
	<p>JPK / SAF-T Transfer</p> <p>Instalacja produktu</p>	
	Wersja: 2018-04-24 (2.0/010)	

Spis treści

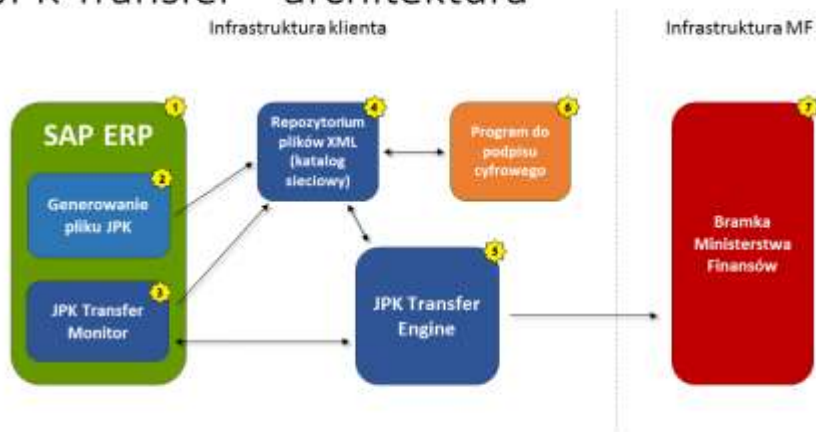
1. Opis instalacji produktu JPK / SAF-T Transfer	2
1.1. Alternatywy instalacji komponentów rozwiązania JPK Transfer	3
1.2. Kroki instalacji	4
2. Instalacja JPK Transfer Engine w Harmonogramie Zadań (opcja)	16
3. Bezpieczeństwo JPK / SAF-T Transfer.....	17
4. Uprawnienia użytkowników SAP rozwiązania JPK / SAF-T Transfer.....	18
5. Opis uaktualnienia produktu JPK / SAF-T Transfer.....	21
6. Konfiguracja plików XSD (schematy sprawdzenia plików XML)	22
7. Lokalne ścieżki do silników JPK na komputerach użytkownika (opcja)	22
8. Ustawienia ścieżek i konfiguracja lokalnych narzędzi podpisujących na komputerach użytkownika (opcja)	22
9. Shutdown serwera JPK Transfer Engine (opcja)	23
10. Certyfikaty konieczne do połączenia z zewnętrznymi systemami	23
11. Więcej informacji	23

1. Opis instalacji produktu JPK / SAF-T Transfer

ID PRODUKTU (duże litery, max 9 znaków):	JPK / SAF-T Transfer
Nazwa produktu	JPK Transfer – Wysyłka plików JPK/ SAF-T do ministerstwa finansów

JPK/ SAF-T Transfer rozszerza funkcjonalność JPK/ SAF-T w SAPie (przygotowanie plików JPK). JPK / SAF-T Transfer szyfruje i transformuje pliki JPK do odpowiedniego formatu, a następnie wysyła na bramkę Ministerstwa Finansów.

JPK Transfer – architektura



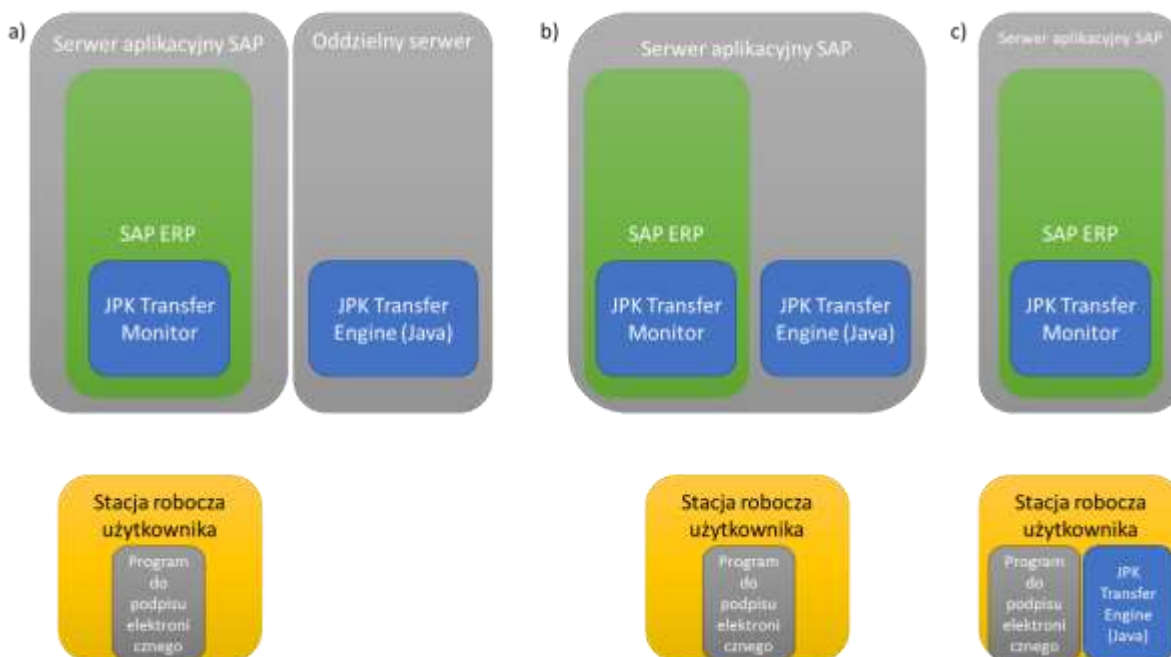
ID transakcji	Opis transakcji
/BCC/JPT	JPK Transfer Monitor
/BCC/JPTC or /BCC/JPT_CUST	JPK Transfer – konfiguracja
/BCC/JPT_XSD	JPK Transfer – ustawienia wersji XSD (sprawdzanie XML)
/BCC/JPT_LEP	JPK Transfer – Ścieżki do lokalnego JPK Transfer Engine (używane opcjonalnie)
/BCC/JPT_STP	JPK Transfer – Ścieżki i ustawienia narzędzia podpisu (używane opcjonalnie)
/BCC/JPT_SHUTDOWN	JPK Transfer – Wyłączanie JPK Transfer Engine

1.1. Alternatywy instalacji komponentów rozwiązania JPK Transfer

Rozwiązanie JPK Transfer może być zainstalowane w kilku konfiguracjach, zależnie od umiejscowienia komponentu JPK Transfer Engine (JAVA) i zależnie od tego, jak dostępne jest repozytorium plików XML (najczęściej współdzielony katalog sieciowy).

Możliwe konfiguracje JPK Transfer Engine:

- JPK Transfer Engine zainstalowany na osobnym serwerze
- JPK Transfer zainstalowany na serwerze aplikacyjnym SAP
- JPK Transfer zainstalowany na stacji roboczej klienta



Rozwiązanie a) jest rozwiązaniem najbardziej złożonym:

- pozwala na upgrade środowiska JAVA dla Transfer Engine niezależną od serwera aplikacyjnego
- pozwala na zarządzanie dostępem do Internetu (patrz rozdział 2 niniejszej instrukcji) dla JPK Transfer Engine niezależne od serwera aplikacyjnego SAP
- pozwala na ciągłą pracę JPK Transfer Engine i wykorzystywanie przez wielu użytkowników.

Rozwiązanie b) jest rozwiązaniem pośrednim:

- pozwala na ciągłą pracę JPK Transfer Engine i wykorzystywanie przez wielu użytkowników,
- wersja JAVA zainstalowana na serwerze aplikacyjnym musi być odpowiednia dla JPK Transfer Engine,
- dostęp do Internetu (wybrane strony usługi JPK) z poziomu serwera aplikacyjnego (można wykorzystywać proxy),
- można korzystać ze serwera współdzielonego katalogu sieciowego (zamontowanego jako napęd (drive) na serwerze aplikacyjnym) lub bezpośrednio z katalogu serwera aplikacyjnego do składowania plików XML.

