

ČSOB BUSINESS CONNECTOR

IMPLEMENTAČNÍ PŘÍRUČKA PRO AUTOMATICKÉ STAHOVÁNÍ A ODESÍLÁNÍ SOUBORŮ

1	Úvod	3
1.1	Funkční celky	3
2	Zprovoznění služby ČSOB Business Connector	4
2.1	Povolení služby ČSOB Business Connector u smlouvy o využívání služby CEB	4
2.2	Získání certifikátu	4
2.2.1	Získání certifikátu od banky	4
2.3	Registrace certifikátu do služby CEB	8
2.4	Konfigurace služby v portálu	9
2.5	Záloha certifikátu a privátního klíče	9
2.6	Zneplatnění certifikátu v případě kompromitace klíče	10
3	Rozhraní služby ČSOB Business Connector pro CEB pro třetí strany	11
3.1	Principy	11
3.1.1	Autentizace	11
3.1.2	Stahování souborů	12
3.1.3	Odesílání souborů	12
3.2	Webová služba (SOAP/HTTPS)	13
3.2.1	Operace GetDownloadFileList	13
3.2.2	Operace StartUploadFileList	15
3.2.3	Operace FinishUploadFileList	17
3.2.4	WSDL a adresa služby	18
3.2.5	Ochranný interval použití služby	18
3.2.6	Odstávka služby	18
3.3	REST služba (HTTP download/upload)	18
3.3.1	HTTP GET (download souboru)	18
3.3.2	HTTP POST (upload souboru)	19
3.4	Chyby spojení	20
3.4.1	Chyby na síťové úrovni	20
3.4.2	Chyby SSL (SSL Alerty)	20
3.4.3	Chyby HTTP (HTTP Status)	20
3.5	Testovací demo prostředí	21
3.6	Technické požadavky	21
3.6.1	Parametry klientského certifikátu	21
3.6.2	Požadavky na SSL spojení	22
3.6.3	Požadavky na HTTP a SOAP	23
4	Formáty souborů	24
4.1	Výpisy	24
4.2	Avíza	24
4.3	Kurzovní lístek	24
4.4	Dávky platebních příkazů	25
4.5	Protokol o importu	25
4.6	Podepsané dávky platebních příkazů	25

1 ÚVOD

Tato příručka představuje uživatelskou a technickou dokumentaci k implementaci služby ČSOB Business Connector pro ČSOB CEB, která umožní zákazníkovi automatickou komunikaci s bankou v podobě přenosu souborů, jako jsou výpisy z účtu, avíza a kurzovní lístky z banky ke klientovi a dávek platebních příkazů od klienta do banky.

Součástí je i technický popis rozhraní, které banka poskytuje pro vlastní implementaci klientské aplikace v prostředí zákazníka nebo integraci tohoto rozhraní do softwaru třetích stran.

Banka poskytuje základní klientskou aplikaci pro instalaci v prostředí Windows ke stažení.

1.1 Funkční celky

Služba ČSOB Business Connector je realizována po funkčních celcích, které postupně budují kompletní funkcionalitu. Přehled funkčních celků popisuje následující tabulka:

Funkční celek	Služby
Stahování souborů	<i>GetDownloadFileList()</i> HTTP GET
Odesílání souborů	<i>StartUploadFileList(), FinishUploadFileList()</i> HTTP POST <i>GetDownloadFileList()</i> – rozšíření o fileType IMPPROT a clientAppGuid
Odesílání podepsaných souborů	<i>StartUploadFileList()</i> – rozšíření o mode SignedAllOrNothing

2 ZPROVOZNĚNÍ SLUŽBY ČSOB BUSINESS CONNECTOR

Pro úspěšné propojení se službou ČSOB Business Connector je třeba splnit několik vstupních podmínek a provést provázání aplikace na klientském počítači vůči službě v bance. K tomu služba využívá elektronických certifikátů, které zaručí identitu klienta a zabezpečí přenosový kanál proti zneužití.

Kroky ke zprovoznění služby jsou tyto:

- **povolení služby** ČSOB Business Connector u smlouvy o využívání služby CEB,
- **získání certifikátu** od certifikační autority nebo přímo od banky,
- **registrace certifikátu** pro použití ve službě ČSOB Business Connector v portálu,
- **konfigurace služby** ČSOB Business Connector v portálu,
- stažení, instalace a konfigurace **základní klientské aplikace** poskytnuté bankou
- nebo **implementace vlastní klientské aplikace**.

2.1 Povolení služby ČSOB Business Connector u smlouvy o využívání služby CEB

Dle obchodních podmínek pro službu CEB je služba ČSOB Business Connector ve výchozím stavu povolena všem klientům, pokud nežádali opak.

Zakázání, resp. povolení, služby ČSOB Business Connector je možné provést v portálu nebo pobočce banky.

2.2 Získání certifikátu

Certifikáty, které jsou vhodné pro použití ve službě ČSOB Business Connector, lze získat od takzvaných certifikačních autorit. Tyto firmy vydají zákazníkovi elektronický certifikát na základě dodaných informací a po kontrole, že tyto údaje jsou platné. Vydaný certifikát má omezenou platnost (zpravidla 1 rok) a před uplynutím této doby je nutné certifikát obnovit. Tj. vydat nový (následný) certifikát s novou platností.

Služba ČSOB Business Connector umožňuje používat certifikáty vydané certifikačními autoritami I. Certifikační autorita a PostSignum.

Certifikační autority (CA) vydávají řadu certifikátů různých typů a pro různá použití. Pro použití ve službě ČSOB Business Connector jsou vhodné pouze takzvané Serverové komerční certifikáty, které musí umožňovat takzvanou Klientskou autentizaci. V případě pochybností se obraťte přímo na danou certifikační autoritu.

Proces získání certifikátu probíhá přes internet a zahrnuje:

- vytvoření privátního klíče a elektronické žádosti o certifikát v klientském počítači,
- odeslání elektronické žádosti na CA, její vyřízení v CA a následné vydání certifikátu,
- stáhnutí vydaného certifikátu a jeho instalace v klientském počítači.

Certifikát lze získat také přímo od banky, a to na stránce nastavení Business Connectoru volbou Požádat o certifikát, viz následující kapitola.

2.2.1 Získání certifikátu od banky

Tento postup musíte provádět v počítači, v němž poběží klientská aplikace ČSOB Business Connector. Vznikne při něm privátní klíč, který se v závěru spojí s vydaným certifikátem a bude k dispozici aplikaci.

2.2.1.1 Ruční vytvoření žádosti o certifikát v klientském počítači

Prvním krokem k získání certifikátu je vytvoření elektronické žádosti o certifikát. Podle platformy, na které je provozována klientská aplikace Business Connector, zvolte postup buď:

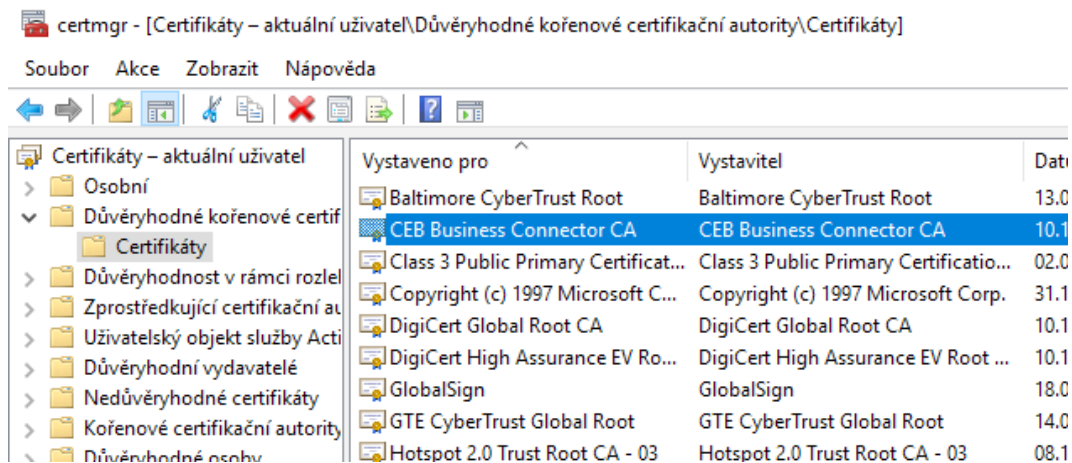
- pomocí nástroje Windows **certreq.exe**, pokud poběží na Windows a chcete mít výsledný certifikát uložen v úložišti certifikátů operačního systému;
- pomocí **openssl**, pokud poběží na Linuxu, MacOS nebo Windows a chcete mít výsledný certifikát uložený v souborech;
- pomocí Java **keytool**, pokud poběží jako Java aplikace na Linuxu, MacOS nebo Windows.

2.2.1.1.1 Pomocí certreq.exe (součást Windows)

Před zahájením tohoto procesu je třeba mít instalovaný kořenový certifikát vydávajícího (banky) a tento certifikát musí být uveden mezi důvěryhodnými kořenovými certifikačními autoritami.

Stiskněte klávesy **Windows + R** a do otevřeného okénka napište certmgr.msc a stiskněte OK.

V nástroji certmgr rozbalte po levé straně *Důvěryhodné kořenové certifikační autority* a *Certifikáty* a v seznamu nalezněte řádek CEB Business Connector CA.



Pokud tam není, stáhněte certifikát vydavatele ze stránky <https://www.csob.cz/portal/documents/10710/15532355/cebbc-ca.crt>. Poté v nástroji certmgr stiskněte pravé tlačítko na složce *Certifikáty* pod *Důvěryhodné kořenové certifikační autority*, zvolte *Všechny úkoly – Importovat...* a vyberte stažený certifikát vydavatele.

