COMMERZBANK
Banka po Vašem boku

PODMÍNKY

pro dálkový přenos dat

Obsah

1. Rozsah služeb

(1) Banka svým klientům (majitelům účtů) umožňuje pomocí elektronických prostředků dálkový přenos dat (dále jen „dálkový přenos dat“).

Dálkový přenos dat zahrnuje zadávání a stahování dat (zejména přenos příkazů a stahování informací).

(2) Banka oznámí klientovi typy služeb, které klient může využívat v rámci dálkového přenosu dat. Používání dálkového přenosu dat podléhá limitu pro disponování, který byl sjednán s bankou.

(3) Dálkový přenos dat je možný prostřednictvím rozhraní EBICS (Přílohy 1a až 1c).

(4) Struktura datových záznamů a souborů pro přenos příkazů a stahování informací je popsána ve Specifikaci datových formátů (Příloha 3) nebo bude sjednána zvlášť.

2. Uživatelé a účastníci, identifikační a bezpečnostní média

(1) Příkazy mohou být zadávány prostřednictvím rozhraní EBICS pouze klientem nebo oprávněnými osobami klienta, které mají oprávnění disponovat účtem.

Klient a osoby oprávněné disponovat účtem jsou dále společně označováni jako „uživatelé“. K autorizaci přenosu příkazu pomocí dálkového přenosu dat potřebuje každý uživatel individuální identifikační médium, které musí aktivovat banka.

Požadavky na identifikační média jsou definovány v Příloze 1a.

Pokud tak bude dohodnuto s bankou, příkazy přeposílané dálkovým přenosem dat mohou být autorizovány podepsaným doprovodným dokumentem / hromadným příkazem.

(2) Pro výměnu dat prostřednictvím rozhraní EBICS může klient kromě oprávněných osob jmenovat „technické účastníky“. Musí to být fyzické osoby, které budou oprávněné provádět pouze výměnu dat.

Uživatelé a techničtí účastníci jsou dále společně označováni jako „účastníci“. Za účelem zajištění ochrany výměny dat potřebuje každý účastník individuální bezpečnostní média, která musí banka aktivovat. Požadavky na bezpečnostní média jsou popsány v Příloze 1a.

3. Procedurální ustanovení

(1) Požadavky popsané v Příloze 1a, v dokumentaci k technickému rozhraní (Příloha 1b) a ve Specifikaci datového formátu (Příloha 3) se vztahují na metodu přenosu sjednanou mezi klientem a bankou.

(2) Klient je povinen zajistit, aby všichni účastníci dodržovali postup a specifikace dálkového přenosu dat.

(3) Přiřazení datových polí se řídí pokyny pro vyplnění a kontrolu, které platí pro použitý specifický formát (Příloha 3).

(4) Uživatel uvede identifikační znak příjemce platby, popř. plátce podle příslušných Zvláštních podmínek.

Poskytovatelé platebních služeb zapojení do realizace platebního příkazu jsou oprávnění zpracovat platbu výhradně na základě uvedené identifikace.

Nesprávně uvedené údaje mohou mít za následek nesprávné zpracování příkazu.

Klient uhradí všechny ztráty nebo škody, které v souvislosti s tím vzniknou. Toto ustanovení platí obdobně, pokud jsou dálkovým přenosem dat přeposílány jakékoliv jiné příkazy (jiné než platební).

(5) Před přenosem příkazu do banky musí být kvůli ověření identifikace vyhotoven záznam o plném obsahu souborů, které mají být přeposlány, a o přenášených údajích. Klient musí tento záznam vést po dobu nejméně 30 kalendářních dnů od data vyhotovení uvedeného v záznamu (v případě převodů), popř. od termínu splatnosti (inkaso) nebo v případě více termínů od nejpozdějšího termínu, a to ve formě, aby mohl být takový záznam bance na její žádost neprodleně opakovaně k dispozici, pokud nebude dohodnuto jinak.