Rozwiązanie c) jest zazwyczaj najprostsze w konfiguracji ale jest zalecane tylko najmniejszym przedsiębiorstwom, w których z rozwiązania JPK Transfer Engine korzysta 1-2 osoby.

Uwaga! JPK Transfer Engine musi występować w tylu kopiach, na ilu systemach SAP/ mandantach ma być wykorzystywany JPK Transfer. Gdy działać ma więcej niż jedna kopia JPK Transfer Engine, każdej

kopii należy w pliku właściwości (plik jpk.properties) ustawić odmienne ID programu serwera (parametr JCO_PROGID=*twój_nowy_ID_programu*, domyślnie ustawiono JPK_ENGINE)!

Możliwe konfiguracje dostępu do plików

Na potrzeby dostępu do plików XML najlepiej przygotować współdzielony *folder sieciowy JPK* (przykład: \\office\bcc\JPK\) „widziany” przez:

- Serwer Aplikacyjny SAP
- JPK Transfer Engine
- Stację Roboczą użytkownika (opcja)

W przypadku konfiguracji a) i c) najlepiej gdy URL *folderu JPK* „widziany” od strony Serwera Aplikacyjnego SAP jest taki sam jak URL widziany od strony JPK Transfer Engine (nie zawsze możliwe gdy inne systemy operacyjne).

W przypadku konfiguracji a) i b) możliwe jest zrezygnowanie udostępniania *folderu sieciowego JPK* Stacji Roboczej użytkownika. W takim przypadku należy wykorzystać łącznie parametry (**TOSIGN_S_COPY_LOCAL**, **AUTO_COPY_SIGNED** (lub **AUTOCOPY**), **AUTO_START_SIGN_TOOL**) umożliwiające przekopiowanie plików do podpisu z serwera aplikacyjnego SAP na stację roboczą użytkownika (podczas uruchamiania podpisu) oraz skopiowanie pliku podpisanego z powrotem na serwer aplikacyjny SAP (w momencie wysyłki).

W przypadku konfiguracji b) na serwerze aplikacyjnym Windows, zalecane jest dodatkowo, by współdzielony folder sieciowy zmapowany był jako dysk w systemie Windows serwera aplikacyjnego. Pozwala to na użycie parametru **AUTO_START_ENGINE_AS**, umożliwiającego automatyczne uruchamianie JPK Transfer Engine.

1.2. Kroki instalacji

Krok 1. Folder sieciowy dla wygenerowanych plików JPK

Folder sieciowy będzie używany do komunikacji między aplikacją generującą pliki JPK, aplikacjami JPK Transfer Monitor i JPK Transfer Engine oraz aplikacją do podpisu kwalifikowanego.

1. Wyznacz przynajmniej 200 GB (zalecane 500 GB) przestrzeni na dysku sieciowym (folder sieciowy), gdzie będą przechowywane wygenerowane pliki JPK.
 - a. Ta przestrzeń dyskowa musi być widoczna zarówno z SAPa (dla aplikacji JPK Transfer Monitor) jak i z niżej opisanej aplikacji JPK Transfer Engine (aplikacji napisanej w Javie, działającej poza SAPem).
 - b. JPK Transfer Engine potrzebuje prawa zapisu do tego folderu.
2. W tej przestrzeni dyskowej rozpakuj plik **jpk-network-folder-structure.zip**. Powstanie nowy folder o nazwie **JPK**. Wewnątrz niego znajduje się podfolder XML. **Do folderu XML mają trafiać wygenerowane pliki JPK (bezpośrednio do folderu, nie np. do podfolderów folderu XML)**. Inne foldery w katalogu JPK są wykorzystywane przez JPK Transfer Engine (silnik wysyłki JAVA).
3. Ten folder sieciowy musi być dostępny bez podania hasła.

Krok 2. Instalacja aplikacji do podpisu kwalifikowanego

Pliki JPK muszą być podpisane podpisem kwalifikowanym. Mogą Państwo wykorzystać posiadane rozwiązanie lub jeśli nie posiadają jeszcze Państwo aplikacji do podpisu kwalifikowanego należy zamówić go u jednego z dostawców i zainstalować na dowolnym komputerze, który ma dostęp do zapisu do katalogu JPK wymienionego w kroku 1 powyżej.

Przykładowi dostawcy:

- 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>

Krok 3. Przygotowanie serwera dla JPK Transfer Engine (silnik wysyłki JPK)

JPK Transfer Engine to aplikacja działająca poza SAPem, ale komunikująca się z SAPem poprzez interfejs RFC. Może być uruchomiona na innym serwerze niż ten, na którym znajdują się pliki JPK, jednak musi mieć dostęp do folderu z plikami JPK.

Uwaga! Rekomenduje się instalowanie JPK Transfer Engine (silnik JPK) na osobnym serwerze z dostępem do plików JPK w katalogach dzielonych, do których dostęp ma także serwer aplikacyjny SAP. W tym przypadku zaleca się uruchamianie tego serwera automatycznie (patrz rozdział 2. Instalacja JPK Transfer Engine w Harmonogramie Zadań) tak by był ciągle włączony. Istnieje możliwość uruchamiania JPK Transfer Engine bezpośrednio na serwerze aplikacyjnym SAP lub na stacji roboczej użytkownika korzystającego z JPK Transfer.

W przypadku instalacji JPK Transfer Engine (silnik wysyłki JPK JAVA) na serwerze aplikacyjnym SAP warto wykorzystać parametr konfiguracyjny `AUTO_START_ENGINE_AS` (transakcja/BCC/JPT_CUST) pozwalający na automatyczne uruchamianie silnika wysyłki po uruchomieniu przez użytkownika transakcji JPK Transfer /BCC/JPT.

W przypadku instalacji JPK Transfer Engine (silnik wysyłki JPK JAVA) na komputerze użytkownika końcowego (to podejście nie jest rekomendowane, jest jednakże wspierane) warto wykorzystać parametr konfiguracyjny `AUTO_START_ENGINE_LC` (transakcja/BCC/JPT_CUST) pozwalający na automatyczne uruchamianie silnika wysyłki po uruchomieniu przez użytkownika transakcji JPK Transfer /BCC/JPT.

W przypadku gdy JPK Transfer ma działać na kilku systemach SAP/ mandantach należy uruchomić kilka instancji serwera JPK Transfer Engine (kilka osobnych kopii, z odmienną konfiguracją pliku `properties`, oddzielone połączenia RFC np. `JPK_JCO1` i `JPK2_JCO2` i różne ID programu serwera np. `JPK_ENGINE1` i `JPK_ENGINE2`).

Wymagania:

1. Serwer z co najmniej 4 GB (rekomendowane 16 GB) pamięci RAM i procesorem z co najmniej 4 rdzeniami.
2. System operacyjny: Windows 7 (lub nowszy), Windows Server 2012 (lub nowszy) lub Linux 64-bit.
3. Java 7 (1.7.0) lub nowsza. Możesz to sprawdzić wpisując w linii komend:
`java -version`
4. Dostęp do katalogu JPK z kroku 1. Jego nazwa powinna zaczynać się od `\\` (dla systemu Windows) lub `/` (dla systemu Linux).
5. Serwer musi być dostępny poprzez interfejs RFC z systemu SAP (otwarty port 33XX, gdzie XX to numer systemu SAP). JPK Transfer Engine będzie działać w trybie serwera używając dedykowanego konta użytkownika SAP.
6. Na maszynie z systemem Windows, biblioteki Visual Studio 2005 C/C++ runtime libraries (8.0.50727.4053 lub nowsza wersja) są wymagane - do pobrania ze strony firmy Microsoft jeśli nie są zainstalowane w Twoim systemie.
1. Połączenie z systemem SAP (pod Windows sprawdź czy masz wpis dla połączenia z `sapgwXX` [XX to SAP system/instance number (nr systemu / instancji SAP)] w systemowym pliku `C:\WINDOWS\system32\drivers\etc\services`; w systemie Linux sprawdź `/etc/services`). Na przykład:

sapgw01 3301/tcp

Nie zapomnij nacisnąć ENTER na końcu tej linii!