Pro ruční vytvoření žádosti o certifikát pomocí příkazové řádky a nástroje certreq.exe je potřeba nejprve vytvořit textový soubor se šablonou žádosti podle vzoru uvedeného níže. K tomu použijte poznámkový blok (notepad.exe, nikoli např. Word). Pozor, některé editory vkládají na začátek souboru neviditelnou značku tzv. BOM. Uložte soubor jako ASCII nebo UTF-8 bez BOM.

```
[NewRequest]
Subject="CN=<BC server>, C=CZ"
KeySpec=1
HashAlgorithm=sha256
KeyLength=2048
UseExistingKeySet=FALSE
Exportable=TRUE
UserProtected=FALSE
MachineKeySet=FALSE
ProviderName="Microsoft RSA SChannel Cryptographic Provider"
ProviderType=12
RequestType=PKCS10
KeyUsage=0xa0
SMIME=False
SuppressDefaults=true
[EnhancedKeyUsageExtension]
OID=1.3.6.1.5.5.7.3.2
```

V šabloně uveďte jméno počítače na řádce Subject=, a to až za znaky CN=. Jméno nesmí obsahovat znak čárka (,), ani uvozovky ("). Toto jméno bude následně obsaženo v názvu vydaného certifikátu.

Soubor se šablonou uložte a pojmenujte např. BCcert.inf ve složce Dokumenty.

Stiskněte klávesy **Windows + R** a do otevřeného okénka napište cmd.exe a stiskněte OK.

Otevře se příkazová řádka, ve které zadejte příkazy cd a certreq:

```
C:\Users\Novák> cd Dokumenty
C:\Users\Novák\Dokumenty> certreq -new BCcert.inf BCcertreq.req
CertReq: Request Created
```

Vytvořená žádost bude uložena v souboru BCcertreq.txt, který je možné zobrazit a kopírovat jako text (jde o base64 zakódovaná binární data):

```
C:\Users\Novák\Dokumenty> notepad.exe BCcertreq.req
```

Soubor s žádostí o certifikát je nutné přenést do počítače, na kterém se přihlašujete do CEBu.

Privátní klíč, který během postupu výše vznikl, je uložen v úložišti certifikát Windows a bude v posledním kroku spojen s vydaným certifikátem. Proto je nutné tento postup dokončit ve stejném počítači, jako byl započat.

2.2.1.1.2 Pomocí openssl (všechny platformy)

Pro vytvoření žádosti o certifikát pomocí openssl nejprve vytvoříme textový soubor s konfigurací žádosti podle tohoto vzoru:

```
[ req ]
default_bits = 2048
default_md = sha256

distinguished_name = req_distinguished_name
prompt = no
string_mask = nombstr
encrypt_key = no

[ req_distinguished_name ]
C = CZ
CN = <BC server>
```

Na řádce CN= uveďte jméno svého počítače, odkud se budete připojovat ke službě Business Connectoru. Toto jméno bude následně obsaženo v názvu vydaného certifikátu. Soubor s konfigurací uložte a pojmenujte např. bccert.cnf v aktuálním adresáři.

Následně v tomto adresáři spusťte následující příkaz:

```
[user@mycomp ~]$ openssl req -config bccert.cnf -new -keyout bccert.key -out bccert.csr
```

Privátní klíč je uložen v souboru bccert.key. Tento soubor ponechte v tomto počítači. Spolu s certifikátem, který dostanete v dalším kroku, je nutný pro sestavení spojení se službou CEB BC. Je vhodné omezit u tohoto souboru práva pro čtení příkazem:

```
[user@mycomp ~]$ chmod 400 bccert.key
```

Vytvořená žádost bude uložena v souboru bccert.csr, který je možné zobrazit a kopírovat jako text (jde o base64 zakódovaná binární data). Tento soubor je nutné přenést do počítače, ve kterém se přihlašujete do CEBu.

2.2.1.1.3 Pomocí Java keytool (všechny platformy)

Pro vytvoření JKS souboru a následně žádosti o certifikát pomocí Java keytool spustíme tyto příkazy (budete dotázáni na zadání nového hesla):

```
[user@mycomp ~]$ keytool -genkey -alias bccert -keyalg RSA -keysize 2048 -dname "CN=<BC server>,C=CZ" -keystore bccert.jks
```

Místo <BC server> uveďte jméno svého počítače, odkud se budete připojovat ke službě Business Connectoru. Toto jméno bude následně obsaženo v názvu vydaného certifikátu.

```
[user@mycomp ~]$ keytool -certreq -alias bccert -keyalg RSA -file bccert.csr -keystore bccert.jks
```

Privátní klíč je uschován v JKS souboru bccert.jks a čeká na import vydaného certifikátu.

Vytvořená žádost bude uložena v souboru bccert.csr, který je nutné přenést do počítače, ve kterém se přihlašujete do CEBu.

2.2.1.2 Podání žádosti o certifikát a vydání certifikátu

Po přihlášení do CEBu otevřete menu, dále nastavení a poté Business Connector.

Úvod	< Menu
Čekárna	Zabezpečení >
Účty	Moje oprávnění rovozní běžák
Platby	Osobní nastavení
Inkasa	Nastavení účtů zdový účet
Karty	CEB Info IR rovozní účet 200
Finanční trhy	Business Connector
Správa financí	Správa služby >
Virtuální pobočka	
Nastavení	

13 Změny ve smlouvě

Stiskněte tlačítko *Požádat o certifikát*,

The screenshot shows the 'Nastavení Business Connector' page. On the left is a navigation menu with items like 'Zabezpečení', 'Moje oprávnění', 'Osobní nastavení', 'Nastavení účtů', 'CEB Info', 'Business Connector', and 'Správa služby'. The main content area is titled 'Nastavení Business Connector' and has a 'Tisk' icon. Under 'Vaše certifikáty', there are two buttons: 'Přidat' and 'Požádat o certifikát', with a mouse cursor pointing at the latter. Below the buttons is a blue information box: 'Pro odesílání a stahování dat do aplikace Business Connector přidejte platný certifikát.' Under 'Kurzovní lístek', there is a 'Stahovat kurzovní lístek' button and the text 'NE'. An 'Upravit' button is at the bottom right.

vyplníte *Název certifikátu* a *vyberte soubor s žádostí o certifikát* (viz 2.2.1.1 *Ruční vytvoření žádosti o certifikát v klientském počítači*), pak potvrďte tlačítkem *Odeslat*.

The screenshot shows the 'Nastavení Business Connector' page with the 'Žádost o certifikát' form. The 'Vybrat soubor' button is highlighted with a green checkmark, and the selected file is 'BCcertreq.req'. The 'Název' field contains 'komunikační certifikát' and also has a green checkmark. There is a 'Zpět' link and an 'Odeslat' button at the bottom right.

Potom *Stáhněte* vydaný certifikát do souboru.

Sériové číslo	Název certifikátu	Subjekt	Vydavatel	Expirace	Stav	
123456789	Jan Nováček	PC_Jan_Novacek	iCA	15.11.2018 09:12:22	aktivní	Stáhnout
987654321	Blokovaný	Mock1	Issuer1	01.02.2020 12:34:55	blokový	Stáhnout ...
Expirovaný						
123123123	Expirovaný aktivní	Mock2	Issuer2	01.01.2017 00:00:00	aktivní	...

2.2.1.3 Instalace vydaného certifikátu v klientském počítači

Posledním krokem je instalace získaného certifikátu zpět do klientského počítače z kroku 1. Postupujte podle návodu pro zvolenou variantu z kapitoly 2.2.1.1.

2.2.1.3.1 Pomocí certreq.exe (součást Windows)

Soubor s vydaným certifikátem BCcert.cer instalujete zpět v počítači, v němž jste vytvářeli žádost o certifikát, takto:

```
C:\Users\Novák> cd Dokumenty  
C:\Users\Novák\Dokumenty> certreq -accept BCcert.cer
```

2.2.1.3.2 Pomocí openssl (všechny platformy)

Soubor s vydaným certifikátem bccert.crt přeneste zpět do počítače, v němž jste vytvářeli žádost o certifikát.

Nyní máte soubory bccert.key (privátní klíč) a bccert.crt (certifikát), které klientská aplikace může (dle implementace) buď používat samostatně, nebo mohou být spojeny do jednoho PKCS12 souboru příkazem:

```
[user@mycomp ~]$ openssl pkcs12 -export -in bccert.crt -inkey bccert.key -out bccert.p12
```

2.2.1.3.3 Pomocí Java keytool (všechny platformy)

Soubor s vydaným certifikátem bccert.cer instalujte v počítači, v němž jste vytvářeli žádost o certifikát, do JKS souboru vytvořeného v 1. kroku. Nejprve musíte importovat certifikát vydávající autority cacert.cer příkazem níže, přičemž budete dotázáni, zda tomuto certifikátu důvěřovat; odpovězte yes.

```
[user@javacomp ~]$ keytool -importcert -alias cacert -file cacert.cer -keystore bccert.jks
```

Následujícím příkazem importujete do stejného JKS souboru i vydaný certifikát:

```
[user@mycomp ~]$ keytool -import -alias bccert -file bccert.cer  
-keystore bccert.jks
```

2.3 Registrace certifikátu do služby CEB

V portálu je možné spravovat seznam certifikátů, které budou opravňovat stahování a odesílání souborů pomocí služby ČSOB Business Connector pro účty v kontraktu.

Certifikát vydaný certifikační autoritou mimo banku je nutné přidat do toho seznamu tlačítkem *Přidat certifikát* a tím provést jeho registraci.

Pokud je certifikát vydán bankou, tlačítkem *Požádat o certifikát* je rovnou zařazen do seznamu registrovaných certifikátů v kontraktu a není třeba soubor certifikátu vkládat tlačítkem *Přidat certifikát*.