(6) Kromě toho musí klient pro každé zadání a každou výměnu dat vygenerovat automatický protokol, jehož obsah bude v souladu s ustanoveními kapitoly 10 Specifikace pro rozhraní EBICS (Příloha 1b), vést protokol o souboru a zpřístupnit ho bance na její žádost.

(7) Pokud banka poskytne klientovi údaje o platebních transakcích, které ještě nejsou v plném rozsahu zpracovány, budou se tyto údaje považovat pouze za nezávaznou informaci. Tyto údaje budou speciálně označeny.

(8) Příkaz předložený prostřednictvím dálkového přenosu dat musí být autorizován buď elektronickým podpisem, nebo podepsaným doprovodným dokumentem / hromadným příkazem podle toho, jak je s bankou dohodnuto.

Tento příkaz bude platný jako příkaz

a) pro data předložená s elektronickým podpisem, pokud

- byly všechny nutné elektronické podpisy uživatelů obdrženy dálkovým přenosem dat ve sjednané době, a
- je možné elektronické podpisy úspěšně prověřit na základě schválených klíčů, nebo

b) pro data předložená s doprovodným dokumentem / hromadným příkazem, pokud

- banka obdrží doprovodný dokument / hromadný příkaz ve sjednané době a
- byl doprovodný dokument / hromadný příkaz podepsán v souladu se zmocněním k účtu.

4. Povinnosti týkající se chování a péče při nakládání s identifikačními médii pro autorizaci příkazů

(1) Na základě postupu přenosu sjednaného s bankou je klient povinen zajistit, aby všichni uživatelé dodržovali identifikační postupy popsané v Příloze 1a.

(2) Uživatel může podat příkazy prostřednictvím identifikačních médií aktivovaných bankou.

Klient je povinen dbát na to, aby každý uživatel zajistil, že žádná třetí strana nezíská do svého vlastnictví identifikační médium uživatele ani nezíská heslo k jeho ochraně, neboť třetí strana, která získala do svého vlastnictví médium nebo jeho příslušný duplikát, by mohla spolu s příslušným heslem zneužít sjednané služby. Za účelem zachování utajení identifikačního média je třeba dodržovat především tato opatření:

- Data identifikující uživatele musí být chráněna před neoprávněným přístupem a musí být zabezpečena.

- Heslo chránící identifikační médium nesmí být zapsáno nebo uchováváno elektronicky nezabezpečené.
- Při zadávání hesla je třeba dbát na to, aby jej žádná jiná osoba nemohla odcizit.

5. Povinnosti týkající se chování a péče při nakládání s bezpečnostními médii pro výměnu dat

V rámci spojení prostřednictvím EBICS je klient povinen zajistit, aby všichni účastníci dodržovali bezpečnostní postupy popsané v Příloze 1a.

Účastník musí zajistit výměnu dat prostřednictvím bezpečnostního média aktivovaného bankou.

Klient je povinen dbát na to, aby každý účastník zajistil, že žádná třetí strana nezíská do svého vlastnictví bezpečnostní médium ani ho nebude používat. Zejména v případě, pokud bude médium uloženo v technickém systému, musí být bezpečnostní médium účastníka uloženo v takovém technickém prostředí, které je chráněno proti neoprávněnému přístupu, neboť třetí strana, která získá přístup k bezpečnostnímu médiu nebo jeho duplikátu, by mohla zneužít výměnu dat.

6. Pozastavení identifikačního a bezpečnostního média

(1) V případě ztráty identifikačního nebo bezpečnostního média, popř. v případě jeho zpřístupnění třetí straně, nebo pokud vznikne podezření, že došlo k zneužití média, musí účastník neprodleně požádat banku, aby pozastavila přístup k dálkovému přenosu dat, popř. aby tento přístup nechala zablokovat. Další podrobnosti jsou uvedeny v Příloze 1a.

Účastník může banku také kdykoliv požádat, aby pozastavila přístup prostřednictvím samostatně sdělených kontaktních údajů.

(2) Kromě pozastavení procesu dálkového přenosu dat může klient požádat o pozastavení identifikačního a bezpečnostního média účastníka nebo o pozastavení celého přístupu k dálkovému přenosu dat prostřednictvím zařízení, které umožňuje pozastavení, sděleného bankou.