Krok 4. Instalacja JPK Transfer Engine

1. Na serwerze przygotowanym w poprzednim kroku rozpakuj plik `jpk-transfer-engine-<wersja>.zip`.
2. Otwórz linię komend i przejdź do katalogu `jpk-transfer-engine`. Uruchom `install.bat` w systemie operacyjnym Windows lub `install.sh` w systemie operacyjnym Linux. Wykonaj instrukcje, które pojawiają się na ekranie. Zobacz **Krok 5.3** poniżej, aby dowiedzieć się co to jest JCO_USER.
3. Otwórz plik `jpk.properties` do edycji. Zawiera on ustawienia dla połączenia RFC / Java Connector (JCo) pomiędzy SAPem a JPK Transfer Engine. **Ten plik zawiera szczegółową informację o każdym ustawieniu.** Proszę wypełnić wszystkie pola oznaczone jako obowiązkowe („mandatory”).
 - a. Jeśli serwer SAP korzysta z jednego serwera aplikacyjnego należy ustawić następujące zmienne:
 - 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. Jeśli SAP korzysta z więcej niż jednego serwera aplikacyjnego należy ustawić następujące zmienne:
 - 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. Jeśli serwer z JPK Transfer Engine używa proxy do połączenia z Internetem to ustaw zmienne `HTTP_PROXY*` oraz `HTTPS_PROXY*`. Zobacz również rozdział *Bezpieczeństwo JPK / SAF-T Transfer*.
4. Uruchom `jpk-transfer-engine\start.bat` (w systemie Windows) lub `start.sh` (w systemie Linux).
5. Poczekaj aż pojawi się komunikat "Connected!".

W razie jakichkolwiek problemów otwórz plik `jpk-transfer-engine\log\log.html` w przeglądarce (ten plik zawiera wszystkie komunikaty, które są wyświetlane w oknie programu JPK Transfer Engine) oraz sprawdź pliki `jpk-transfer-engine*.trc`

Krok 5. Instalacja JPK Transfer Monitor w systemie SAP

Akcja	Szczegóły												
Proszę o wgranie dostarczonych transportów w kolejności folderów zawierających zlecenia transportowe:	Transporty zawierają obiekty:												
0. JPK Transfer & NIP Checker BASE (wczytać tylko przy pierwszej instalacji wersji 2.0!!!)	<table><tr><td>Pakiet</td><td>R3TR</td><td>DEVC</td><td>/BCC/JPW</td></tr><tr><td>Pakiet</td><td>R3TR</td><td>DEVC</td><td>/BCC/JPT</td></tr><tr><td>Pakiet</td><td>R3TR</td><td>DEVC</td><td>/BCC/JPN</td></tr></table>	Pakiet	R3TR	DEVC	/BCC/JPW	Pakiet	R3TR	DEVC	/BCC/JPT	Pakiet	R3TR	DEVC	/BCC/JPN
Pakiet	R3TR	DEVC	/BCC/JPW										
Pakiet	R3TR	DEVC	/BCC/JPT										
Pakiet	R3TR	DEVC	/BCC/JPN										
1. JPK Transfer Update (wczytać przy instalacji i każdym update rozwiązania)	Role: Z_JPT_JCO_REGISTRATION, Z_JPT_USER, Z_JPT_ADMIN												
2. JPK Transfer Transaction & Programs (wczytać przy instalacji i każdym update rozwiązania)													
3. NIP Checker Update (wczytać tylko jeśli osobne rozwiązanie NIP checker nie jest wykorzystywane, w przypadku korzystania z NIP Checkera użyj najnowszej paczki instalacyjnej NIP Checkera zamiast tego zlecenia)													
4. Authorization Role Z_JPT_JCO_REGISTRATION (dla użytkownika RFC) (zaleca się wczytywać tylko przy pierwszej instalacji. Przy update zaleca się ręczną aktualizację ról wg rozdziału 4).													
5. Authorization Roles Z_JPT_USER (dla użytkownika) Z_JPT_ADMIN (dla administratora rozwiązania) (zaleca się wczytywać tylko przy pierwszej instalacji. Przy update zaleca się ręczną aktualizację ról wg rozdziału 4).													
Uwaga! W opcjach wszystkich transportów koniecznym może być wybranie opcji: Nadpisanie oryginałów Ignorowanie niepasującej wersji komponentu.													

Kroki instalacji:

Krok 5.1. Wgraj transporty o numerach podanych w powyższej tabeli (kolumna akcja). Transporty znajdują się w plikach *transport*.zip*.

Krok 5.2. Utwórz połączenie RFC:

Uwaga! **W przypadku gdy JPK Transfer ma działać na kilku systemach SAP/ mandantach należy uruchomić kilka instancji serwera JPK Transfer Engine (kilka osobnych kopii, z odmienną konfiguracją pliku properties, oddzielne połączenia RFC np. JPK_JCO1 i JPK2_JCO2 i różne ID programu serwera np. JPK_ENGINE1 i JPK_ENGINE2).**

- Wejdź do transakcji sm59 i utwórz nowe połączenie TCP/IP – wypełnij pola: Miejsce przezn. RFC, Rodzaj aktywacji, Zarejestr. program serwera, Limit czasu CPIC. Przykład połączenia:

Miejsce przeznaczenia RFC JCO

Test połączenia Test unicode

Miejsce przezn. RFC: **JCO**

Typ połączenia: **1** Połączenie TCP/IP Opis

Opis

Opis 1: JCo outbound

Opis 2:

Opis 3:

Informacje administr. **Ustawienia techniczne** Logowanie i bezpiecz. Unicode O...

☐ Rozpocz. na serwerze aplikacji

☒ **Zarejestrowany progr. serwera**

☐ Rozpocz. na serwerze jawnych

☐ Uruchom. na serwerze prezentacji

Zarejestr. program serwera

ID programu: **JPK_ENGINE**

Rodzaj uruch. programu zewnętrznego

☒ Wartość stand. branki

☐ Samod. Exec

☐ Samod. Shell

☐ Serwint. JShell

Limit czasu CPIC

☐ Wartość stand. branki

☒ Zdefiniowane czas przerwy: **5** Zdefiniowana wartość w sek.

Opcje bramki

Serwer gateway: **Ustawiane**

- Jeżeli używany jest **więcej niż jeden serwer aplikacyjny** (grupa serwerów) należy uzupełnić adres jednego z serwerów w polu Serwer gateway (ten sam co w pliku `jpk-transfer-engine\jpk.properties`). W przeciwnym wypadku – gdy używany jest tylko jeden serwer aplikacji – pole może pozostać puste.
- Jeśli chcesz użyć inny **ID programu** musisz dodać następującą linię:
`JCO_PROGID=twój_nowy_ID_programu`
do pliku `jpk-transfer-engine\jpk.properties`.