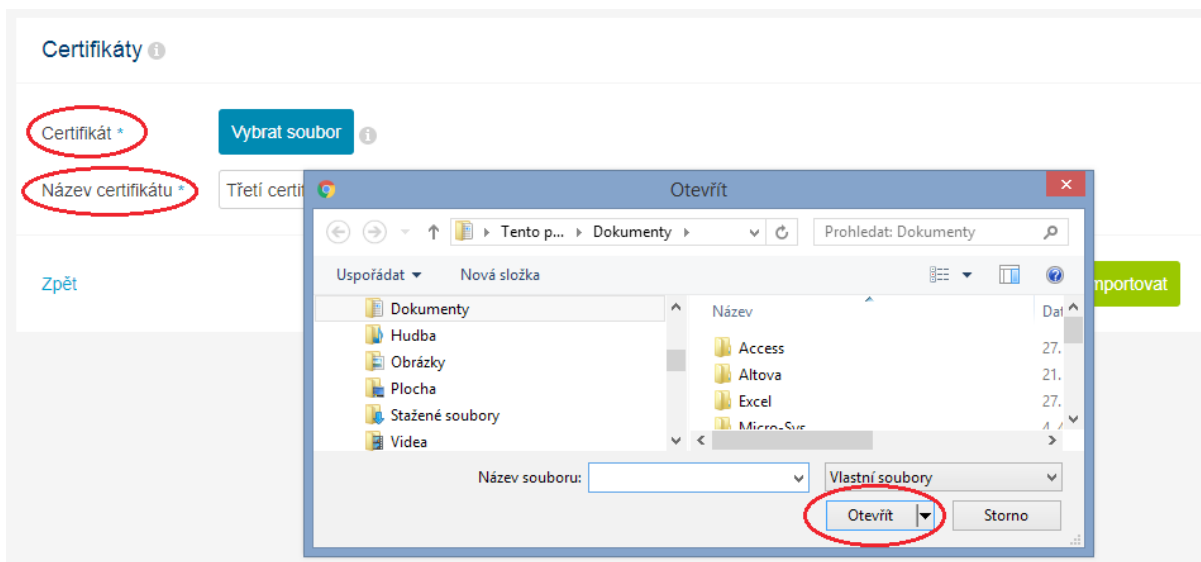
Certifikáty ?

Přidat certifikát

Požádat o certifikát

Sériové číslo 123456789	Název certifikátu Jan Nováček	Subjekt PC_Jan_Novacek	Vydavatel iCA
Sériové číslo 987654321	Název certifikátu Blokovaný	Subjekt Mock1	Vydavatel Issuer1
Expirovaný			
Sériové číslo 123123123	Název certifikátu Expirovaný aktivní	Subjekt Mock2	Vydavatel Issuer2
Expirovaný			
Sériové číslo 321321321	Název certifikátu Expirovaný blokovaný	Subjekt Mock3	Vydavatel Issuer3

Pokud jste získali certifikát jinou cestou, je třeba jej zařadit do seznamu registrovaných certifikátů ke kontraktu tlačítkem *Přidat certifikát*.



Po otevření souboru s certifikátem přes *Vybrat soubor* a vyplnění *Názvu certifikátu* je třeba tlačítkem *Importovat* certifikát k vybranému kontraktu zaregistrovat.

2.4 Konfigurace služby portálu

V portálu je nutné povolit požadované operace, které bude klient pomocí ČSOB Business Connectoru využívat.

Je možné povolit:

- stahování kurzovních lístků (ČNB a ČSOB),
- stahování výpisů pro konkrétní účty,
- stahování avíz pro konkrétní účty,
- odesílání souborů platebních příkazů pro konkrétní účty,
- odesílání podepsaných souborů platebních příkazů pro konkrétní účty.

Nastavení Business Connector

Kurzovní lístek ⓘ

Stahovat kurzovní lístek

Zpět Uložit

Nastavení propojení Tisk

Účet

Účet	277430302/0300, CZK, provozní běžák
Typ účtu	ČSOB Plus Konto v CZK
Název	JIŘÍ VOHNOUT-CEB1

Stahování dat

Avíza

Výpisy

Výpisy pro prohlížení ⓘ

Odesílání dat

Odesílání

Odesílání s podpisem ⓘ

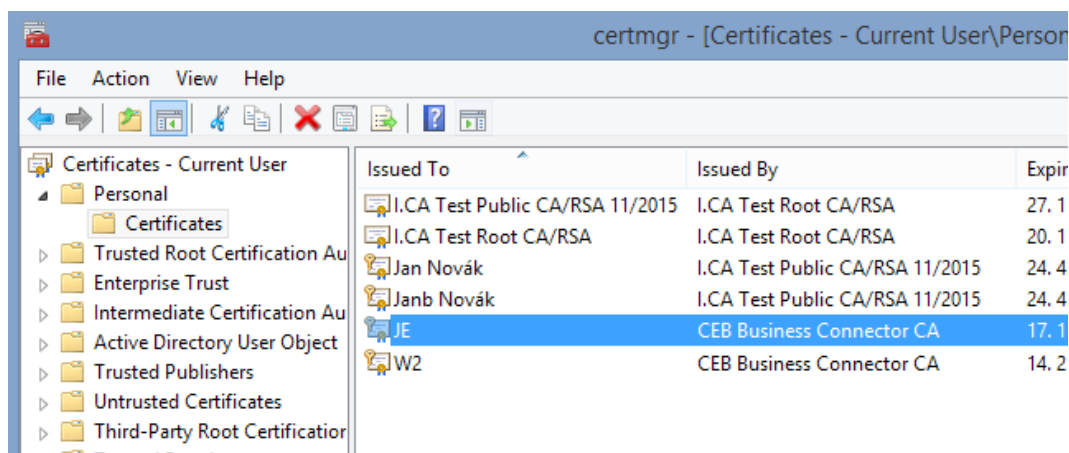
Zpět Uložit

2.5 Záloha certifikátu a privátního klíče

Doporučujeme po zprovoznění konektivity s bankou provést zálohu certifikátu a privátního klíče podle následujícího postupu. Záloha souboru s certifikátem (*.cer, popř. *.crt) není dostačující pro znovuvedení do provozu např. po chybě HW nebo reinstalaci operačního systému, jelikož tento soubor neobsahuje privátní klíč.

Stiskněte klávesy **Windows + R** a do otevřeného okénka napište certmgr.msc a stiskněte OK.

V nástroji certmgr rozbalte po levé straně *Osobní* a v seznamu nalezněte řádek certifikátu. Bude mít vydavatele CEB Business Connector CA a jméno subjektu, které jste zvolili.



Stiskněte na certifikátu pravé tlačítko myši a v kontextovém menu vyberte *Všechny úkoly a Exportovat...*

V průvodci exportem certifikátu vyberte *Ano, exportovat privátní klíč* a následně proved'te export do souboru PKCS #12 s koncovkou .pfx.

2.6 Zneplatnění certifikátu v případě kompromitace klíče

Pokud nastane situace, že došlo ke ztrátě nebo zneužití privátního klíče k certifikátu (krádež počítače, hackerský útok, neoprávněná manipulace zaměstnancem apod.), máte povinnost certifikát zneplatnit. K tomu slouží standardní mechanismus příslušné vydávající certifikační autority (I. CA, PostSignum). Tím dojde k zablokování certifikátu pro veškeré použití včetně možnosti komunikovat se službou ČSOB Business Connector v bance.

Dále je vhodné takový certifikát zablokovat nebo úplně odebrat v administraci ČSOB Business Connectoru v portálu, kde jste jej registrovali.

Certifikáty ⓘ

[Přidat certifikát](#) [Požádat o certifikát](#)

Sériové číslo	Název certifikátu	Subjekt	Vydavatel	Expirace	Stav	
123456789	Jan Nováček	PC_Jan_Novacek	iCA	15.11.2018 09:12:22	aktivní	Stáhnout Zablokovat Smazat
987654321	Blokovaný	Mock1	Issuer1	01.02.2020 12:34:55	blokový	Stáhnout Zablokovat Smazat
Expirovaný						
123123123	Expirovaný aktivní	Mock2	Issuer2	01.01.2017 00:00:00	aktivní	...
Expirovaný						
321321321	Expirovaný blokový	Mock3	Issuer3	01.01.2017 00:00:00	blokový	...
Expirovaný						

Certifikáty vydané bankou nemají mechanismus odvolání platnosti certifikátu.

Pro zablokování kompromitovaného certifikátu, který byl vydán přímo bankou, slouží administrativní rozhraní pro konfiguraci ČSOB Business Connectoru v portálu. Konkrétně je nutné certifikát zablokovat nebo odebrat ze seznamu certifikátů.

Pokud je certifikát používán ve více smlouvách, je nutné ho zablokovat nebo odebrat ze seznamu certifikátů u všech smluv.

3 ROZHRANÍ SLUŽBY ČSOB BUSINESS CONNECTOR PRO CEB PRO TŘETÍ STRANY

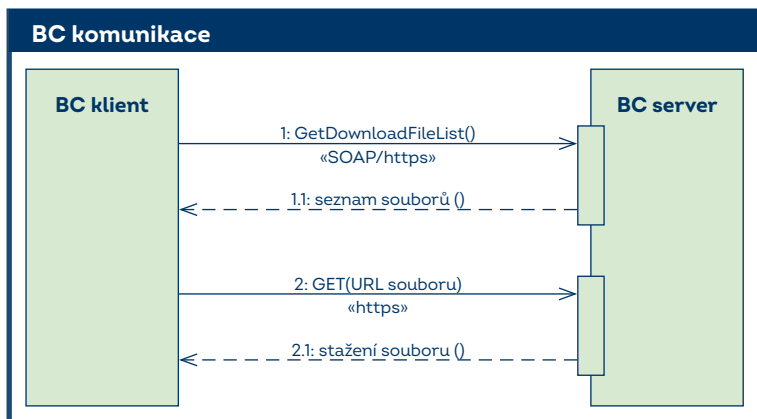
Tato kapitola popisuje technické rozhraní služby pro potřeby implementace vlastní aplikace pro komunikaci s bankou.