(3) Pokud vznikne podezření, že došlo k zneužití média, banka pozastaví celý přístup k dálkovému přenosu dat a bude klienta informovat o pozastavení procesu dálkového přenosu dat mimo proces dálkového přenosu dat.

Toto pozastavení nemůže být zrušeno prostřednictvím dálkového přenosu dat.

7. Nakládání s údaji na došlých příkazech bankou

(1) Údaje příkazu přeposílané do banky dálkovým přenosem dat budou zpracovány v rámci běžného pracovního postupu.

(2) Na základě podpisů vygenerovaných účastníky pomocí bezpečnostního média banka ověří, zda je odesílatel oprávněn provádět výměnu dat.

Pokud budou při tomto ověření zjištěny jakékoliv nesrovnalosti, banka dotčený příkaz nezpracuje a bude o tom klienta neprodleně informovat.

(3) Banka ověří identifikaci uživatele, popř. uživatelů a autorizaci údajů příkazu přeposílaných dálkovým přenosem dat na základě elektronických podpisů vygenerovaných uživateli pomocí identifikačního média nebo na základě poskytnutého doprovodného dokumentu / hromadného příkazu a prověří, zda datové záznamy o údajích příkazu odpovídají ustanovením uvedeným v Příloze 3.

Pokud budou při tomto ověření zjištěny jakékoliv nesrovnalosti, banka dotčený příkaz nezpracuje a bude o tom klienta neprodleně informovat.

Banka může vymazat údaje příkazu, který není plně autorizován, po uplynutí časové lhůty, kterou banka oznámila zvlášť.

(4) Pokud banka během ověření souborů nebo datových záznamů podle Přílohy 3 zjistí chyby, banka tyto chyby v souborech nebo datových záznamech vhodnou formou doloží a bude o tom neprodleně informovat uživatele.

Pokud banka nebude moci zajistit řádné provedení příkazu, je oprávněná vyloučit soubory nebo datové záznamy s chybami z dalšího zpracování.

(5) Banka je povinna zdokumentovat v klientském protokolu výše uvedené postupy (viz Příloha 1a) a odeslání příkazů ke zpracování.

Klient je povinen si neprodleně vyžádat klientský protokol a informace o stavu zpracovaného příkazu. V případě nesrovnalostí je povinen kontaktovat banku.

8. Odvolání příkazu

(1) Před autorizací údajů na příkazu může klient soubor stáhnout zpět. Jednotlivé údaje na příkazu mohou být změněny pouze odvoláním celého souboru a opětovným zadáním příkazu. Banka může akceptovat odvolání pouze tehdy, pokud bude doručeno včas, aby bylo možné ho zohlednit v rámci běžného pracovního procesu.

(2) Rozsah, v jakém může být příkaz odvolán, se řídí platnými zvláštními podmínkami (např. Podmínky pro poskytování platebních služeb).

Příkaz může být odvolán mimo proces dálkového přenosu dat nebo podle ustanovení uvedených v kapitole 11 příloha 3, pokud tak bylo dohodnuto s klientem. Klient musí v tomto případě informovat banku o jednotlivých podrobnostech uvedených v původním příkaze.

9. Provedení příkazů

(1) Banka provede příkazy, pokud budou dodrženy, popř. budou splněny veškeré níže uvedené požadavky na provedení příkazu:

- údaje na příkazu podaném dálkovým přenosem dat musí být schváleny v souladu s bodem 3 odstavec 8,
- musí souhlasit definovaný formát dat,
- nesmí být překročen limit pro nakládání s příkazem,
- požadavky na provedení musí být splněny v souladu se zvláštními podmínkami platnými pro příslušný typ příkazu a
- provedení příkazu nesmí porušit žádné jiné právní předpisy.

(2) Jestliže nebudou splněny podmínky pro provedení příkazu podle odstavce 1, banka neprovede příkaz a bude klienta dohodnutým způsobem neprodleně informovat, že příkaz nebyl proveden. Jestliže to bude možné, oznámí banka klientovi důvody a chyby, které způsobily neprovedení příkazu, a možné nápravy těchto chyb. To neplatí, pokud by uvedením důvodů byly porušeny jiné právní předpisy.