Krok 5.3. Utwórz użytkownika RFC typu „B System”. Proszę przypisać rolę: Z_JPT_JCO_REGISTRATION dla utworzonego użytkownika. Rola ta jest zdefiniowana w pliku transportowym do instalacji JPK Transfer

Wyświetlanie użytkownika

Użytkownik: **JCO_RFC**

Ostatnia zmiana: **08.08.2016 12:10:54** Status: **Zapamięt.**



Adres **Dane logow.** SNC Wartości stałe Parametr Role Profile G...

Alias:

Typ użytkownika: **B System**

Hasło:









Wyświetlanie użytkownika

Użytkownik: JCO_RFC

Ostatnia zmiana: 08.08.2016 12:10:54 Status: Zapamięt.

Adres Dane logow. SNC Wartości stałe Parametr **Rola** Profile G...

       Rola  Rola

Użytkownik referencji dla dodatkowych uprawn.

Przypisania ról

S...	Rola	Typ	Ważne od	Ważne do	Oznaczenie
<input checked="" type="checkbox"/>	JPT_JCO_REGISTRATION	<input type="checkbox"/>	28.06.2016	31.12.9999	JPT communication user

Krok 5.4. Wypełnij tabelę konfiguracyjną: /BCC/JPT_DB_TCU dla wszystkich systemów SAP, na których instalowane jest rozwiązanie (za pomocą transakcji /BCC/JPT_CUST lub SM30).

a) Przykładowa konfiguracja produktu, dla JPK Transfer Engine zainstalowanego na osobnym serwerze, gdzie stacja robocza nie ma dostępu do współdzielonego foldera sieciowego i pliki do podpisu kopiowane są z serwera aplikacyjnego do podkatalogu lokalnego C:\LocFiles\JPK\TOSIGN, a plik z podpisem kopiowany jest z powrotem z tego samego katalogu i rozpoznawany po rozszerzeniu *.XAdES:

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) Przykładowa konfiguracja produktu, dla JPK Transfer Engine zainstalowanego na serwerze aplikacyjnym:

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) Przykładowa konfiguracja produktu, dla JPK Transfer Engine zainstalowanego lokalnie:

JPT - tabela konfiguracyjna			
JG	JPK	Klucz konfiguracyjny	Wartość klucza konfiguracyjnego
		▼ 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

Klucze obowiązkowe:

- **PATH_XML** – Ścieżka do katalogu w którym znajdują się pliki JPK („Folder z plikami JPK”). Podana tutaj ścieżka, będzie podpowiadana na ekranie Monitora wysyłki. Uwaga! Parametr może być podany na poziomie ogólnym (JG = „*” i typ JPK = „*”) lub na poziomie szczegółowym (inny dla poszczególnych JG/ typów JPK). Ścieżka musi kończyć się na \XML lub /XML w zależności od systemu operacyjnego.
- **RFC_CONNECTION** – Nazwa utworzonego połączenia RFC w SM59. Uwaga! Parametr może być podany na poziomie ogólnym (JG = „*” i typ JPK = „*”) lub na poziomie szczegółowym bez uwzględnienia typów JPK (inny dla poszczególnych JG, ale taki sam dla wszystkich typów JPK).

Zaleca się ustawienie co najmniej następujących parametrów opcjonalnych: PATH_XML_SAP, AUTO_START_SIGN_TOOL i AUTHORIZATION_CHECK (ostatni jeśli różne jednostki gospodarcze mają być obsługiwane przez różne zespoły).

Klucze opcjonalne:

- **PATH_XML_E** – Ścieżka do katalogu w którym znajdują się pliki JPK widziana przez serwer JPK Transfer Engine. Parametr należy podawać tylko jeśli ścieżka do plików XML „widziana” przez JPK Transfer Engine jest inna niż ścieżka po stronie SAP (np. gdy dostęp do plików jest przez serwer aplikacyjny SAP na linuxie, a Transfer Engine na Windows). Uwaga! Parametr może być podany na poziomie ogólnym (JG = „*” i typ JPK = „*”) lub na poziomie szczegółowym (inny dla poszczególnych JG/ typów JPK). Ścieżka musi kończyć się na \XML lub /XML w zależności od systemu operacyjnego.
- **PATH_XML_SAP** – określa domyślną wartość parametru „Folder SAP” dla ścieżki „Folder z plikami JPK”. Pozwala na ustalenie, czy od strony SAP dostęp do folderów JPK będzie się odbywał poprzez uprawnienia użytkownika ze stacji roboczej (Folder SAP = „”), czy poprzez serwer aplikacyjny (Folder SAP = X). Zaleca się ustawienie dostępu poprzez serwer aplikacyjny. Uwaga! Parametr może być podany na poziomie ogólnym (JG = „*” i typ JPK = „*”) lub na poziomie szczegółowym (inny dla poszczególnych JG/ typów JPK). Przewidziane są 4 wartości tego parametru:

Wartość parametru	Pole „Folder SAP” – dostęp przez serwer aplikacyjny	Możliwość zmiany pola „Folder SAP” na ekranie selekcji
Brak konfiguracji parametru		Tak (zachowanie kompatybilności z poprzednimi wersjami)
		Nie
X	X	Nie
1		Tak (zachowanie kompatybilności z poprzednimi wersjami)
2	X	Tak (zachowanie kompatybilności z poprzednimi wersjami)

Uwaga! Jeśli wybrano dostęp przez folder serwera plikowego SAP (Folder SAP = „X”), dostęp do katalogów będzie odbywał się nie za pomocą uprawnień użytkownika stacji roboczej, ale użytkownika, na którym uruchomiony jest serwer SAP. Jest to zazwyczaj użytkownik **SAPServiceXYZ**, gdzie XYZ to SID systemu. Aby przeszukanie w domenie zadziałało, musi być utworzony użytkownik DEOMENA\SAPServiceXYZ, który będzie mieć dostęp do katalogu sieciowego.

- **PATH_XML_MANUAL** – jeśli wprowadzono jakąkolwiek wartość dla tego klucza (zazwyczaj „X”) to możliwe wprowadzenie ręcznej wartości ścieżki nadpisującej ścieżkę pobieraną z konfiguracji. Uwaga! Parametr może być podany na poziomie ogólnym (JG = „*” i typ JPK = „*”) lub na poziomie szczegółowym (inny dla poszczególnych JG/ typów JPK).