3.1 Principy

Rozhraní služby ČSOB Business Connector je kombinací:

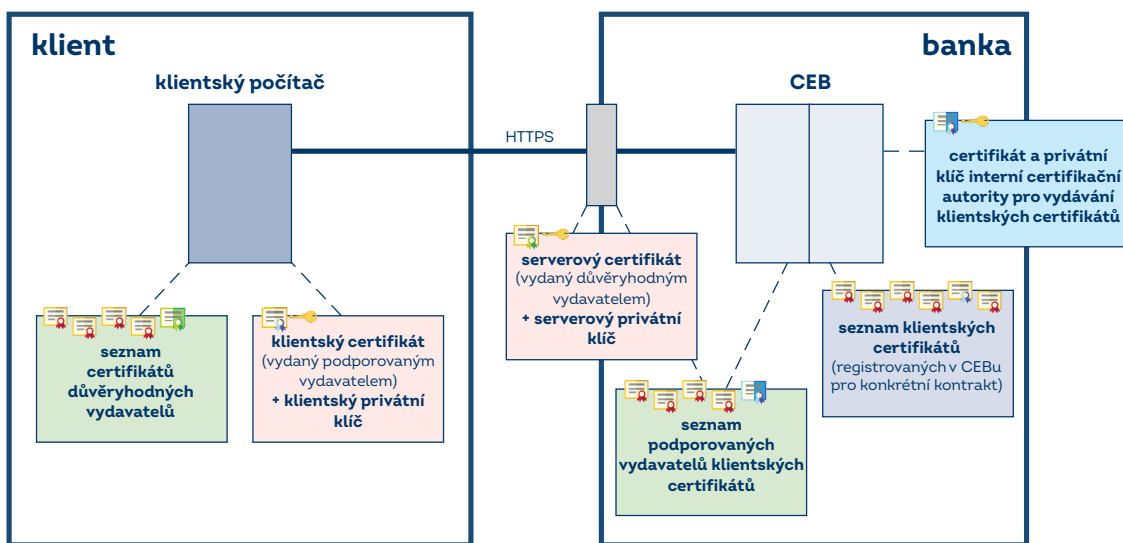
- webové služby využívající SOAP/HTTPS a
- REST služby využívající HTTP operace GET a POST.

Operace webové služby slouží ke koordinaci a řízení procesu, zatímco REST rozhraní slouží k vlastnímu přenosu souborů, viz následující diagram:



3.1.1 Autentizace

Webová služba (rozhraní SOAP/HTTPS) využívá SSL spojení se vzájemnou autentizací certifikátů klienta a serveru. To znamená, že jak server banky, tak aplikace u klienta se prokazují svým certifikátem a autentizují se privátním klíčem příslušným k certifikátu. Což znamená, že oproti běžnému HTTPS spojení navíc klient použije klientský přístupový SSL certifikát k autentizaci. Tento certifikát musí být registrován pro použití ve službě ČSOB Business Connector, viz [kap. 2.2](#).



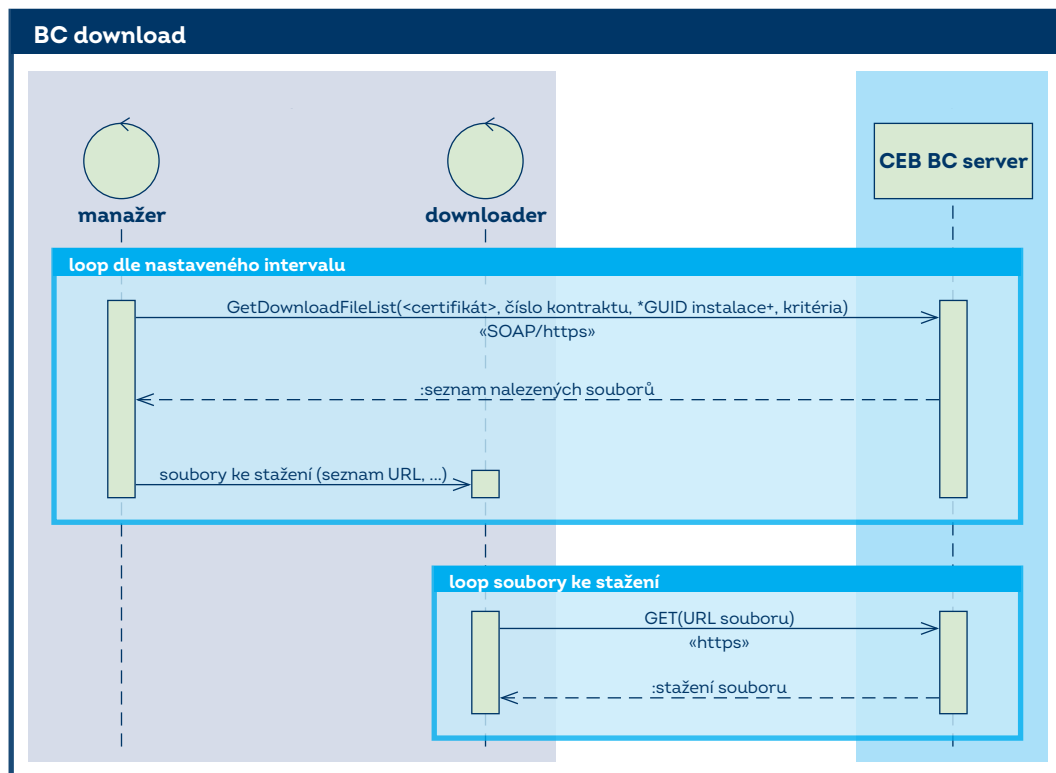
- certifikát serveru s privátním klíčem
- certifikát vydavatele certifikátu serveru
- klientský certifikát s privátním klíčem
- klientský certifikát
- certifikát vydavatele klientského certifikátu

Pozn.: Certifikát vydavateléské CA klientského certifikátu není doporučeno instalovat jako globální důvěryhodný certifikát OS. Pro autentizaci a komunikaci to není obvykle nutné. Může být ovšem nutné (dle možností platformy a implementace) tento CA certifikát např. instalovat do seznamu důvěryhodných vydavatelů klientské aplikace.

REST služba (rozhraní HTTPS) pro stahování/odesílání souborů využívá také SSL spojení se vzájemnou autentizací certifikátů klienta a serveru. Navíc je identita klienta obsažena v HTTP hlavičce a současně (v zašifrované podobě) i přímo v URL.

3.1.2 Stahování souborů

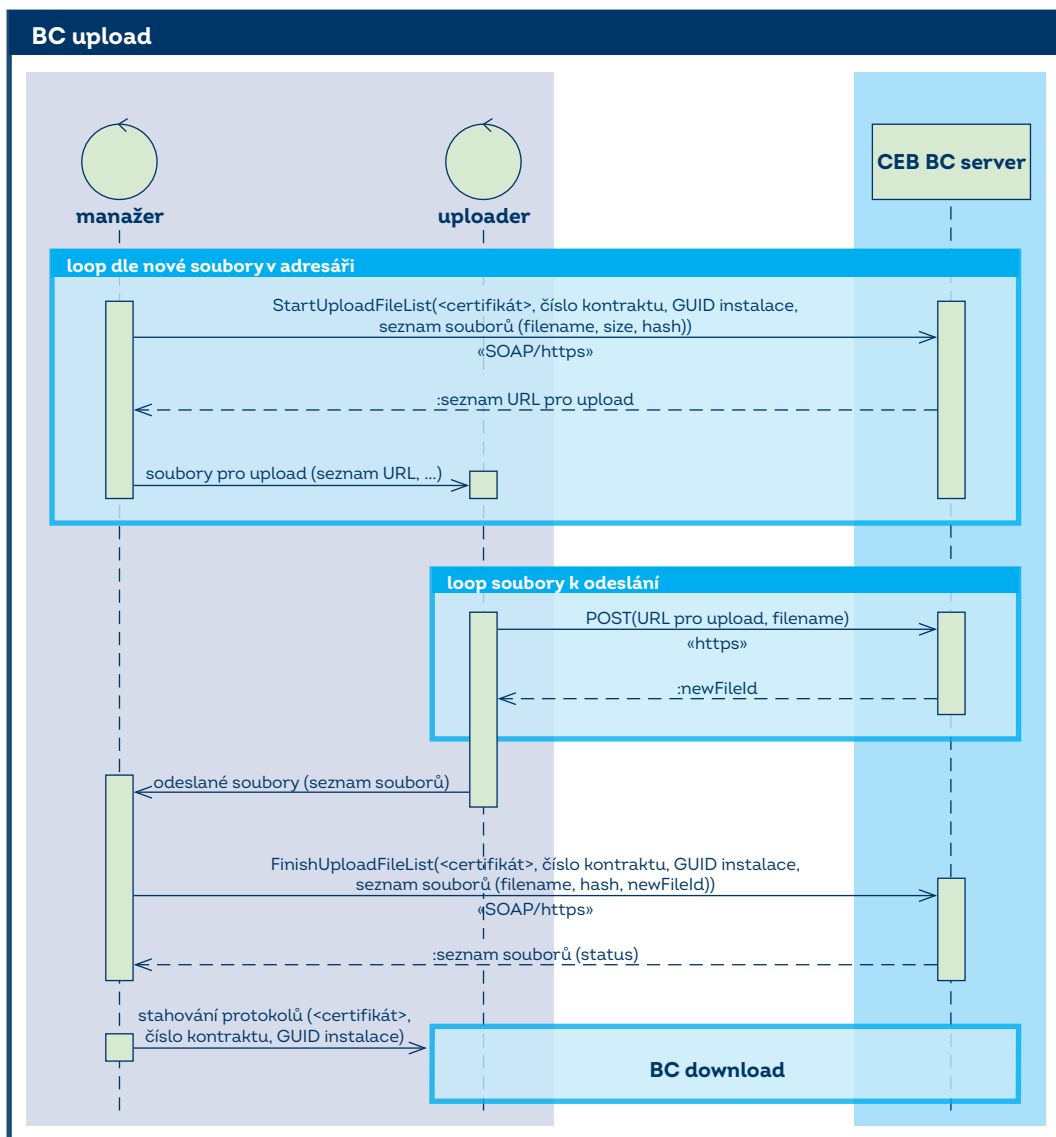
Proces stahování souborů by měl probíhat ve dvou vláknech. Vlákno manažer pravidelně zjišťuje, zda se na serveru objevily nové soubory ke stažení. Oddělené vlákno provádí průběžné stahování těchto souborů.