10. Bezpečnost klientského systému

Klient je povinen zabezpečit dostatečnou ochranu jím používaných systémů pro dálkový přenos dat. Požadavky na zabezpečení, které platí pro postup EBICS, jsou popsány v Příloze 1c.

11. Odpovědnost

11.1 Odpovědnost banky v případě neautorizovaných příkazů a příkazů neprovedených, provedených nesprávně nebo provedených opožděně
Odpovědnost banky v případě neautorizovaných příkazů a příkazů neprovedených, provedených nesprávně nebo provedených opožděně je upravena ve zvláštních podmínkách sjednaných pro příslušný typ příkazů (např. Podmínky pro poskytování platebních služeb).

11.2 Odpovědnost klienta v případě zneužití identifikačního nebo bezpečnostního média

11.2.1 Odpovědnost klienta v případě neautorizovaných platebních transakcí před žádostí o zablokování

(1) Odpovědnost klienta, který není spotřebitelem. Pokud je neautorizovaná platební transakce před žádostí o zablokování založena na zneužití identifikačního nebo bezpečnostního média, bude klient odpovědný za ztráty následně utrpěné bankou, pokud účastník jednal z nedbalosti nebo z úmyslu, a porušil tím povinnosti týkající se chování a péče.

11.2.2 Odpovědnost klienta v případě jiných neautorizovaných transakcí před žádostí o zablokování

Pokud je neautorizovaná transakce, která není platební transakcí, před žádostí o zablokování založena na použití ztraceného nebo odcizeného identifikačního nebo bezpečnostního média nebo na jiné formě zneužití identifikačního nebo bezpečnostního média, a jestliže bance tím vznikla škoda, nahradí klient a banka škodu podle míry spoluzavinění stanovené zákonem.

11.2.3 Odpovědnost banky po žádosti o zablokování

Poté, co banka obdržela od účastníka žádost o zablokování, nese odpovědnost za veškeré škody způsobené v důsledku neautorizovaných transakcí. To neplatí, pokud účastník jednal s úmyslem podvodu.

11.3 Vyloučení odpovědnosti
Nároky vyplývající z odpovědnosti jsou vyloučeny, jestliže okolnosti zakládající nárok vycházejí z neobvyklé nebo nepředvídatelné události, na kterou strana, která se dovolává této události, nemá vliv a jejímž důsledkům nebylo možné zabránit i přes vynaložení řádné péče.

12. Závěrečná ustanovení

Přílohy uvedené v těchto podmínkách jsou součástí smlouvy uzavřené s klientem.

Přílohy:

Příloha 1a: Rozhraní EBICS

Příloha 1b: Specifikace pro rozhraní EBICS

Příloha 1c: Bezpečnostní požadavky pro klientský systém EBICS

Příloha 2: V současnosti se nepoužívá

Příloha 3: Specifikace datového formátu

Příloha 1a: Rozhraní EBICS

1. Identifikační a bezpečnostní postupy

Klient (majitel účtu) oznámí úvěrové instituci účastníky a jejich oprávnění týkající se dálkového přenosu dat.

Pro rozhraní EBICS se používají následující identifikační a bezpečnostní postupy:

- elektronické podpisy,
- ověřovací podpis,
- šifrování.

Pro každý identifikační a bezpečnostní proces má účastník k dispozici individuální soubor klíčů, který se skládá ze soukromého a veřejného klíče. Veřejné účastnické klíče mohou být oznámeny úvěrové instituci v souladu s postupem popsaným v článku 2.

Veřejné klíče banky musí být chráněny před neoprávněnou změnou v souladu s postupem popsaným v článku 2. Soubor účastnických klíčů lze rovněž použít pro komunikaci s jinými úvěrovými institucemi.