- **PATH_TOSIGN_S** – Ścieżka do folderu TOSIGN używana przez narzędzie podpisujące (kiedy parametr AUTO_START_SIGN_TOOL jest wykorzystany). Parametr PATH_TOSIGN_S powinien być używany JEDYNNIE jeśli folder TOSIGN nie może być ustalony na podstawie ścieżki zdefiniowanej parametrem PATH_XML. Uwaga! Parametr może być podany na poziomie ogólnym (JG = „*” i typ JPK = „*”) lub na poziomie szczegółowym (inny dla poszczególnych JG/ typów JPK). Ścieżka musi kończyć się na \TOSIGN lub /TOSIGN w zależności od systemu operacyjnego.
- **TOSIGN_S_COPY_LOCAL** – Może być wykorzystany tylko łącznie z PATH_TOSIGN_S (lub lokalnie ustawionym dla narzędzia podpisującego parametrem TOSIGN) i AUTO_COPY_SIGNED (lub lokalnym AUTOCOPY). Używany, gdy użytkownik końcowy nie ma dostępu do katalogów JPK. Gdy ustawiona wartość niepusta „X”, JPK Transfer Monitor przed uruchomieniem narzędzia podpisującego kopiuje plik z podkatalogi globalnego TOSIGN do folderu lokalnego (PATH_TOSIGN_S). Z kolei przed wysłaniem pliku do MF następuje kopiowanie pliku podpisanego ze stacji roboczej (PATH_TOSIGN_S, lub folder z AUTOCOPY) do folderu SIGN serwera.
- **AUTHORIZATION_CHECK** – jeśli wprowadzono jakąkolwiek wartość dla tego klucza (zazwyczaj „X”) to sprawdzany jest obiekt uprawnień /BCC/JPK01 pod kątem uprawnień do JG i typu JPK. Uwaga! Parametr może być podany jedynie na poziomie ogólnym (JG = „*” i typ JPK = „*”).
- **SAVE_SENT_XML** – jeśli wprowadzono jakąkolwiek wartość dla tego klucza (zazwyczaj „X”) to przy pobraniu UPO plik jest archiwizowany w tabeli indeksowej SAP (/bcc/jpt_db_indx). Można go później pobrać za pomocą przycisku „Pobierz zarchiwizowany XML”. Uwaga! Jeśli brak tego parametru lub brak zarchiwizowanych plików przycisk nie pojawia się. Uwaga! Parametr może być podany na poziomie ogólnym (JG = „*” i typ JPK = „*”) lub na poziomie szczegółowym (inny dla poszczególnych JG/ typów JPK).
- **AUTO_COPY_SIGNED** – Parametr ułatwiający podpisywanie plików xml, w przypadku gdy program podpisujący nie ma automatycznej możliwości przenoszenia plików podpisu do innego folderu. Jeśli wprowadzono wartość X, to system, w momencie wysyłki jeśli pliku, jeśli odpowiedniego pliku podpisu z rozszerzeniem .xades nie ma w katalogu „SIGN”, będzie próbował kopiować odpowiedni plik z rozszerzeniem .xades z podkatalogu „TOSIGN” do katalogu „SIGN”. W przypadku innych rozszerzeń plików podpisu lub korzystania z systemów UNIX, w których rozpoznawana jest wielkość liter można zamiast wartości „X” parametru podać wartość filtra jaki ma być stosowany do rozpoznawania plików podpisu do przeniesienia, np. “*. XAdES”.
Uwaga! W przypadku programu proCertum SmartSign, jeśli podpisane pliki mają trafiać do różnych folderów zależnie od JG lub typu JPK, należy skonfigurować jeden folder do którego kopiowane jest wykonywane automatycznie przez program podpisujący np. D:\JPK\SS a potem w parametrze AUTO_COPY_SIGNED (lub lokalnie w AUTOCOPY) podać ścieżkę + maskę plików do przekopiowania do właściwego katalogu z podpisanymi plikami np.: “D:\JPK\SS*.xml”.
Uwaga! Jeśli ustawiono parametr AUTO_START_SIGN_TOOL, wtedy kopiowanie może być zarządzane lokalnie, przez parametr AUTOCOPY (menu *Inne > Ustaw program podpisu*) na poziomie każdego komputera. W takim przypadku AUTO_COPY_SIGNED jest nadpisywany jeśli podano jakąkolwiek niepustą wartość AUTOCOPY. Uwaga! Parametr AUTO_COPY_SIGNED może być podany jedynie na poziomie ogólnym (JG = „*” i typ JPK = „*”).
- **AUTO_START_ENGINE_LC** – Parametr umożliwiający uruchamianie JPK Transfer Engine (silnika wysyłki JPK / JAVA) na komputerze użytkownika w momencie uruchomienia transakcji JPK Transfer (/BCC/JPT) przez danego użytkownika. Wykorzystywany jedynie, gdy silnik wysyłki JAVA (JPK Transfer Engine) nie jest

zainstalowany na osobnym serwerze, a jedynie na komputerach poszczególnych użytkowników. Jeśli wprowadzono jakąkolwiek wartość dla tego klucza (zazwyczaj „X”) to przy uruchomieniu transakcji /BCC/JPT system szuka ścieżki i pliku startowego JPK Transfer Engine w tabeli /BCC/JPT_DB_TCU3. Jeśli znajdzie wpis odpowiadający komputerowi użytkownika, wtedy uruchamia podany program (najczęściej start.bat JPK Transfer Engine). Każdy użytkownik, może mieć zainstalowane pliki JPK transfer Engine w innym katalogu, dlatego każdy użytkownik może sam skonfigurować ścieżkę do programu uruchamiającego JPK Transfer Engine z poziomu listy ALV transakcji JPK Transfer. Poprzez menu *Inne > Ustaw plik silnika* można podać plik startowy JPK Transfer Engine. Alternatywnie ścieżki dla poszczególnych komputerów może ustawić administrator w tabeli /BCC/JPT_DB_TCU3. Uwaga! Parametr może być podany jedynie na poziomie ogólnym (JG = „*” i typ JPK = „*”).

- **AUTO_SHUT_ENGINE_LC** – parametr używany jedynie łącznie z parametrem AUTO_START_ENGINE_LC. Ustawienie tego parametru w przyszłych wersjach programu będzie umożliwiało automatyczne wyłączenie JPK Transfer Engine (silnik wysyłki JAVA) na komputerze lokalnym jeśli był uruchamiany automatycznie przy starcie transakcji. Uwaga! Parametr może być podany jedynie na poziomie ogólnym (JG = „*” i typ JPK = „*”).
- **AUTO_START_ENGINE_AS** – Parametr umożliwiający uruchamianie JPK Transfer Engine (silnika wysyłki JPK/ JAVA) na serwerze aplikacyjnym SAP w momencie uruchomienia transakcji JPK Transfer (/BCC/JPT) o ile silnik jeszcze nie był uruchomiony. Ustawienie parametru powoduje wywołanie polecenia zewnętrzne zdefiniowanego w transakcji SM69 o identyfikatorze **ZIPT_ENGINE_ST_XXX (gdzie XXX to numer mandanta w systemie)**. Przykładowe polecenie uruchamiające JPK Transfer engine z folderu D:\JPK\start.bat:

```
cmd /c "D: & CD \JPK\ & start.bat"
```

 lub

```
powershell "D: ; CD \JPK\jpk-transfer-engine$$\ ; Start-Process start.bat"
```

 Parametr AUTO_START_ENGINE_AS może przyjmować wartość X, lub być identyfikatorem serwera aplikacyjnego (nazwa serwera docelowego) na którym ma być uruchomiony silnik wysyłki. Uwaga! Parametr może być podany jedynie na poziomie ogólnym (JG = „*” i typ JPK = „*”). Patrz także parametr AUTO_SHUT_ENGINE_LC.
- **AUTO_START_SIGN_TOOL** – Parametr włączający w transakcji JPK Transfer (/BCC/JPT) dodatkową ikonę umożliwiającą bezpośrednie uruchomienie programu podpisującego z transakcji SAP. Jeśli parametr ma wartość X w JPK Transfer pojawia się nowa ikona *Uruchom podpis*, oraz w menu dostępna jest opcja *Inne > Ustaw program podpisu*. Ustawienie programu podpisu polega na:
 - podaniu ścieżki do pliku uruchamiającego narzędzie podpisu
 - podaniu parametrów wywołania pliku (ciąg &FILE& zostanie zastąpiony pełną nazwą pliku do podpisu)
 - podaniu czy transakcja ma kopiować podpisane pliki z foldera TOSIGN do SIGN i jakie rozszerzenie mają takie pliki (ciąg pusty oznacza brak kopiowania – wartość domyślna, ciąg „*.xades” oznacza że kopiowane będą pliki z rozszerzeniem „xades”. Uwaga! Jeśli program podpisujący może zapisywać pliki w odpowiednim katalogu lepiej ustawić tę opcję w programie podpisującym niż zlecać to SAP. Uwaga! Parametr może być podany jedynie na poziomie ogólnym (JG = „*” i typ JPK = „*”).
- **EXT_FILE_MASK** – używany tylko gdy wysyłane są zewnętrzne pliki (nie przygotowane produktem JPK Pliki). Wartością tego parametru jest maska nazwy pliku pozwalająca na odczytanie atrybutów pliku z jego nazwy. Bez tego parametru atrybuty pliku zewnętrznego można ustawić ręcznie (patrz instrukcja użytkownika), ale jeśli można

odczytać je z nazwy pliku jest to opcja zalecana i mniej podatna na błędy. W masce pliku następujące znaki/ ciągi mają specjalne znaczenie:

? – odpowiada dowolnemu pojedynczemu znakowi w nazwie pliku

* - odpowiada dowolnej liczbie znaków w nazwie pliku. Jeśli znak * występuje wewnątrz ciągu maski pliku, za nim powinien znaleźć się znak, który nie jest znakiem specjalnym (który można odnaleźć).