3.1.3 Odesílání souborů

Odesílání souborů probíhá v několika krocích, které mohou být realizovány v oddělených vláknech. Vlákno manažer monitoruje registrovaný adresář a pro soubory, které se zde objeví, si od serveru vyžádá URL, kam je možné tyto soubory odeslat. Oddělené vlákno provádí průběžné odesílání těchto souborů a po úspěšném odeslání souboru (jednotlivě nebo po skupinách) informuje server, že soubor je odeslán a že může započít s jeho zpracováním.

Server soubory zpracovává asynchronně a generuje protokoly o zpracování dávek, které je možné stáhnout pomocí mechanismu stahování souboru, viz předchozí kapitola.



3.2 Webová služba (SOAP/HTTPS)

3.2.1 Operace GetDownloadFileList

Tato metoda je připravena pro pravidelné zjišťování, zda na straně banky nevznikly nové soubory, které je možné stáhnout. Klientská aplikace poskytne kritéria, jaké soubory sleduje. Služba vrátí seznam nalezených souborů a URL, kde je možné soubory stáhnout přes HTTP GET.

3.2.1.1 Vstup

Parametr	Popis
ContractNumber	číslo smlouvy o využívání služby CEB
PrevQueryTimestamp	[nepovinné] datum a čas, kterým klient určuje okamžik, od kterého jej zajímají nové soubory; viz kapitola Monitorování nových souborů; na časový údaj starší než 45 dní v minulosti se nepřihlíží; pokud parametr není uveden, použije se čas 45 dní zpět; formát viz níže
Filter	[nepovinné] filtr, který omezí seznam vrácených souborů podle zadaných kritérií, viz kapitola Filtrovací kritéria níže
Filter/FileTypes Filter/FileTypes/FileType	[nepovinné, násobné] jen soubory vyjmenovaných typů; možné typy jsou: VYPIS – výpisy z účtů AVIZO – avíza plateb KURZY – kurzovní lístky ČNB a ČSOB IMPPROT – protokoly o importu

Filter/FileFormats Filter/FileFormats/FileFormat [od verze služby v3]	[nepovinné, násobné] jen soubory vyjmenovaných formátů; možné formáty jsou pro: <ul style="list-style-type: none"> - lidsky čitelné výpisy z účtu: PDF, TXT - datové výpisy z účtu: XML, BBGPC, BBMT940, BBTXT, BBBBF, SEPAXML - avíza: MT942, BBF, CAMT052 - kurzovní lístky: N/A, tj. FileFormat je ignorován
Filter/FileName	[nepovinné] jen soubor daného jména, včetně přípony
Filter/CreatedAfter	[nepovinné] jen soubory vytvořené po zadaném datu a času (včetně); formát viz níže
Filter/CreatedBefore	[nepovinné] jen soubory vytvořené před zadaným datem a časem (včetně); formát viz níže
Filter/ClientAppGuid	[nepovinné] plus soubory vytvořené speciálně pro danou instanci klientské aplikace (např. protokoly o importu)

3.2.1.1 Filtrovací kritéria

Služba umožňuje použít seznam podmínek, které poslouží jako filtrovací kritéria omezující seznam vrácených souborů.

Je možno seznam omezit (možná i kombinace kritérií):

- podle data vystavení souborů – klient může zadat parametr datum od-do (použití filtru dle **CreatedAfter** a/nebo **CreatedBefore**),
- podle typu – klient si může vybrat jeden typ souboru, více typů nebo všechny (použití filtru **FileType**),
- podle formátu – klient si může vybrat konkrétní formát souboru, seznam formátů nebo bez omezení formátem (použití filtru **FileFormat**),
- podle názvu – možnost stáhnout konkrétní soubor (použití filtru **FileName**),
- dosud nestážené (použití parametru **PrevQueryTimestamp**).

Veškeré časové údaje jsou ve standardním xsd:dateTime formátu YYYY-MM-DDTHH:MM:SS+ZZ:ZZ, který značí:

- **YYYY-MM-DD** – rok, měsíc, den zarovnaný na 4, resp. 2 cifry; měsíc počítaný od 1.,
- **T** – znak velké T oddělující datum a čas,
- **HH:MM:SS** – hodinu, minutu a sekundu časového údaje ve 24hodinovém formátu,
- **+ZZ:ZZ** – časovou zónu v číselném formátu HH:MM, tj. posun oproti GMT; +01:00 pro středoevropský čas a +02:00 pro středoevropský letní čas.

3.2.1.2 Výstup

Parametr	Popis
QueryTimestamp	datum a čas provedení volání služby vygenerované serverem, určené pro použití v následujícím volání jako obsah parametru PrevQueryTimestamp
FileList/FileDetail	[nepovinné, násobné] seznam nalezených souborů
FileList/FileDetail/Url	[nepovinné] URL, kde je možné soubor stáhnout; pokud je soubor teprve připravován pro download nebo příprava selhala, tak tento element nebude vyplněn; URL je možné získat opakovaným dotazem (s původním PrevQueryTimestamp)
FileList/FileDetail/Filename	jméno souboru včetně přípony
FileList/FileDetail/Type	možné typy jsou: VYPIS – výpisy z účtů AVIZO – avíza plateb KURZY – kurzovní lístky ČNB a ČSOB IMPPROT – protokoly o importu
FileList/FileDetail/Format [od verze služby v3]	formát souboru; možné formáty jsou: <ul style="list-style-type: none"> - pro lidsky čitelné výpisy z účtu: PDF, TXT - pro datové výpisy z účtu: XML, BBGPC, BBMT940, BBTXT, BBBBF, SEPAXML - pro avíza: MT942, BBF, CAMT052 - pro kurzovní lístky: nebude uveden
FileList/FileDetail/CreationDateTime	datum a čas, kdy byl soubor vygenerován
FileList/FileDetail/Size	velikost souboru v bajtech

FileList/FileDetail/UploadFileHash	[nepovinné] jen u protokolů o importu; MD5 suma identifikující odeslaný soubor s platebními příkazy, pro který byl tento soubor s protokolem vytvořen (32 hex znaků)
FileList/FileDetail/Status	stav přípravy souboru ke stažení: R – zkusit znovu, soubor se připravuje D – možno zahájit download dle URL F – permanentní chyba, zalogovat
TicketId	unikátní identifikace původního requestu pro dohledání chyby v bance

3.2.1.3 Chyby

V případě aplikační chyby služba vrací SOAP Fault, kde indikuje problém, který nastal.

Parametr	Popis
Code	chybový kód, viz níže
Text	chybová zpráva
TicketId	unikátní identifikace původního requestu pro dohledání chyby v bance

Možné chybové kódy jsou:

Code	Popis
1000	obecná chyba na straně serveru
1002	kontrakt nemá povolen přístup přes Business Connector
1011	certifikát není registrován pro použití v Business Connectoru, kontrakt neexistuje nebo není aktivní
1012	certifikát je blokován pro použití v Business Connectoru
1101	přístup je dočasně blokován kvůli nadměrnému počtu volání

3.2.1.4 Verze

Verze	popis
v1	originální verze – již nelze používat
v2	doplněn TicketId v odpovědi
v3	přidána možnost filtrovat dle FileFormat (PDF, TXT, ...)

3.2.1.5 Monitorování nových souborů

Pokud se na vstupu použije parametr *PrevQueryTimestamp*, služba vrátí pouze ty soubory, které začaly být k dispozici pro stažení až po tomto uvedeném čase. Aplikace může tohoto využít k monitorování, že jsou k dispozici nové soubory ke stažení. Hodnotu *QueryTimestamp*, kterou služba *GetDownloadFileList()* vrací v každé odpovědi, aplikace při následujícím volání dosadí do vstupního parametru *PrevQueryTimestamp*. Aby byly výsledky konzistentní, musí aplikace mezi těmito voláními zachovat ostatní parametry jako *ContractNumber* a *Filter*. Pokud služba vrátí chybu, aplikace musí volání zopakovat s původním *PrevQueryTimestamp*.

Pokud soubor již byl v bance vygenerován, služba o něm ví a vrací ho v odpovědi, ale ještě není připraven ke stažení, bude v odpovědi tato skutečnost indikována u souboru statusem 'R' a URL pro stažení bude (zatím) chybět. Klientská aplikace musí volání zopakovat později s původním *PrevQueryTimestamp*, dokud služba vrací v seznamu souborů některý soubor bez URL ke stažení. Soubory, které již jsou k dispozici pro stažení (tj. služba u nich vrátila status 'D' a URL), mohou být mezitím již stahovány. Aplikace by měla použít jiný (kratší) interval na takové opakované volání služby, avšak musí stále respektovat minimální ochranný interval mezi voláními.

Poznámka: Služba vrátí jen takové soubory, které vznikly v době, kdy bylo v nastavení Business Connectoru povoleno stahování souborů pro konkrétní účet. Služba nevrátí soubory vygenerované v bance před tím, než bylo povoleno stahovat aktivováno, nebo v době, kdy bylo povolení ke stahování souborů dočasně vypnuté.

3.2.2 Operace StartUploadFileList

Tato metoda slouží k zahájení procesu odeslání souborů do banky. Klient ji volá v okamžiku, kdy potřebuje odeslat soubor, např. na své straně zjistil, že se v adresáři objevily nové soubory. Klientská aplikace zasílá seznam obsahující informace o souborech, které hodlá odesílat. Služba vrací seznam URL, na která je možné soubory nahrát přes HTTP POST.

