
	<p>JPk / SAF-T Transfer</p> <p>Administrator Installation Manual</p>	
	Version: 2017-02-10 (1.2/009)	

Table of contents

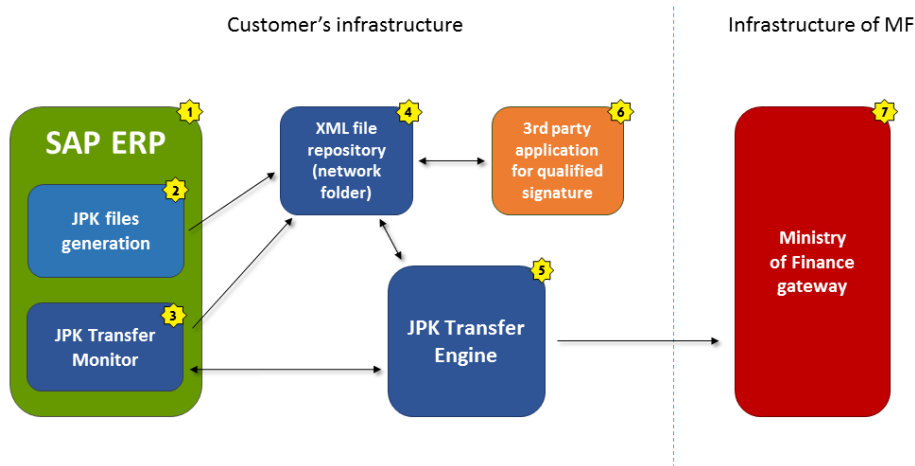
1. JPK Transfer installation description.....	2
1.1. Installation steps	2
2. Installation of JPK Transfer Engine as a scheduled task	11
3. Security of JPK / SAF-T Transfer	12
4. Authorizations of SAP users in JPK / SAF-T Transfer	13
5. JPK Transfer update description.....	16
6. JPK Transfer XSD version configuration.....	17
7. JPK Transfer Engine local paths	17
8. Signing tools local user configuration	17
9. More information	17

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.

JPK Transfer – architecture



Transaction ID	Transaction description
/BCC/JPT	JPK Transfer Monitor
/BCC/JPT_CUST	JPK Transfer – 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)
	JPK Transfer – Paths and settings of local signing tool
/BCC/JPT_SHUTDOWN	JPK Transfer – JPK Transfer Engine shutdown (NOT used in this version)

1.1. 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 where generated JPK files will be stored. The network space has to be 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.
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.** 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/>
- Certum: <https://sklep.certum.pl/uslugi-kwalifikowane/zestawy-do-podpisu-elektronicznego/certum-mini.html>
- 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 user's workstation. Although this is not recommended approach it is also supported. When the Java Transfer Engine is installed on user's workstation, then it is possible to start it automatically when the user is using JPK Transfer transaction /BCC/JPT– see AUTO_START_ENGINE_LC settings (in configuration table /BCC/JPT_DB_TCU)

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.
2. Edit jpk.properties file for RFC / Java Connector (JCo) connection between SAP and JPK Transfer Engine. The file contains detailed explanation of each option. 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_PASSWD
 - vi. JCO_LANG
 - vii. JCO_GWHOST
 - viii. 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*.
- 3. Run jpk-transfer-engine\start.bat (if you use Windows) or start.sh (in case of Linux).
- 4. Wait until you will see "Connected!" message.

In case of any issue open jpk-transfer-engine\log\log.html 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 in the given order: 910487 – JPKT solution 910381 – role Z_JPT_JCO_REGISTRATION Important! If present, set in transport options, the checkbox 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 Role: Z_JPT_JCO_REGISTRATION

Installation steps:

1. Load the transport requests (see numbers in the table above- column Action)
2. Create RFC connection:

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

Example on the below screen:

RFC Destination JCO

Connection Test Unicode Test

RFC Destination: JCO

Connection Type: TCP/IP Connection

Description:

Description 1:
Description 2:
Description 3:

Administration **Technical Settings** Logon & Security Unicode Special Options

☐ Start on Application Server
☐ Start on Explicit Host
☐ Start on Front-End Work Station
☒ **Registered Server Program**

Registered Server Program

Program ID: JPK_ENGINE

Start Type of External Program

☒ Default Gateway Value
☐ Remote Execution
☐ Remote Shell
☐ Secure Shell

CPI-C Timeout

☐ Default Gateway Value
☒ Specify Timeout 5 Defined Value in Seconds

Gateway Options

Gateway Host: Delete

Note 1

If you use more than one SAP Application Server 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.