&CC& - odpowiada jednostce gospodarczej (4 znaki)

&TY& - odpowiada typowi JPK (2 lub 3 znaki)

&YF& - odpowiada ROKOWI od (4 znaki)

&yf& - odpowiada ROKOWI od (2 znaki)

&MF& - odpowiada MIESIĄCOWI od (2 znaki)

&DF& - odpowiada DNIU miesiąca od (2 znaki)

&YT& - odpowiada ROKOWI do (4 znaki)

&yt& - odpowiada ROKOWI do (2 znaki)

&MT& - odpowiada MIESIĄCOWI do (2 znaki)

&DT& - odpowiada DNIU miesiąca do (2 znaki)

&VE& - odpowiada Wersji (1 lub 2 cyfry)

Przykład:

maska: &CC&_&TY&_&YF&&MF&&DF&_&YT&&MT&&DT&_&VE&

nazwa pliku: Y001_VAT_20170201_20170228_10 skutkowało by odczytaniem następujących atrybutów:

- Jednostka gospodarcza Y001 (string &CC&)
- TYp JPK VAT (string &TY&)
- Data od 20170201 (three strings together &YF& &MF& &DF&)
- Data do 20170228 (three strings together &YT& &MT& &DT&)
- Wersja 10 (string &VE&)

Uwaga! Parametr może być podany jedynie na poziomie ogólnym (JG = „*” i typ JPK = „*”).

- **EXT_FILE_MASK_AUTO** – używany razem z parametrem EXT_FILE_MASK. Kiedy ten parametr jest ustawiony (“X”), wtedy jeśli uda się wydobyć za pomocą maski wszystkie atrybuty pliku, plik jest automatycznie zapamiętywany (użytkownik nie musi zapamiętywać atrybutów ikoną Zapisz). Uwaga! Parametr może być podany jedynie na poziomie ogólnym (JG = „*” i typ JPK = „*”).
- **EXT_FILE_DISTINCT** – Kiedy ten parametr jest ustawiony (“X”), wtedy tylko unikalne wartości atrybutów są możliwe. Oznacza to, że system sprawdza czy plik z tymi samymi atrybutami już istnieje i nie pozwala zapisać drugiego z powtarzającymi się. Pole wersja jest w takim przypadku czyszczone. Uwaga! Parametr może być podany jedynie na poziomie ogólnym (JG = „*” i typ JPK = „*”).
- **ONLY_TEST_MODE** – jeśli ustawiony („X”), możliwe jest wykonanie tylko przebiegu testowego wysyłki. Do ustawienia w systemach testowych by zabezpieczyć przed przypadkową wysyłką na serwer produkcyjny MF.

Uwaga! Podanie dla Jednostki gospodarczej / typu JPK wartości „*” jest równoznaczne z pozostawieniem tej wartości pustej i oznacza branie pod uwagę klucza niezależnie od JG/ typu JPK.

Uwaga! Tabela konfiguracyjna wersji XML (/BCC/JPT_DB_TCU2) powinna być z założenia wypełniana poprzez transporty aktualizacyjne otrzymywane od producenta. Wpis w tej tabeli powinien odpowiadać plikom w ścieżce \JPK\XSD\ . W przypadku dodawania wpisów ręcznie należy dodać odpowiedni plik .xsd do katalogu.

Krok 5. 5. Dostosuj zabezpieczenia Gateway

Aby komunikacja programu JPK_ENGINE z systemem ABAP była możliwa, należy na systemie ABAP dodać następującą linię w pliku reginfo:

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

oraz następującą linię w pliku secinfo:

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

gdzie **XX** to adres serwera – FQDN (fully qualified domain name), na którym działa JPK Transfer Engine.

Sprawdź czy pierwsza linijka w pliku secinfo/reginfo to:

```
#VERSION=2
```

Plik reginfo.DAT/secinfo.DAT zlokalizowany jest w katalogu danej instancji SAP w podkatalogu "data".

Po aktualizacji tych plików należy odświeżyć konfigurację GATEWAY.

Transakcja SMGW – proszę wybrać z menu:

Goto -> Expert Functions -> External Security -> Reread.

2. Instalacja JPK Transfer Engine w Harmonogramie Zadań (opcja)

JPK Transfer Engine (silnik wysyłki JAVA) może być uruchamiany:

- a) na wydzielonym serwerze (opcja rekomendowana)
- b) na serwerze aplikacyjnym SAP (patrz parametr konfiguracji AUTO_START_ENGINE_AS)
- c) na stacji roboczej użytkownika (patrz parametry konfiguracji AUTO_START_ENGINE_LC, AUTO_SHUT_ENGINE_LC)

W przypadku, gdy JPK Transfer Engine ma być uruchomiony na wydzielonym serwerze (opcja a) można dodać JPK Transfer Engine do Harmonogramu Zadań (tylko w systemie Windows). Po utworzeniu wpisu harmonogramu zadań wg poniższych wskazówek, w przypadku restartu komputera lub zatrzymania procesu, JPK Transfer Engine będzie uruchamiane automatycznie w tle i działać podobnie do usług systemu Windows.

1. By uruchomić Harmonogram Zadań wpisz **Taskschd.msc** w okienko wyszukiwania Windows. Uruchom program **Harmonogram Zadań**.
2. W programie Harmonogram zadań, kliknij po lewej w "Biblioteka harmonogramu zadań" i otwórz menu kontekstowe za pomocą prawego przycisku myszy, wybierz z menu "Nowy folder..." i nadaj mu nazwę np.: "JPK"
3. Dla właśnie utworzonego folderu "JPK" z menu kontekstowego wybierz "Utwórz zadanie podstawowe..."
 1. Nadaj zadaniu rozpoznawalną nazwę i opis
 2. Wyzwalacz "Przy uruchamianiu komputera"
 3. Akcja "Uruchom program" - Ścieżka do jpk-transfer-engine\start.bat; "Rozpocznij w: - (Ścieżka do jpk-transfer-engine)
 4. Zakończ (Zaznacz *Otwórz okno dialogowe właściwości ...*)
 5. Właściwości zadania:
 1. Zakładka Ogólne: Zaznacz *Uruchom niezależnie od tego, czy użytkownik jest zalogowany*
 2. Zakładka Ogólne: Zaznacz *Uruchom z najwyższymi uprawnieniami*
 3. Zakładka Warunki: Odznacz *Uruchom zadanie tylko wtedy, gdy komputer jest na zasilaniu sieciowym*
 4. Zakładka Warunki: Zaznacz *Wznów pracę komputera, aby uruchomić to zadanie*
 5. Zakładka ustawienia: Zaznacz *Uruchom zadanie szybko, jeśli pominięto zaplanowane uruchomienie*
 6. Zakładka ustawienia: Zaznacz *Po błędzie uruchom ponownie co:*
 7. Zakładka ustawienia: Odznacz *Zatrzymaj zadanie jeśli działa dłużej niż*