1.1 Elektronické podpisy

1.1.1 Elektronické podpisy účastníků

Pro elektronické podpisy (EP) účastníků jsou definovány tyto podpisové třídy:

- podpis samostatně (typ „E"),
- první podpis (typ „A"),
- druhý podpis (typ „B"),
- transportní podpis (typ „T").

Typickými elektronickými podpisy pro použití v bankovnictví jsou elektronické podpisy typu „E", „A" nebo „B". Bankovní elektronické podpisy se používají pro autorizaci příkazů. Příkazy mohou vyžadovat několik bankovních elektronických podpisů různých uživatelů (majitelů účtů a osob oprávněných disponovat účtem). Pro každý podporovaný typ příkazu sjednají úvěrová instituce a klient minimální počet potřebných bankovních elektronických podpisů.

Elektronické podpisy typu „T" jsou označeny jako transportní podpisy a nemohou být použity k autorizaci příkazů, ale pouze pro přeposlání příkazů do bankovního systému. „Technickým účastníkům" (viz článek 2.2) může být přidělen pouze elektronický podpis typu „T".

Program používaný klientem může generovat různé zprávy (například tuzemské nebo zahraniční platební příkazy, ale také zprávy týkající se inicializace, stažení protokolu a vyvolání informací o účtu a obratu). Úvěrová instituce informuje klienta o tom, jaký typ zprávy může použít a který typ elektronického podpisu musí být ve specifickém případě použit.

1.2 Ověřovací podpisy

Na rozdíl od elektronického podpisu, který se používá k podpisu příkazu, se ověřovací podpis používá pro jednotlivé zprávy EBICS a je konfigurován prostřednictvím kontrolních a přihlašovacích údajů a elektronických podpisů v nich obsažených. S výjimkou několika typů příkazů týkajících se systému, které jsou definovány ve specifikaci pro rozhraní EBICS, musí ověřovací podpisy poskytovat jak systém klienta, tak bankovní systém, a to v každém kroku transakce. Klient musí zajistit, aby se používal software, který v souladu se specifikací pro rozhraní EBICS (viz Příloha 1b) ověřuje ověřovací podpisy každé zprávy EBICS přeposílané úvěrovou institucí, která bere v úvahu aktuální platnost a pravost uložených veřejných klíčů úvěrové instituce.

1.3 Šifrování

K zajištění důvěrného charakteru bankovních údajů na úrovni aplikace musí klient příkaz zašifrovat v souladu se specifikací pro rozhraní EBICS (viz Příloha 1b). Klient musí vzít také v úvahu aktuální platnost a pravost uložených veřejných klíčů úvěrové instituce. Navíc se musí pro externí přenosové cesty mezi systémy klienta a banky používat transportní šifrování. Klient musí zajistit používání softwaru, který v souladu se specifikací pro rozhraní EBICS (viz Příloha 1b) ověří aktuální platnost a pravost certifikátů pro server používaný úvěrovou institucí.

2. Inicializace rozhraní EBICS

2.1 Instalace komunikačního rozhraní

Komunikace se inicializuje využitím URL (Uniform Resource Locator – jednotná adresa zdroje). Alternativně je možné pro příslušnou úvěrovou instituci použít IP adresu. URL a IP adresa budou klientovi sděleny při uzavření smlouvy s úvěrovou institucí. Za účelem zahájení inicializace rozhraní EBICS oznámí úvěrová instituce účastníkům jmenovaným klientem tyto údaje:

- URL nebo IP adresa úvěrové instituce,
- název úvěrové instituce,
- hostitelské ID,
- povolená verze (povolené verze) protokolu EBICS a bezpečnostních postupů,
- partnerské ID (ID klienta),
- uživatelské ID,
- systémové ID (pro technické účastníky),
- další specifické podrobnosti o autorizaci klienta a účastníka.

Účastníkům přiřazeným klientovi úvěrová instituce přiřadí jedno uživatelské ID, které účastníka jasně identifikuje. Vzhledem k tomu, že klientovi je přiřazen jeden nebo více technických účastníků (systém více uživatelů), přiřadí úvěrová instituce kromě uživatelského ID také systémové ID. Pokud není definován žádný technický účastník, budou systémové ID a uživatelské ID stejné.