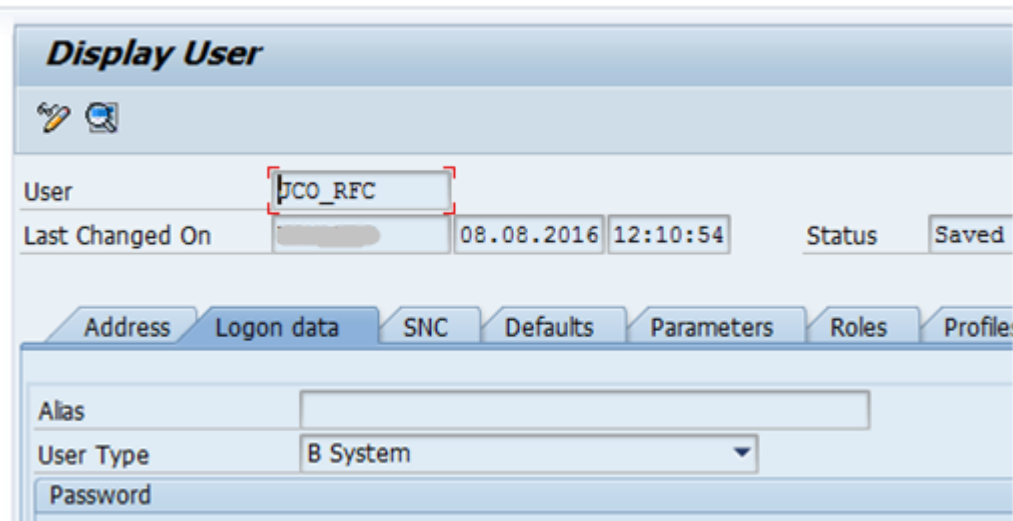
Note 2

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.