3. Bezpieczeństwo JPK / SAF-T Transfer

JPK Transfer Engine łączy się z SAPem (poprzez połączenie RFC JCo) oraz z 3 zewnętrznymi hostami:

1. e-dokumenty.mf.gov.pl (port SSL 443) – tylko w trybie produkcyjnym JPK Transfer Monitor
2. test-e-dokumenty.mf.gov.pl (port SSL 443) – tylko w trybie testowym JPK Transfer Monitor
3. *.blob.core.windows.net (port SSL 443) – grupa serwerów (nazwa hosta różni się przy każdym połączeniu) używanych przez JPK Transfer Monitor do wysyłania plików do Ministerstwa Finansów
4. crd.gov.pl (port HTTP 80) – używane podczas walidacji plików JPK

4. Uprawnienia użytkowników SAP rozwiązania JPK / SAF-T Transfer

4.1. Uprawnienia dla użytkownika zdalnego (połączenie z silnikiem JAVA JPK Transfer)

Ten użytkownik jest zdefiniowany w pliku properties silnika JAVA JPK. Ten użytkownik powinien korzystać z roli **Z_JPT_JCO_REGISTRATION** dostarczonej wraz z plikami instalacyjnymi JPK (można użyć kopii tej roli).

Ważne: Przy upgrade do wersji 2.0 należy wgrać na nowo transport z uaktualnioną rolą, lub ręcznie dodać następujące obiekty uprawnień:

```

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

S_RFC
RFC_TYPE: FUGR
RFC_NAME:      SDIFRUNTIME
  
```

4.2. Uprawnienia użytkownika wysyłającego pliki JPK

Użytkownik walidujący, przygotowujący i wysyłający pliki za pomocą rozwiązania JPK transfer, powinien posiadać przynajmniej następujące uprawnienia (obiekt **/BCC/JPK01** może być dostosowany do uprawnień organizacyjnych użytkownika np. dana JG, i jest używany wyłącznie jeśli paramter **AUTHORIZATION_CHECK** jest ustawiony w tabeli konfiguracyjnej).

Obiekt uprawnień **S_DATASET** jest konieczny jedynie jeśli dostęp do plików jest wykonywany przez serwer aplikacyjny (checkbox **Folder SAP**).

Obiekt uprawnień **S_LOG_COM** jest konieczny jedynie jeśli wykorzystywana jest opcja automatycznego uruchamiania JPK Transfer Engine na serwerze aplikacyjnym (**AUTO_START_ENGINE_AS**).

The screenshot displays the SAP authorization configuration for user **Z_JPK_USER**. The configuration is organized into a hierarchical tree structure with the following main sections:

- Role: Niezależne od aplikacji - obiekty uprawnień** (AAS2)
 - Role: Kontrola kodów transakcji podczas uruchamiania transakcji** (S_TCODE)
 - Standard: Kontrola kodów transakcji podczas uruchamiania transakcji** (T-B677002400)
 - Kod transakcji** (/BCC/JPT) (TCD)
 - Standard: Kontrola kodów transakcji podczas uruchamiania transakcji** (T-B677002401)
 - Kod transakcji** (SUS3) (TCD)
 - Standard: Kontrola kodów transakcji podczas uruchamiania transakcji** (T-B677002402)
 - Kod transakcji** (/BCC/JPM) (TCD)
- Role: Basis - Administracja** (BC_A)
 - Standard: Uprawnienie dla dostępu do pliku** (S_DATASET)
 - Standard: Uprawnienie dla dostępu do pliku** (T-B677002400)
 - Działanie** (ACTVT)
 - Nazwa pliku** (FILENAME)
 - Nazwa programu z pomocą wysz.** (/BCC/JPM, /BCC/JPT_P_MONITOR) (PROGRAM)
 - Standard: Uprawnienie do działań GUI** (S_GUI)
 - Standard: Uprawnienie do działań GUI** (T-B677002400)
 - Działanie** (02, 61) (ACTVT)
 - Standard: Uprawnienia do wykonywania logicznych poleceń systemu oper.** (S_LOG_COM)
 - Standard: Authorization to Execute Logical Operating System Commands** (T-B677002400)
 - Nazwa polecenia logicznego** (S_JPT_ENGINE_START) (COMMAND)
 - Nazwa bieżącego serwera aplika** (HOST)
 - System operacyjny serwera apli** (OSYSTEM)
- Role: Basis - funkcje centralne** (BC_Z)
 - Standard: Standardowy układ ALV** (S_ALV_LAYO)
 - Standard: Standardowy układ ALV** (T-B677002400)
 - Działanie** (33) (ACTVT)
 - Standard: Układy specyficzne dla raportów ALV** (S_ALV_LAYR)
 - Standard: Układy specyficzne dla raportów ALV** (T-B677002400)
 - Działanie** (33) (ACTVT)
 - ID zezwolenia dla wywoł. wiel** (LOG_GROUP)
 - Logiczne pojęcie grupowe** (REPORT)
 - Abstr. Nazwa raportu** (/BCC/JPM, /BCC/JPT_P_MONITOR)
- Role: Jednolity Plik Kontrolny** (S_JPK)
 - Standard: Jednostka gospodarcza i typ pliku JPK** (/BCC/JPK01)
 - Standard: Jednostka gospodarcza i typ pliku JPK** (T-B677002400)
 - Typ pliku JPK** (/BCC/JPK_T)
 - Jednostka gospodarcza** (SUERS)

4.3. Uprawnienia administratora JPK zmieniającego tabele konfiguracyjne JPK w systemie SAP

Użytkownik zmieniający wpisy konfiguracyjne w tabel /BCC/JPT_DB_TCU* za pomocą transakcji /BCC/JPT_CUST, /BCC/JPT_XSD, /BCC/JPT_LEP, /BCC/JPT_STP, /BCC/JPT_SHUTDOWN powinien posiadać następujące uprawnienia:

S_TPT_ADMIN			
S_TPT_ADMIN			
☐ Ręcznie	Niezależne od aplikacji obiekty uprawnień	AMAB	
☐ Ręcznie	Kontrola kodów transakcji podczas uruchamiania transakcji	S_TCODE	
☐ Standard	Transaction Code Check at Transaction Start	T-B677002500	
☐ Kod transakcji	/BCC/JPT_CUST, /BCC/JPT_LEP, /BCC/JPT_SHUTDOWN, /BCC/JPT_STP, /BCC/JPT_XSD	TCD	
☐ Ręcznie	Transaction Code Check at Transaction Start	T-B677002501	
☐ Kod transakcji	ZUS3	TCD	
☐ Ręcznie	Kontrola kodów transakcji podczas uruchamiania transakcji	T-B677002502	
☐ Kod transakcji	/BCC/JPHO, /BCC/JPTC	TCD	
Opracowane Bazie - Administracja			
☐ Standard	Opracowanie tabel niezależnych od mandanta	S_TABU_CLI	
☐ Standard	Cross-Client Table Maintenance	T-B677002500	
☐ Wskaźnik dla opracowania niest.			CLIENTMAINT
☐ Opracowane	Opracowanie tabeli (poprzez stand. narzędzia takie jak SM30)	S_TABU_D18	
☐ Opracowane	Table Maintenance (via standard tools such as SM30)	T-B677002500	
☐ Działanie	02, 03		ACTIVE
☐ Grupa uprawnień tabeli	ZJPK		DICHERCLE
Opracowane Bazie - Środowisko projektowe			
☐ Opracowane	Obiekt uprawnień dla środowiska tłumaczeniowego	S_TRANSLAT	
☐ Opracowane	Translation environment authorization object	T-B677002500	
☐ Działanie	02		ACTIVE
☐ Język docelowy	*		TRANLANGUAGE
☐ Tłumaczenie: oznaczenie rodzaju	*		TRANOBJ