2.2 Inicializace klíčů

2.2.1 První inicializace klíčů účastníka

Kromě obecných podmínek popsaných v článku 1 musí soubor klíčů používaný účastníkem pro bankovní elektronické podpisy, šifrování údajů příkazu a ověřovací podpis odpovídat níže uvedeným požadavkům:

(1.) Soubor klíčů musí být přiřazen výlučně a jednoznačně účastníkovi.

(2.) Pokud si účastník generuje klíče sám, musí být privátní klíče generovány způsobem, který je výhradně pod kontrolou účastníka.

(3.) Pokud jsou klíče zpřístupněny třetí stranou, musí být zajištěno, že je účastník jediným příjemcem privátních klíčů.

(4.) Pokud jde o privátní klíče používané pro identifikaci, každý uživatel musí stanovit pro každý klíč heslo, které bude chránit přístup k příslušnému privátnímu klíči.

(5.) Pokud jde o privátní klíče používané k ochraně výměny dat, každý účastník musí stanovit heslo pro každý klíč, které chrání přístup k příslušnému privátnímu klíči. Na použití tohoto hesla se nemusí trvat, pokud je bezpečnostní médium účastníka uloženo v technickém prostředí, které je chráněno proti neoprávněnému přístupu.

K inicializaci účastníka úvěrovou institucí je nutný přenos veřejných účastnických klíčů do bankovního systému. Za tímto účelem přepošle účastník své veřejné klíče do úvěrové instituce prostřednictvím dvou nezávislých komunikačních kanálů:

- prostřednictvím rozhraní EBICS pomocí typů příkazu poskytnutých systémem pro tento postup a
- prostřednictvím inicializačního dopisu podepsaného majitelem účtu nebo osobou oprávněnou disponovat účtem.

K inicializaci účastníka ověří úvěrová instituce pravost veřejných účastnických klíčů přeposlaných prostřednictvím EBICS na základě inicializačních dopisů podepsaných majitelem účtu nebo osobou oprávněnou disponovat účtem.

Inicializační dopis musí pro každý veřejný účastnický klíč obsahovat níže uvedené údaje:

- účel veřejného účastnického klíče,
- elektronický podpis,
- ověřovací podpis,
- šifrování,
- příslušná verze pro každý soubor klíčů,
- specifikace délky exponentu,
- hexadecimální zápis exponentu veřejného klíče,
- specifikace délky modulu,
- hexadecimální zápis modulu veřejného klíče,
- hexadecimální zápis hodnoty transformace veřejného klíče.

Úvěrová instituce ověří podpis majitele účtu nebo osoby oprávněné disponovat účtem v inicializačním dopise a také zda jsou hodnoty transformace veřejného účastnického klíče přenášené prostřednictvím EBICS shodné s hodnotami přeposílanými písemně. Pokud je ověření kladné, úvěrová instituce bude aktivovat příslušného účastníka pro sjednané typy příkazů.

2.3 Inicializace bankovních klíčů
Účastník si stáhne veřejný klíč úvěrové instituce s typem příkazu, který systém pro tento účel speciálně poskytuje. Hodnota transformace veřejného bankovního klíče bude úvěrovou institucí dodatečně zpřístupněna prostřednictvím druhého komunikačního kanálu samostatně sjednaného s klientem. Před prvním přenosem dat prostřednictvím EBICS účastník ověří pravost veřejných bankovních klíčů zaslaných dálkovým přenosem dat tak, že srovná jejich hodnoty transformace s hodnotami transformace sdělenými úvěrovou institucí prostřednictvím samostatně sjednaného komunikačního kanálu. Klient zajistí, aby byl používán software, který ověřuje platnost certifikátů serveru používaného v souvislosti s transportním šifrováním prostřednictvím certifikační cesty samostatně sdělené úvěrovou institucí.

