

4.3. Authorizations for JPK administrator changing JPK customizing tables in the SAP system

User that changes entries in the JPK Transfer customizing tables /BCC/JPT_DB_TCU* using transactions (/BCC/JPT_CUST (or /BCC/JPTC), /BCC/JPT_XSD, /BCC/JPT_LEP, /BCC/JPT_STP, /BCC/JPT_SHUTDOWN) requires following authorizations.



5. JPK Transfer update description

Steps:

1. JPK Transfer Monitor
    a. Log out from Monitor
    b. Load new transport files (this is a full version; no need to load files from the previous versions)
    c. Consider using new configuration parameters (SM30 table /BCC/JPT_DB_TCU) described in section 1, step 4.
    d. Check in section 4, whether the new version does not require more user authorizations, and grant them if applicable.
2. JPK Transfer Engine (upgrade required only with main product version changes e.x. 2.0 => 2.1)
    a. Close Engine (close the application's console window)
    b. Copy jpk-transfer-engine\jpk.properties file to an external folder
    c. Remove jpk-transfer-engine folder
    d. Unzip jpk-transfer-engine-*.zip file
    e. To new jpk-transfer-engine\jpk.properties file copy the contents of the earlier version of jpk.properties file
    f. Run Engine (jpk-transfer-engine\start.bat – in Windows or start.sh – in Linux)

You have to update both Monitor and Engine at the same time! Do not run any of them unless both are updated!

6. JPK Transfer XSD version configuration

Transaction **/BCC/JPT_XSD** can be used to set the valid XSD (XML Schema Definition) files for JPK files depending on time. The transaction changes entries in table /BCC/JPT_DB_TCU2. Normally these entries should be provided by BCC in form of transport requests. But in the case of urgent changes the JPK administrator can adjust the entries manually. In the case of adding a new entry to the table one should add correctly named XSD file to the XSD folder. The hidden global parameter VER_DEP_ON_DATA_DATE governs whether configuration data relates to system date (default) or to start date of the data range (VER_DEP_ON_DATA_DATE=X).

7. JPK Transfer Engine local paths

Transaction **/BCC/JPT_LEP** can be used to set the paths to local (placed on user's workstation) files starting JPK Transfer Engine (Java) in the table /BCC/JPT_DB_TCU3. This table is used only when configuration parameter **AUTO_START_ENGINE_LC** is set. Normally the entries are maintained by users themselves. They can define the path to the JPK Transfer Engine files via menu option *Others > Set Engine file path.* Transaction **/BCC/JPT_LEP** gives the possibility to the administrator to change/ prepare the entries in the table /BCC/JPT_DB_TCU3 manually.

8. Signing tools start for local user configuration

Transaction **/BCC/JPT_STP** can be used to configure executing signing process from JPK Transfer Monitor transaction (signing programs must be placed on user's workstation). Normally the entries in table /BCC/JPT_DB_TCU4 are configured via end user for themselves via menu *Others* in transaction /BCC/JPT. The entries are only relevant for the JPK Transfer monitor if general setting **AUTO_START_SIGN_TOOL** is set. The administrator can maintain entries of the signing tool start configuration for all user's workstations regarding:
- paths to the executable files starting the signing tool
- command line parameters used while execution
- defining file masks (extensions e.g. *.xades, called AUTOCOPY) that allow SAP to copy signed files from TOSIGN to SIGN folder (used only when signing tool cannot do it, should be left empty if the signing program already copies the file). This setting can be also left empty. See also **AUTO_COPY_SIGNED** configuration parameter (local user setting precedes global configuration parameter). Important! Special value *NOT* inactivates the auto copying function irrespective of the AUTO_COPY_SIGNED setting.
- define TOSIGN local folder paths in the case that the folders on user computer are different that the folders used in JPK Transfer Engine (e.g. JPK Transfer Engine an application server on UNIX, and user workstation on Windows). This setting can be also left empty. See also **PATH_TOSIGN_S** configuration parameter (local user setting precedes global configuration parameter).

When defining command line parameters one can use special codes that will be replaced with real values during runtime:

&FILE&	- full path to the file to be signed
&FOLDER&	- folder of the file to be signed
&TFOLDER&	- target folder when the signed files
&FILESHORT&	- filename of the file to be signed (without full path)
&JPKTYP&	- JPK type ID
&BUKRS&	- Company code ID

9. JPK Transfer Engine shutdown

Transaction **/BCC/JPT_SHUTDOWN** can be used to shut the JPK Transfer Engine down from within the SAP system. In test mode the transaction verifies the connection to the JPK Transfer Engine, in actual sends shutdown requests to the JPK Transfer Engine.

10. Certificates required for connection with external HTTPS services

The certificates are stored at **ssl_certificates.jks** file and are given by BCC with the installation package. However after some time due to Ministry of Finance of Poland infrastructure changes new certificates may be needed. For maintenance customers updated certificate files will be furnished by BCC.

Starting from version 2.0 009 the administrators can add certificates to Transfer Engine on their own. The certificates can be added via **keytool** program (should be stored in your java bin directory).
To add certificates to **ssl_certificates.jks** file one can execute the command (in the directory with ssl_certificates.jks file):

keytool -importcert -file certificate.cer -keystore ssl_certificates.jks -alias "alias"

Example:
C:\java\bin\keytool -importcert -file services-jpk.bcc.com.pl.cer -keystore ssl_certificates.jks -alias "services-jpk.bcc.com.pl"

Password ssl_certificates.jks:
@zTL98s!32fk

11. More information

More information can be found in User's Manual or on https://jpk.bcc.com.pl