5. Opis uaktualnienia produktu JPK / SAF-T Transfer

Kroki:

1. JPK Transfer Monitor
 - a. Wylogować się z Monitora
 - b. Wczytać nowe pliki transportowe (jest to pełna wersja, nie ma potrzeby wczytywać plików z poprzednich wersji)
 - c. Rozważenie użycia nowych parametrów konfiguracyjnych opisanych w sekcji 1 krok 4, jeśli wprowadza je nowa wersja (SM30 table /BCC/JPT_DB_TCU).
 - d. Weryfikacja, czy uprawnienia wymagane przez nową wersję nie są większe niż uprawnienia wymagane przez poprzednią wersję i jeśli konieczne, uaktualnienie uprawnień użytkowników (sekcja 4)
2. JPK Transfer Engine (update JPK Transfer Engine jest wymagany przy zmianach głównej wersji produktu np. z wersji 2.0 do wersji 2.1).
 - a. Zatrzymać Engine (zamknąć okno aplikacji)
 - b. Skopiować plik `jpk-transfer-engine\jpk.properties` do zewnętrznego katalogu
 - c. Usunąć katalog `jpk-transfer-engine`
 - d. Rozpakować plik `jpk-transfer-engine-*.zip`
 - e. Do nowego pliku `jpk-transfer-engine\jpk.properties` skopiować zawartość zachowanego wcześniej pliku `jpk.properties`
 - f. Uruchomić Engine (`jpk-transfer-engine\start.bat` – w Windows lub `start.sh` – w Linux)

Nie należy uruchamiać żadnego z tych programów dopóki obydwa nie zostaną uaktualnione!

6. Konfiguracja plików XSD (schematy sprawdzenia plików XML)

Transakcja **/BCC/JPT_XSD** może zostać użyta by skonfigurować schematy XSD (XML Schema Definition) w zależności od czasu. Transakcja zmienia wpisy w tabeli **/BCC/JPT_DB_TCU2**. Normalnie wpisy w tej tabeli powinny być dostarczane przez BCC w formie zleceń transportowych. W przypadkach konieczności dokonania nagłych zmian administrator może uzupełnić wpisy w tej tabeli ręcznie. W przypadku dodawania wpisów do tej tabeli administrator powinien dodać odpowiednio nazwany plik XSD do folderu XSD. Ukryty parametr globalny **VER_DEP_ON_DATA_DATE** decyduje, czy wersja XSD jest ustalana na podstawie daty systemowej (domyślnie), czy na podstawie daty początkowej pliku XML do przesłania (**VER_DEP_ON_DATA_DATE=X**).

7. Lokalne ścieżki do silników JPK na komputerach użytkownika (opcja)

Transakcja **/BCC/JPT_LEP** może być użyta do wskazania ręcznie ścieżek do plików uruchamiających silnik JPK Transfer (ulożonych na stacjach roboczych użytkowników) – wpisy w tabeli **/BCC/JPT_DB_TCU3**. Tabela ta jest używana tylko jeśli ustawiony jest parametr konfiguracyjny **AUTO_START_ENGINE_LC**. Normalnie wpisy w tej tabeli są ustalane przez użytkowników samodzielnie z użyciem opcji menu *Inne > Ustaw plik silnika*. Transakcja **/BCC/JPT_LEP** umożliwia zmianę wpisów w tabeli **/BCC/JPT_DB_TCU3** ręcznie.

8. Ustawienia ścieżek i konfiguracja lokalnych narzędzi podpisujących na komputerach użytkownika (opcja)

Transakcja **/BCC/JPT_STP** może być użyta do wskazania ręcznie (wpisy w tabeli **/BCC/JPT_DB_TCU4**):

- ścieżek do plików uruchamiających narzędzie podpisujące (ulożonych na stacjach roboczych użytkowników),
- parametrów wywołania tych narzędzi,
- zdefiniowania czy pliki z podpisem mają być kopiowane z katalogu TOSIGN do katalogu SIGN przez SAP – funkcja AUTOCOPY (jeśli nie może tego zrobić program podpisujący). Patrz parametr globalny **AUTO_COPY_SIGNED**. AUTOCOPY może pozostać puste. Ustawienie niepustej wartości AUTOCOPY ma pierwszeństwo przed parametrem globalnym **AUTO_COPY_SIGNED**. Specjalna wartość AUTOCOPY „NOT” dezaktywuje dla użytkownika/komputera funkcjonalność kopiowania.
- zdefiniowanie lokalnej ścieżki do katalogu TOSIGN w przypadkach, gdy katalogi na komputerze lokalnym są widziane inaczej niż na serwerze i w narzędziu JPK Transfer Engine. Zobacz także parametr globalny **PATH_TOSIGN_S**. Ustawienia lokalne dla użytkownika nadpisują parametr globalny.

Tabela ta jest używana tylko jeśli ustawiony jest globalny parametr konfiguracyjny **AUTO_START_SIGN_TOOL**. Normalnie wpisy w tej tabeli są ustalane przez użytkowników dla siebie samodzielnie z użyciem opcji menu *Inne > Ustaw program podpisu*. Transakcja **/BCC/JPT_STP** umożliwia zmianę wpisów w tabeli **/BCC/JPT_DB_TCU4** ręcznie i umożliwia ręczną zmianę dla wszystkich użytkowników.

Podczas definiowania parametrów linii komend można użyć następujących kodów specjalnych, które zostaną zastąpione właściwymi wartościami dla przetwarzanego pliku w czasie uruchamiania narzędzia podpisu:

&FILE&	- pełna ścieżka do pliku do podpisania
&FOLDER&	- folder zawierający plik do podpisania
&TFOLDER&	- folder docelowy plików podpisanych
&FILESHORT&	- nazwa pliku do podpisania (bez ścieżki)
&JPKTYP&	- ID typu JPK
&BUKRS&	- ID jednostki gospodarczej

9. Shutdown serwera JPK Transfer Engine (opcja)

Transakcja **/BCC/JPT_SHUTDOWN** może być użyta do ręcznego wyłączenia serwera wysyłki java – JPK Transfer Engine. W trybie testowym można za jej pomocą sprawdzić połączenie, w przebiegu rzeczywistym wysła do serwera żądanie wyłączenia się.

10. Certyfikaty konieczne do połączenia z zewnętrznymi systemami

Certyfikaty konieczne dla uzyskania połączenia https są przechowywane w pliku **ssl_certificates.jks**. Certyfikaty te są dostarczane przez BCC wraz z paczką instalacyjną. Na skutek zmian w infrastrukturze Ministerstwa Finansów mogą być wymagane nowe certyfikaty. Dla użytkowników z wykupioną opcją maintenance dodatkowe certyfikaty będą dostarczane przez BCC.

Od wersji 2.0 administratorzy mogą dodawać certyfikaty samodzielnie.

Certyfikaty mogą być dodawane narzędziem keytool (powinno znajdować się w folderze bin instalacji JAVA).

Aby dodać do pliku ssl_certificates.jks certyfikat Należy wykonać poniższą komendę w folderze JPK Transfer Engine (w miejscu gdzie znajduje się plik ssl_certificates.jks).

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

Przykład:

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

Hasło dla ssl_certificates.jks:

@zTL98s!32fk

11. Więcej informacji

Więcej informacji o JPK Transfer można znaleźć w instrukcji użytkownika oraz na forum *JPK by BCC*:

<https://jpk.bcc.com.pl>