3.2.2.1 Vstup

Parametr	Popis
ContractNumber	číslo smlouvy o využívání služby CEB
ClientAppGuid	GUID konkrétní instalace klientské aplikace, která volání provedla – očekává se řetězec hex znaků ve formátu: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx (tedy 8zn-4zn-4zn-4zn-12zn bez složených závorek), viz https://en.wikipedia.org/wiki/Universally_unique_identifier
FileList	[povinné, násobné] seznam souborů, které klient hodlá odeslat
FileList/ImportFileDetail	detail souboru
FileList/ImportFileDetail/Filename	jméno souboru včetně přípony; omezeno na 50 znaků
FileList/ImportFileDetail/Hash	MD5 suma obsahu souboru (32 hex znaků)
FileList/ImportFileDetail/Size	velikost souboru v bajtech
FileList/ImportFileDetail/Format	formát souboru (ABO, DUZ, MC TPS, MC ZPS, TXT TPS, TXT ZPS, XLS TPS, XLS ZPS, XLSX TPS, XLSX ZPS, MT101, XML SEPA, XML TPS, XML ZPS)
FileList/ImportFileDetail/Separator	[nepovinné] oddělovač polí; znaky , /, :, ;, ; nebo ;; pokud není uveden, jedná se o soubor s pevnou šířkou polí
FileList/ImportFileDetail/Mode	způsob reakce na chyby při importu: IncludeIncorrect – přijmout i chybné položky OnlyCorrect – přijmout pouze bezchybné položky AllOrNothing – nepřijmout žádnou položku při výskytu chyby SignedAllOrNothing [pro Odesílání podepsaných souborů] – automaticky autorizovat, ale nepřijmout žádnou položku při výskytu chyby

3.2.2.2 Výstup

Parametr	Popis
FileList	[povinné, násobné] seznam nalezených souborů
FileList/FileUrl	detail pro nahrání souboru
FileList/FileUrl/Filename	jméno souboru včetně přípony ze vstupu
FileList/FileUrl/Hash	MD5 suma obsahu souboru (32 hex znaků) ze vstupu
FileList/FileUrl/Status	stav souboru: R – odmítnuto (již importováno, ...) – zalogovat U – možno zahájit upload dle URL
FileList/FileUrl/Url	[nepovinné] URL, kam je možné soubor nahrát, pokud je Status = "U"
TicketId	unikátní identifikace původního requestu pro dohledání chyby v bance

3.2.2.3 Chyby

V případě aplikační chyby služba vrací SOAP Fault, kde indikuje problém, který nastal.

Parametr	Popis
Code	chybový kód, viz níže
Text	chybová zpráva
TicketId	unikátní identifikace původního requestu pro dohledání chyby v bance

Možné chybové kódy jsou:

Code	Popis
1000	obecná chyba na straně serveru
1002	kontrakt nemá povolen přístup přes Business Connector
1011	certifikát není registrován pro použití v Business Connectoru, kontrakt neexistuje nebo není aktivní
1012	certifikát je blokován pro použití v Business Connectoru
1101	přístup je dočasně blokován kvůli nadměrnému počtu volání

3.2.2.4 Verze

Verze	popis
v1	URL, které služba vrací, jsou určeny pro upload ve formátu „octet-stream“ (viz kap. 3.3.2)
v2	URL, které služba vrací, jsou určeny pro upload ve formátu „multipart“ (viz kap. 3.3.2)

3.2.3 Operace FinishUploadFileList

Tato metoda slouží k dokončení odesílání souborů do banky. Klient ji volá v okamžiku, kdy úspěšně nahrál soubory na URL poskytnutá službou *StartUploadFileList()* a chce zahájit jejich zpracování. Klientská aplikace posílá seznam souborů a jejich identifikaci odkazující na předchozí volání metody *StartUploadFileList()* a HTTP POST. Služba zahájí asynchronní zpracování souborů. Výsledek zpracování je později k dispozici ve formě protokolu, který klientská aplikace stáhne pomocí volání *GetDownloadFileList()*.

3.2.3.1 Vstup

Parametr	Popis
ContractNumber	číslo smlouvy o využívání služby CEB
ClientAppGuid	GUID konkrétní instalace klientské aplikace, která volání provedla – očekává se řetězec hex znaků ve formátu: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx (tedy 8zn-4zn-4zn-4zn-12zn bez složených závorek), viz https://en.wikipedia.org/wiki/Universally_unique_identifier
FileList	[povinné, násobné] seznam souborů, které klient odeslal
FileList/FileId	identifikace souboru
FileList/FileId/Filename	jméno souboru včetně přípony; omezeno na 50 znaků
FileList/FileId/Hash	MD5 suma obsahu souboru (32 hex znaků)
FileList/FileId/NewFileId	zakódované ID, které vrátil HTTP POST

3.2.3.2 Výstup

Parametr	Popis
FileList	[povinné, násobné] seznam nalezených souborů
FileList/FileStatus	detail pro nahrání souboru
FileList/FileStatus/Filename	jméno souboru včetně přípony ze vstupu
FileList/FileStatus/Hash	MD5 suma obsahu souboru (32 hex znaků) ze vstupu
FileList/FileStatus/Status	stav souboru: R – odmítnuto (již jednou importováno, vadný podpis, ...) → zapsat do logu, neopakovat odesílání I – import zahájen → naplánovat stažení protokolu o importu
TicketId	unikátní identifikace původního requestu pro dohledání chyby v bance

3.2.3.3 Chyby

V případě aplikační chyby služba vrací SOAP Fault, kde indikuje problém, který nastal.

Parametr	Popis
Code	chybový kód, viz níže
Text	chybová zpráva
TicketId	unikátní identifikace původního requestu pro dohledání chyby v bance

Možné chybové kódy jsou:

Code	Popis
1000	obecná chyba na straně serveru
1002	kontrakt nemá povolen přístup přes Business Connector
1011	certifikát není registrován pro použití v Business Connectoru, kontrakt neexistuje nebo není aktivní
1012	certifikát je blokován pro použití v Business Connectoru
1101	přístup je dočasně blokován kvůli nadměrnému počtu volání

3.2.4 WSDL a adresa služby

<https://www.csob.cz/portal/documents/10710/15100026/ceb-bc-wsdl.zip>

Služba je vystavena na následujícím URL.

Produkční prostředí:

<https://ceb-bc.csob.cz/ceb-bc/api>

Demo prostředí (sandbox) pro testování API:

<https://testceb-bc.csob.cz/ceb-bc/api>

3.2.5 Ochranný interval použití služby

Webová služba ČSOB Business Connectoru nedovolí častější volání, než je definovaný počet za určitou dobu. Tento počet volání je sledován pro konkrétní dvojici číslo smlouvy / klientský přístupový certifikát a jeho účelem je ochrana služby před přetížením.

V současné době je tento počet nastaven na hodnotu 30 volání za 20 minut (může být bankou upraven).

Implementace klienta musí zajistit takový režim a časování využití služeb, aby se chyba 1101 (přístup je blokován kvůli nadměrnému počtu volání) neobjevovala pravidelně. Tato chyba se může objevit jen např. při ručním vyvolání služby mimo pravidelný interval.

Pokud by aplikace prováděla takové množství volání soustavně, nedojde kvůli neustálému obnovování časovače nikdy k úspěšnému vyřízení.

Pokud existuje více běžících klientských aplikací, které pracují se stejným kontraktem a používají stejný klientský přístupový certifikát, hrozí při příliš krátkém intervalu stahování, resp. odesílání, souborů souběh volání mezi aplikacemi, který povede k pravidelnému výskytu chyby 1101. Proto doporučujeme pro každou instalaci klientské aplikace jiný certifikát.

3.2.6 Odstávka služby

V případě odstávky služby bude služba vracet HTTP status:

503 Service Unavailable

3.3 REST služba (HTTP download/upload)

Služba je vystavena na URL:

- <https://ceb-bc.csob.cz/ExtFileHubDown/...> pro stahování souborů,
- <https://ceb-bc.csob.cz/ExtFileHubUp/...> pro odesílání souborů jako multipart a
- <https://ceb-bc.csob.cz/OBSOLETE/ExtFileHubUp/...> pro odesílání souborů jako octet-stream.

Testovací prostředí používá URL:

- <https://testceb-bc.csob.cz/ceb-mock/download?id=...> pro stahování souborů a
- <https://testceb-bc.csob.cz/ceb-mock/upload?id=...> pro odesílání souborů.

Klientská aplikace použije vždy beze změny takové URL, jaké vrátila příslušná webová služba GetDownloadFileList, resp. StartUploadFileList.

3.3.1 HTTP GET (download souboru)

Příklad požadavku na stažení souboru z URL (získané z odpovědi služby GetDownloadFileList).

<https://ceb-bc.csob.cz/ExtFileHubDown/v2/download?id=aQGdgoeBcZdGxGco+pVDseLnBeN>.

GET /ExtFileHubDown/v2/download?id=aQGdgoeBcZdGxGco+pVDseLnBeN HTTP/1.1

3.3.1.1 HTTP Status

Služba vrací tyto chybové status kódy:

HTTP Status	Obsah	Řešení
200	OK	OK, hotovo
400	URL expirovalo; soubor je možné stáhnout pouze 15 dní	NOK, konec
401	chyba autorizace	NOK, konec
404	soubor expiroval; soubor je možné stáhnout pouze 15 dní	NOK, konec
500	interní chyba serveru	zkusit znovu
503	služba není dostupná	zkusit znovu

3.3.2 HTTP POST (upload souboru)

3.3.2.1 Odeslání souboru jako octet-stream (pouze pro URL z verze v1 služby StartUploadFileList)

Příklad požadavku na odeslání souboru jako octet-stream:

```
POST /ExtFileHubUp/v2/upload?id=jwomfHhnMqmPkLJGHg HTTP/1.1
```

```
Content-Disposition: attachment; filename="<jméno souboru>"
```

```
Content-Type: application/octet-stream
```

```
Content-Length: <velikost souboru>
```

<obsah souboru>

HTTP Header	Obsah
Content-Disposition:	attachment; filename="<jméno souboru>", kde <jméno souboru> je jméno odesílaného souboru; pokud obsahuje např. české znaky, tak musí být použit MIME encoding, viz https://tools.ietf.org/html/rfc2047
Content-Type	application/octet-stream
Content-Length	velikost souboru v bajtech

Obsah a přítomnost dalších standardních hlaviček viz popis protokolu HTTP.

