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.

蕕 certmgr - [Certifikáty – aktuální uživatel\Důvěryhodné kořenové certifikační autority\Certifikáty]

Soubor Akce Zobrazit Nápově	éda		
🗢 🔿 🗖 📅 🤞 🗶 🖻	🗟 🔽 🖬		
 Certifikáty – aktuální uživatel Osobní Důvěryhodné kořenové certif Certifikáty Důvěryhodnost v rámci rozlel 	Vystaveno pro Baltimore CyberTrust Root CEB Business Connector CA Class 3 Public Primary Certificat Copyright (c) 1997 Microsoft C	Vystavitel Baltimore CyberTrust Root CEB Business Connector CA Class 3 Public Primary Certificatio Copyright (c) 1997 Microsoft Corp.	Dat 13.0 10.1 02.0 31.1
 Zprostředkující čertifikáchi ač Živatelský objekt služby Acti Důvěryhodní vydavatelé Nedůvěryhodné certifikáty Kořenové certifikační autority Důvěryhodné osoby 	DigiCert Global Root CA DigiCert High Assurance EV Ro GlobalSign GTE CyberTrust Global Root Hotspot 2.0 Trust Root CA - 03	DigiCert Global Root CA DigiCert High Assurance EV Root GlobalSign GTE CyberTrust Global Root Hotspot 2.0 Trust Root CA - 03	10.1 10.1 18.0 14.0

Pokud tam není, stáhnete certifikát vydavatele ze stránky

<u>https://www.csob.cz/portal/documents/10710/15532355/cebbc-ca.crt</u>. 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] 0ID=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.

ČSOB CEB		C ¹³		Kontakty 499 900 500
û Úvod	< Menu			
Čekárna	Zabezpečení	>		
🧶 Účty	Moje oprávnění		rovozní bě	éžák
e. Platby	Osobní nastavení			
🥝 Inkasa	Nastavení účtů		zdový úč	et
Karty	CEB Info		IR rovozní úd	čet 200
🗠 Finanční trhy	Business Connector			
Správa financí	Správa služby	>		
Virtuální pobočka				
Nastavení			13	Změny ve smlouvě
			15	

Stiskněte tlačítko Požádat o certifikát,

ČSOB CEB		C Kontakty JIŘÍ VOHNOUT 499 900 500 HQ 1U Prezentace EB, id: 42712955 EN (2) 19:29	Odhlásit se
< Menu		Nastavení Business Connector	🖶 Tisk
Zabezpečení	>		
Moje oprávnění		Vase certifikaty	
Osobní nastavení		Přidat Požádat o certifikát	
Nastavení účtů			
CEB Info		Pro odesílání a stahování dat do aplikace Business Connector přidejte platný certifikát.	
Business Connector			_
Správa služby	>	Kurzovní lístek	
		Stahovat kurzovní lístek NE	
			Upravit

vyplňte 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.

ČSOB CEB		Ģ	13) []	C Kontakty 499 900 500	JIŘÍ VOHNOU JIŘÍ VOHNOUT	JT - Prezentace, id: 42711965	~	EN	(2) 19:50	Odhlásit se
< Menu		Nastavení Bu	siness	Connector						🖶 Tisk
Zabezpečení	>									
Moje oprávnění		Žádost o certifiká	t							
Osobní nastavení		Žádost o certifikát *	Vybrat sou	ibor 🥑						
Nastavení účtů		Názov *	BCcertreq.r	eq		D				
CEB Info		NdZev -	KOITIUTIIKAC	пі сеніпкац		9				
Business Connector		Zpět								Odeslat
Správa služby	>									

Potom Stáhněte vydaný certifikát do souboru.

Sériové číslo	Název certifikátu	Subjekt	Vydavatel	Expirace	Stav	<u>rout</u>
123456789	Jan Nováček	PC_Jan_Novacek	iCA	15.11.2018 09:12:22	aktivní Stáhr	
Sériové číslo	Název certifikátu	Subjekt	Vydavatel	Expirace	Stav Stáhr	nout
987654321	Blokovaný	Mock1	Issuer1	01.02.2020 12:34:55	blokovaný	
Expirovaný Sériové číslo 123123123	Název certifikátu Expirovaný aktivní	Subjekt Mock2	Vydavatel Issuer2	Expirace 01.01.2017 00:00:00	Stav 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 certifiká	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*.

Certifikát * Vybrat soubor Název certifikátu * Třetí certif ♥ Otevřít ● Zpět ● Uspořádat ▼ Nová složka ● ● ● <	×
Název certifikátu * Třetí certif Otevřít Zpět	×
Zpět C Dokumenty V C Prohledat: Dokumenty Uspořádat v Nová složka E V Dokumenty Název	
Zpět Uspořádat v Nová složka III v Název	P
Dokumenty ^ Název	
Hudba	Dai ^
🕒 et cit	27.
📮 Obrazky	21.
Excel	27.
Videa V	>
Název souboru:	

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 v 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 Busine	ss Connector			
Kurzovní lístek 🚯				
Stahovat kurzovní lístek				
Zpět		Uložit		
Nastavení propojen	ú		ē	Tisk
Účet				
Účet Typ účtu Název	277430302/0300, CZK, provozní běžák ČSOB Plus Konto v CZK JIŘÍ VOHNOUT-CEB1			
Stahování dat				
 Avíza Výpisy Výpisy pro prohlížení () 				
Odesílání dat				
 Odesílání Odesílání s podpisem (1) 				
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 znovuuvedení 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.

a	certmgr	- [Certificates - Current User\	Persor
File Action View Help Image: Constraint of the state of the stat] 🛃 🛛 🖬		
 Certificates - Current User Personal Certificates Trusted Root Certification Au Enterprise Trust Intermediate Certification Au Active Directory User Object Trusted Publishers Untrusted Certificates Third-Party Root Certificatior 	Issued To I.CA Test Public CA/RSA 11/2015 I.CA Test Root CA/RSA Jan Novák Janb Novák	Issued By I.CA Test Root CA/RSA I.CA Test Root CA/RSA I.CA Test Public CA/RSA 11/2015 I.CA Test Public CA/RSA 11/2015 CEB Business Connector CA CEB Business Connector CA	Expir 27. 1 20. 1 24. 4 24. 4 17. 1 14. 2

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 proveďte 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 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 kontraktech, je nutné ho zablokovat nebo odebrat ze seznamu certifikátů u všech smluv.