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

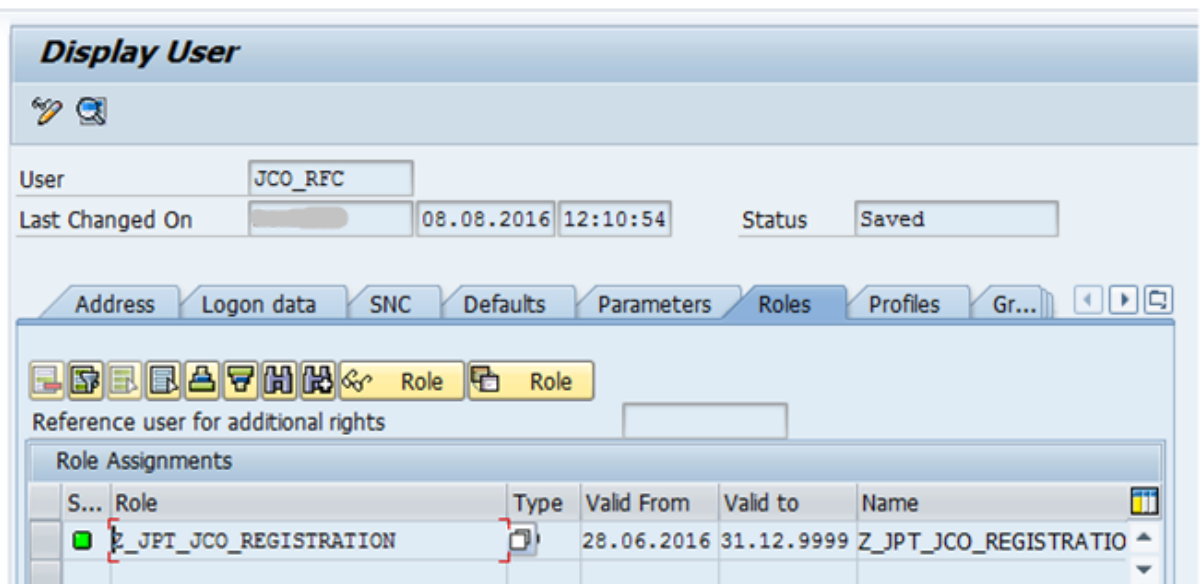
Status: Saved

Address Logon data SNC Defaults Parameters Roles Profiles

Alias

User Type: B System

Password



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

S...	Role	Type	Valid From	Valid to	Name
█	Z_JPT_JCO_REGISTRATION		28.06.2016	31.12.9999	Z_JPT_JCO_REGISTRATIO

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**).

Example of JPK Transfer Monitor configuration:

CoCd	JPK	Configuration key	Configuration key value
		AUTHORIZATION_CHECK	X
		AUTO_COPY_SIGNED	*.xades
		PATH_XML_SAP	X
		RFC_CONNECTION	JCO
		SAVE_SENT_XML	X
0001		PATH_XML	\\office\bcc\0001\JPK\XML
Y001		PATH_XML	\\office\bcc\Y001\JPK\XML

Obligatory keys:

- **PATH_XML** – Path to the default directory with JPK files. This parameter defines 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).
- **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).

Optional keys:

- **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 only on general level (Company Code = "*" and SAF-T(JPK) 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 compatibility)
		No
X	X	No
1		Yes (for backward compatibility)
2	X	Yes (for backward compatibility)

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. You also need entry in SAP in the AL11 transaction to point to the "JPK" folder (e.g.: [\\somenetworkpath\JPK](#)), or alternatively three separate entries pointing to XML,

TOSIGN, SIGN folders). Important! On the linux system these folders should be in capital letters.

- **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).
- **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). Important! Setting SAVE_SENT_XML works only if the XML folder can be accessed via application server (since the saving is done in the background when the answer is received)!
- **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 TOSIGN. 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! When AUTO_START_SIGN_TOOL is set, then the copying property is set locally and AUTO_COPY_SIGNED is used only as default value. If for the signing tool for the given computer other 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 = "*").

- 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) **ZIPT_ENGINE_START** and tries to execute it. The example of such a command to call D:\JPK\start.bat:
 cmd /c "D: & CD \JPK\ & 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 = “*”).
- 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 = “*”). Important! IN THIS PROGRAM VERSION THIS PARAMETER IS NOT USED. IT IS DESIGNED FOR FUTURE PROGRAM VERSIONS.

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.

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 config parameter)

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 is 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 for upgrades of JPK Transfers solution (when not importing new Z_JPT_JCO_REGISTRATION role)! A new functionality introduced on 2016.11.16 of automatic import into SAP system of xml-type JPK file, while importing UPO from Ministry of Finance, requires **new authorizations**. It means the SAP user used in RFC communication between SAP (JPK Transfer Monitor) and JPK Transfer Engine should have the following ones:

- object S_DATASET: field ACTVT value 33, field FILENAME value JPK files folder with
* at the end, field PROGRAM value /BCC/JPT_CL_UTILS=====CP , e.g.:

Uprawnienie dla dostępu do pliku		S_DATASET
Działanie	33	ACTVT
Nazwa pliku	*	FILENAME
Nazwa programu z pomocą wysz.	/BCC/JPT_CL_UTILS=====CP	PROGRAM

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**).