3.3.2.2 Odeslání souboru jako multipart (pouze pro URL z verze v2 služby StartUploadFileList)

Příklad požadavku na odeslání souboru jako MIME multipart:

```
POST /ExtFileHubUp/v2/upload?id=encodedValue
```

```
Content-Type: multipart/form-data; boundary=---ABCDEFHG
```

```
Content-Length: <velikost zprávy>
```

```
---ABCDEFHG
```

```
Content-Disposition: form-data; name="fileupload"; filename="<jméno souboru>"
```

```
Content-Type: application/octet-stream
```

<obsah souboru>

```
---ABCDEFHG--
```

HTTP Header	Obsah
Content-Type	multipart/form-data; boundary="<náhodný řetězec>"
Content-Length	počet bajtů celé MIME zprávy

Obsah a přítomnost dalších standardních hlaviček viz popis protokolu HTTP.

MIME part header	obsah
Content-Disposition:	attachment; filename="<jméno souboru>", kde <jméno souboru> je jméno odesílaného souboru; pokud obsahuje např. české znaky, tak musí být použit MIME encoding viz https://tools.ietf.org/html/rfc2047
Content-Type	application/octet-stream

3.3.2.3 Odpověď

Služba vrací v případě úspěchu JSON objekt v tomto tvaru:

```
{
  "Status": "201",
  "ExtFileUrl": "",
  "NewFileId": "QqGQl_Zk5e9RGphGoKv4YbAihKSeTadC"
}
```

HTTP Status	Obsah
Status	výsledek uploadu (rozšířený HTTP Status, viz níže)
ExtFileUrl	nepoužito
NewFileId	identifikátor odeslaného souboru

Služba vrací tyto status kódy:

HTTP Status	Popis	Řešení
200	OK	OK, hotovo
201	OK, soubor vytvořen	OK, hotovo
400	V requestu chybí povinné parametry; soubor neexistuje	NOK, konec
401	chyba autorizace	NOK, konec
403	neautorizováno; URL expirovalo	NOK, konec
408	timeout	zkusit znovu
200 Status: 450	překročena velikost souboru	NOK, konec
200 Status: 451	nepovolená přípona souboru	NOK, konec
200 Status: 452	nepovolený typ souboru	NOK, konec
200 Status: 453	soubor neprošel antivirovou kontrolou	NOK, konec
200 Status: 454	nepovolený tvar URL nebo obsahu; nelze uploadovat na takovou adresu anebo nelze použít takový Content Type	NOK, konec
200 Status: 455	timeout	zkusit znovu
200 Status: 456	timeout	zkusit znovu
500	interní chyba serveru	zkusit znovu
502	chyba na gateway	zkusit znovu
503	služba není dostupná	zkusit znovu
504	timeout	zkusit znovu

3.4 Chyby spojení

Je zodpovědností implementace klientské aplikace rozlišovat a logovat důvody nenavázání spojení na:

- síťové úrovni (např. timeout spojení, DNS resolution apod.),
- úrovni SSL (např. certifikát je neplatný, certifikát je zneplatněný, verze protokolu apod.),
- HTTP úrovni (např. odstávka služby, timeout, neautorizováno apod.),
- SOAP úrovni (např. příliš časté dotazy, neznámý certifikát, služba není povolena smluvně apod.)

tak, aby bylo možné provést korektně diagnostiku a nalézt příčinu problému.

3.4.1 Chyby na síťové úrovni

Problémy na této úrovni jsou způsobeny nestabilním internetovým připojením, chybou konfigurace, přetížením služby apod. a mají obvykle dočasný charakter. Klientská aplikace by měla provést opakovaný pokus o spojení dříve, než je uživatelem nastavený interval pro zjišťování změn, resp. odesílání souborů, ne však dříve než po uplynutí minimálního ochranného intervalu.

3.4.2 Chyby SSL (SSL Alerts)

Služba vrací standardní chybové (alert) kódy definované v RFC příslušných protokolů (viz <https://tools.ietf.org/html/rfc5878#section-4>).

3.4.3 Chyby HTTP (HTTP Status)

Služba vrací standardní chybové (status) kódy HTTP k indikaci problémů na úrovni HTTP (viz <https://tools.ietf.org/html/rfc2616#section-10>).

3.5 Testovací demo prostředí

Pro účely testování implementace klientských aplikací pro vývojáře třetích stran bylo zřízeno zkušební (sandbox) prostředí s těmito vlastnostmi.

- Rozhraní webových i REST služeb je shodné s produkčním prostředím, liší se pouze doménová část URL adresy služby, viz [3.2.5](#).
- Odpovědi webových i REST služeb jsou statické, částečně generované dle jednoduchých pravidel.
- Prostředí neudrží žádnou stavovou informaci mezi jednotlivými voláními.
- Číslo smlouvy na vstupu webových služeb (element ContractNumber) je ignorováno.
- Kritéria filtrování souboru v GetFileDownloadList jsou ignorována.
- Služby nevyžadují dodržování ochranného intervalu, viz [3.2.5](#).
- Autentizace certifikátem je vyžadována, ale nemá vliv na obsah zpráv.
- Akceptovány jsou certifikáty vydané stejnými certifikačními autoritami jako v produkčním prostředí včetně certifikátů vydávaných interně ČSOB a testovací certifikáty těchto certifikačních autorit.
- Není vyžadována registrace certifikátu v CEBu ani není nutné mít CEB vůbec zřízený.

3.6 Technické požadavky

3.6.1 Parametry klientského certifikátu

Certifikát a soukromý klíč použitý na straně klienta musí splňovat tyto požadavky:

Požadavek	
vydavatel certifikátu	I.CA: <ul style="list-style-type: none">- C=CZ, O=První certifikační autorita, a.s., CN = I.CA Root CA/RSA 05/2022, serialNumber=NTRCZ-26439395 Not Before: May 03 12:05:00 2022 GMT Not After : May 03 12:05:00 2047 GMT SHA-1:461fdd19e71cd4329aadf224dc8c8628cd10fae8- C=CZ, O=První certifikační autorita, a.s., CN=I.CA Root CA/ECC 05/2022, serialNumber=NTRCZ-26439395 Not Before: May 03 12:10:00 2022 GMT Not After : May 03 12:10:00 2047 GMT SHA-1: 702723132527203947e0a97829a0731372b03917- C=CZ, O=První certifikační autorita, a.s., CN = I.CA Root CA/RSA 05/2022, serialNumber=NTRCZ-26439395 Not Before: Jun 20 12:00:22 2022 GMT Not After : Jun 17 12:00:22 2032 GMT SHA-1: 000c90caa3a95065fd2e5d7836bd45eed38c18f- C=CZ, O=První certifikační autorita, a.s., CN = I.CA Root CA/ECC 05/2022, serialNumber=NTRCZ-26439395 Not Before: Jun 20 12:52:24 2022 GMT Not After : Jun 17 12:52:24 2032 GMT SHA-1: 6aa1d638ce08e8ff85c617e6b4b4c5cb1541b999- C=CZ, O=První certifikační autorita, a.s., CN=I.CA Root CA/RSA, serialNumber=NTRCZ-26439395 Not Before: May 27 12:20:00 2015 GMT Not After : May 27 12:20:00 2040 GMT SHA-1: 9b0959898154081bf6a90e9b9e58a4690c9ba104- C=CZ, CN=I.CA Public CA/RSA 07/2015, O=První certifikační autorita, a.s., serialNumber=NTRCZ-26439395 Not Before: Jul 8 12:36:40 2015 GMT Not After : Jul 5 12:36:40 2025 GMT SHA-1: a9d6b0afdd51691a2f9130d9af998c8195f97a83

- C=CZ, CN=I.CA SSL CA/RSA 07/2015, O=První certifikační autorita, a.s., serialNumber=NTRCZ-26439395
Not Before: Jul 8 12:18:18 2015 GMT
Not After : Jul 5 12:18:18 2025 GMT
SHA-1: 984fd6ba71dbb50fe2aca83e476d4f61584d4243

PostSignum:

- C=CZ, O=Česká pošta, s.p. [IČ 47114983], CN=PostSignum Root QCA 2
Not Before: Jan 19 09:04:31 2010 GMT
Not After : Jan 19 09:04:31 2025 GMT
SHA-1: A0F8DB3F0BF417693B282EB74A6AD86DF9D448A3
- C=CZ, O=Česká pošta, s.p. [IČ 47114983], CN=PostSignum Public CA 3
Not Before: Mar 20 09:28:38 2017 GMT
Not After : Jan 19 09:04:31 2025 GMT
SHA-1: 92A04A6805AD4317234F11D16B583981A64F02A1
- C=CZ, O=Česká pošta, s.p., CN=PostSignum Root QCA 4
Not Before: Jul 26 09:56:08 2018 GMT
Not After : Jul 26 09:56:08 2038 GMT
SHA-1: aa40d2579ba82424cd27719b1d6b1f3571738099
- C=CZ, O=Česká pošta, s.p., CN=PostSignum Public CA 4, 2.5.4.97=NTRCZ-47114983
Not Before: Sep 27 10:19:35 2018 GMT
Not After : Sep 27 10:19:35 2033 GMT
SHA-1: 1311e16d9903f914167e222b2326f699d4835fee
- C=CZ, O=Česká pošta, s.p., CN=PostSignum Public CA 5, 2.5.4.97=NTRCZ-47114983
Not Before: Oct 03 06:48:01 2018 GMT
Not After : Oct 03 06:48:01 2033 GMT
SHA-1: a6147a88433278d9able655bb8ba315fec4640d2

Certifikáty vydávané interně ČSOB Business Connectorem:

- CN= CEB Business Connector CA, O=Československá obchodní banka a.s., C=CZ, S = Prague
Not Before: Mar 21 13:01:22 2018
Not After : Mar 21 13:01:22 2028
SHA-1: A72CA62B0A214EBB1904EF9B1D5574A71EDB649E

algoritmus podpisu	SHA256 nebo silnější
délka klíče	RSA min 2048 bitů
užití klíče (pokud je přítomno)	Digitální podpis nebo Výměna klíčů
rozšířené užití klíče (pokud je přítomno)	SSL klientská autentizace

3.6.2 Požadavky na SSL spojení

Klientská aplikace musí vytvářet SSL spojení pomocí co nejvyšší verze protokolu SSL/TLS.