The screenshot displays the SAP authorization object tree for user **Z_JPT_USER**. The tree is organized into several main categories, each with a 'Manually' icon and a description. The categories and their details are as follows:

- Cross-application Authorization Objects (AAAB)**
 - Transaction Code Check at Transaction Start (S_TCODE)**
 - Standard: *Kontrola kodów transakcji podczas uruchamiania transakcji* (T-B677002400)
 - Transaction Code: **/BCC/JPT** (TCD)
 - Kontrola kodów transakcji podczas uruchamiania transakcji (T-B677002401)**
 - Transaction Code: **SU53** (TCD)
- Basis: Administration (BC_A)**
 - Authorization for file access (S_DATASET)**
 - Manually: *Uprawnienie dla dostępu do pliku* (T-B677002400)
 - Activity: ***** (ACTVT)
 - Physical file name: ***** (FILENAME)
 - Program Name with Search Help: **/BCC/JPT_P_MONITOR** (PROGRAM)
 - Authorization for GUI activities (S_GUI)**
 - Manually: *Uprawnienie do działań GUI* (T-B677002400)
 - Activity: **02, 61** (ACTVT)
 - Authorization to Execute Logical Operating System Commands (S_LOG_COM)**
 - Manually: *Authorization to Execute Logical Operating System Commands* (T-B677002400)
 - Logical command name: **ZJPT_ENGINE_START** (COMMAND)
 - Name of Current Application Se: ***** (HOST)
 - Operating System of Applicatio: ***** (OPSYSTEM)
- Basis - Central Functions (BC_Z)**
 - ALV Standard Layout (S_ALV_LAYO)**
 - Manually: *Standardowy układ ALV* (T-B677002400)
 - Activity: **23** (ACTVT)
 - ALV Report-Specific Layouts (S_ALV_LAYR)**
 - Manually: *Układy specyficzne dla raportów ALV* (T-B677002400)
 - Activity: **23** (ACTVT)
 - Mgt. ID for repeated calls fro: ***** (HANDLE)
 - Logical group name: ***** (LOG_GROUP)
 - ABAP Program Name: **/BCC/JPT_P_MONITOR** (REPORT)
- ZJPK**
 - /BCC/JPK01**
 - Manually: *Jednostka gospodarcza i typ pliku JPK* (T-B677002400)
 - JPK file type: ***** (/BCC/JPK_T)
 - Company Code: ***** (BUKRS)

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, /BCC/JPT_XSD, /BCC/JPT_LEP, /BCC/JPT_STP, /BCC/JPT_SHUTDOWN) requires following authorizations.

Z_JPT_ADMIN				JPK Transfer administrator			
				Cross-application Authorization Objects			
				AAAB			
				Transaction Code Check at Transaction Start			
				S_TCODE			
				Transaction Code Check at Transaction Start			
				T-B677002500			
				Transaction Code			
				/BCC/JPT_CUST, /BCC/JPT_LEP, /BCC/JPT_SHUTDOWN, /BCC/JPT_STP, /BCC/JPT_XSD			
				TCD			
				Transaction Code Check at Transaction Start			
				T-B677002501			
				Transaction Code			
				SU53			
				TCD			
				Basis: Administration			
				BC_A			
				Cross-Client Table Maintenance			
				S_TABU_CLI			
				Cross-Client Table Maintenance			
				T-B677002500			
				Indicator for cross-client mai			
				CLIIDMAINT			
				Table Maintenance (via standard tools such as SM30)			
				S_TABU_DIS			
				Table Maintenance (via standard tools such as SM30)			
				T-B677002500			
				Activity			
				02, 03			
				ACTVT			
				Table Authorization Group			
				ZJPK			
				DICBERCLS			
				Basis - Development Environment			
				BC_C			
				Translation environment authorization object			
				S_TRANSLAT			
				Translation environment authorization object			
				T-B677002500			
				Activity			
				02			
				ACTVT			
				Target language			
				*			
				TLANGUAGE			
				Translation: Text type name			
				*			
				TRANOBJ			

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
 - 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 signing tool start configuration for all user's workstations regarding:

- paths to the files executing the signing tool
- command line parameters used while execution
- defining file masks (extensions e.g. *.xades) 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)
- define TOSIGN local folder paths in the case that the folders on user computer are different than the folders used in JPK Transfer Engine (e.g. JPK Transfer Engine an application server on UNIX, and user workstation on Windows)

9. More information

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