Server banky klade tyto požadavky:

Požadavek	
verze SSL/TLS	doporučeno TLS 1.2, min. TLS 1.1
subjekt certifikátu na straně banky	atribut CN=ceb-bc.csob.cz ostatní neurčeny
vydavatel certifikátu na straně banky	standardní důvěryhodná certifikační autorita evidovaná ve Windows

3.6.3 Požadavky na HTTP a SOAP

Požadavek	
verze HTTP	HTTP 1.1 nebo HTTP 1.0
verze SOAP	SOAP 1.1
povinné HTTP hlavičky	Content-Type: text/xml; charset=utf-8 SOAPAction: "{operace}" kde {operace} je hodnota atributu soapAction z WSDL elementu <soap:operation> Content-Length: {délka těla zprávy v bajtech}

4 FORMÁTY SOUBORŮ

4.1 Výpisy

Popis struktury formátů pro výpisy obdržené ze služby ČSOB Business Connector naleznete na www.csob.cz/ceb.

4.2 Avíza

Popis struktury formátů pro avíza obdržená ze služby ČSOB Business Connector naleznete na www.csob.cz/ceb.

4.3 Kurzovní lístek

Formát pro kurzovní lístek obdržený ze služby ČSOB Business Connector – zpráva typu QUOTES.

Jméno souboru je:

- EXRT_CNB_yyyymmdd.BBF pro kurzovní lístek ČNB,
- EXRT_CSOb_yyyymmdd.BBF pro kurzovní lístek ČSOB.

Zpráva QUOTES se skládá z jednoho hlavičkového záznamu a ze dvou typů datových záznamů.

Hlavička 01 je dlouhá 32 a má následující tvar:

QUOTES – ZÁZNAM 01 (1krát – první záznam zprávy)

Název	Typ	L	Poz	M/O	Popis
Bankovní aplikace	C	1	1	M	Bankovní aplikace, konst. „T“
Identifikace klienta	C	8	2	M	BB identifikace aplikace klienta
Typ zprávy	C	6	10	M	Typ zprávy
Oddělovač	C	1	16	M	Oddělovač – 1 mezera
Typ záznamu	C	2	17	M	Typ záznamu: „01“ – Hlavičkový záznam zprávy
Unikátní číslo zprávy	C	14	19	M	Jednoznačné číslo zprávy, spolu s app_id (služební položky), musí tvořit jednoznačnou identifikaci zprávy pro všechny zprávy v systému

Záznamy jsou pak rozlišeny položkou „typ záznamu“ (rec_typ) ve služebních položkách na začátku záznamu:

- záznam s obecnými údaji, rec_typ je „02“. Tento záznam obsahuje obecné údaje zprávy QUOTES. Záznam se vyskytuje 1;
- záznam s kurzem, rec_typ je „03“. Tento záznam obsahuje kurzy pro jednu měnu. Záznam se vyskytuje 1-9999. Záznam je podřízený záznamu „02“.

Záznam 02 je dlouhý 76 a má následující tvar:

QUOTES – ZÁZNAM 02

Název	Typ	L	Poz	M/O	Popis
Bankovní aplikace	C	1	1	M	Bankovní aplikace, konst. „N“
Identifikace klienta	C	8	2	M	BB identifikace aplikace klienta
Typ zprávy	C	6	10	M	Typ EDIFACT zprávy – QUOTES
Oddělovač	C	1	16	M	Oddělovač – 1 mezera
Typ záznamu	C	2	17	M	Typ záznamu: „02“ – Datový záznam
Pořadové číslo	N	3	19	O	Pořadové číslo kurzovního lístku
Počátek platnosti	D	8	22	M	Počátek platnosti kurzovního lístku; FORMAT=„CCYYMMDD“
Název poskytovatele	C	35	30	M	Název zdroje (poskytovatele)
Timestamp	C	12	65	M	Timestamp

Záznam 03 je dlouhý 124 a má následující tvar:

QUOTES – ZÁZNAM 03

Název	Typ	L	Poz	M/O	Popis
Bankovní aplikace	C	1	1	M	Bankovní aplikace, konst. „N“
Identifikace klienta	C	8	2	M	BB identifikace aplikace klienta

Typ zprávy	C	6	10	M	Typ EDIFACT zprávy – QUOTES
Oddělovač	C	1	16	M	Oddělovač – 1 mezera
Typ záznamu	C	2	17	M	Typ záznamu: „03“ – Datový záznam
Země	C	35	19	M	Název země
Množství	N	4	54	M	Množství
Filler 2	C	2	58	M	
Kód měny	C	3	60	M	Kód měny
Filler 3	C	1	63	M	
Deviza nákup	N	10.3	64	M	Kurz pro DEVIZY / nákup
Deviza prodej	N	10.3	74	M	Kurz pro DEVIZY / prodej
Deviza střed	N	10.3	84	M	Kurz pro DEVIZY / střed
Filler 4	C	1	94	M	
Valuta nákup	N	10.3	95	M	Kurz pro VALUTY / nákup
Valuta prodej	N	10.3	105	M	Kurz pro VALUTY / prodej
Valuta střed	N	10.3	115	M	Kurz pro VALUTY / střed

Poznámka: Formát pro kurzy je "C.D" 6 míst+"."+3 místa

Příklad souboru se záznamy kurzů:

TTDCEB	QUOTES	0120180831057299								
NTDCEB	QUOTES	0216820180831CSOB							201808310656	
NTDCEB	QUOTES	03AUSTRALIAN DOLLAR	1	AUD	15.617	16.415	16.016	0.000	0.000	0.000
NTDCEB	QUOTES	03CANADIAN DOLLAR	1	CAD	16.553	17.400	16.977	0.000	0.000	0.000
NTDCEB	QUOTES	03SWISS FRANC	1	CHF	22.244	23.385	22.815	22.244	23.385	22.815
NTDCEB	QUOTES	03CHINA JUAN	1	CNY	3.033	3.421	3.227	0.000	0.000	0.000
NTDCEB	QUOTES	03DANISH KRONER	1	DKK	3.371	3.543	3.457	3.371	3.543	3.457
NTDCEB	QUOTES	03EUROPEAN CURRENCY UNIT	1	EUR	25.135	26.412	25.773	25.135	26.412	25.773
NTDCEB	QUOTES	03BRITISH POUND	1	GBP	28.027	29.459	28.743	28.027	29.459	28.743
NTDCEB	QUOTES	03CHORVATSKA KUNA	1	HRK	3.375	3.555	3.465	0.000	0.000	0.000
NTDCEB	QUOTES	03HUNGARIAN FORINT	100	HUF	7.681	8.080	7.881	0.000	0.000	0.000
NTDCEB	QUOTES	03JAPANESE YEN	100	JPY	19.406	20.397	19.901	0.000	0.000	0.000
NTDCEB	QUOTES	03NORWEGIAN KRONER	1	NOK	2.581	2.714	2.647	2.581	2.714	2.647
NTDCEB	QUOTES	03POLISH ZLOTY	1	PLN	5.840	6.144	5.992	0.000	0.000	0.000
NTDCEB	QUOTES	03RUMANIAN LEI	1	RON	5.407	5.685	5.546	0.000	0.000	0.000
NTDCEB	QUOTES	03RUSSIAN ROUBLE	100	RUB	30.444	34.349	32.396	0.000	0.000	0.000
NTDCEB	QUOTES	03SWEDISH KRONER	1	SEK	2.361	2.482	2.421	2.361	2.482	2.421
NTDCEB	QUOTES	03TURECKÁ LIRA	1	TRY	3.016	3.544	3.280	0.000	0.000	0.000
NTDCEB	QUOTES	03UNITED STATES DOLLAR	1	USD	21.547	22.645	22.096	21.547	22.645	22.096

4.4 Dávky platebních příkazů

Popis struktury formátů pro import dávek příkazů do služby ČSOB CEB naleznete na www.csob.cz/ceb.

4.5 Protokol o importu

Formát pro exportní soubor Protokol o importu ze služby ČSOB Business Connector:

Formát protokolu o importu	XSD pain.002 (ČSOB) a popis formátu protokolu
XML PAIN.002 – protokol import - výstupní protokol o provedeném/ neprovedeném importu dávek příkazů založený na standardu ISO20022 SWIFT pain.002	https://www.csob.cz/portal/documents/10710/15100026/protokol-pain.zip

4.6 Podepsané dávky platebních příkazů

Jedná se o stejnou množinu typů souborů jako v předchozí kapitole. V souboru je navíc vložen interní elektronický podpis ve formátu CAdES-BES a doplněna koncovka .p7m (takže soubor obsahuje dvě koncovky, např. 125456_10000141.zps.p7m). Tento soubor není textovým souborem, textová informace v něm ale není šifrována.

Soubor musí být podepsán certifikátem (na čipové kartě), který je používán pro práci v portálu a k autorizaci transakcí v čekárně – tedy nikoli klientským přístupovým certifikátem určeným pro ČSOB Business Connector, o kterém hovoří kapitola 2!

Podpis CAdES-BES musí být vytvořen v souladu s normami:

- ETSI TS 101 733 (v2.1.1) v úrovni shody BES.
- ETSI EN 319 122-1 v úrovni shody B-B.
- ETSI TS 103 173 v úrovni shody B.

S omezujícími podmínkami:

- V podpisech jsou podporovány atributy content-type, signing-time, signing-certificate (tedy ESS signing-certificate, resp. ESS signing-certificate v2), message-digest. Jakékoliv jiné atributy jsou během procesu ověření ignorovány a neprovádí se jejich kontrola.
- Nejsou podporovány podpisy s definovanou podpisovou politikou.

Podpora vícenásobného podpisu:

Je podporováno ověření paralelních (nezávislých) podpisů. Ověření jiných typů vícenásobných podpisů není podporováno.

Služba ČSOB Business Connector ani klientská aplikace nenabízejí vytváření podepsaných souborů platebních příkazů, vzhledem k standardnímu formátu podpisu je však možné využít komerční software třetích stran.