3. Zadávání příkazů u banky

Uživatel ověří správnost údajů příkazu a zajistí, aby byly elektronicky podepsány pouze ověřené údaje. Po inicializaci komunikace banka nejprve ověří oprávnění týkající se účastníka, jako je autorizace typu příkazu nebo ověření možných dohodnutých limitů. Výsledky dalších bankovních ověření, jako je ověření limitu nebo ověření autorizace k disponování účtem budou sděleny klientovi později v protokolu klienta. Příkazy přenášené do bankovního systému mohou být schváleny takto:

(1.) Veškeré nutné bankovní elektronické podpisy jsou přenášeny spolu s údaji na příkazu.

(2.) Pokud byl s klientem sjednán distribuovaný elektronický podpis pro příslušný typ příkazu a přeposílané elektronické podpisy nejsou k bankovnímu schválení dostatečné, příkaz se uloží v bankovním systému, dokud nebudou použity všechny požadované elektronické podpisy.

(3.) Pokud se klient a banka dohodnou, že údaje na příkazu předané prostřednictvím dálkového přenosu dat a příkazy mohou být schváleny prostřednictvím samostatně přenášeného doprovodného dokumentu/hromadného

příkazu, musí být pro technickou ochranu údajů na příkaze doplněn místo bankovního elektronického podpisu uživatele transportní podpis (typ „T“). Za tímto účelem musí soubor obsahovat speciální kód označující, že pro tento příkaz neexistují žádné další elektronické podpisy kromě transportního podpisu (typ „T“). Příkaz bude schválen poté, co úvěrová instituce úspěšně potvrdí podpis uživatele na doprovodném dokumentu/hromadném příkazu.

3.1 Zadání příkazů prostřednictvím distribuovaného elektronického podpisu
Způsob, jakým klient použije distribuovaný elektronický podpis, se sjedná s úvěrovou institucí. Distribuovaný elektronický podpis se použije tam, kde mají být příkazy schváleny nezávisle na přenášení údajů příkazu, a to, pokud je to možné, několika účastníky. Dokud nebudou použity veškeré bankovní elektronické podpisy nutné k autorizaci, může být příkaz oprávněným uživatelem vymazán. Pokud byl příkaz již plně autorizován, je možné podle článku 8 Podmínek pro dálkový přenos dat příkaz pouze odvolat. Banka může příkazy, které nebyly plně schváleny, vymazat po uplynutí časového limitu samostatně sděleného bankou.

3.2 Ověření identifikace bankou
Došlý příkaz banka provede pouze poté, co obdrží a kladně ověří nutný bankovní elektronický podpis nebo podepsaný doprovodný dokument/hromadný příkaz.

3.3 Protokol klienta
Banka v protokolech klienta zdokumentuje následující transakce:

- přenos údajů příkazu do bankovního systému,
- přenos informačních souborů z bankovního systému do systému klienta,
- výsledek všech ověření identifikace pro příkazy od klienta do bankovního systému,
- další zpracování příkazů, pokud se týkají ověření podpisů a zobrazení údajů na příkazu. Účastník je povinen brát na vědomí informace o výsledku ověření provedených úvěrovou institucí okamžitým stažením protokolu klienta. Účastník zahrne tento protokol, jehož obsah odpovídá ustanovením článku 10 Přílohy 1b, do svých souborů a předloží jej úvěrové instituci na její žádost.

4. Změna účastnického klíče s automatickou aktivací

Pokud je období platnosti identifikačního a bezpečnostního média používaného účastníkem omezeno, musí účastník do banky odeslat nové veřejné klíče včas před datem vypršení platnosti tohoto období. Po datu vypršení platnosti starých klíčů musí být provedena nová inicializace. Pokud si účastník generuje klíče sám, musí být účastnické klíče obnoveny s použitím typů příkazů poskytnutých pro tento účel systémem v den sjednaný s úvěrovou institucí. Klíče musí být přeposlány včas před datem vypršení platnosti starých klíčů. Pro automatickou aktivaci nových klíčů bez obnovené inicializace účastníka se použijí následující typy příkazů:

- aktualizace veřejného bankovního klíče (PUB),
- aktualizace veřejného ověřovacího klíče a veřejného šifrovacího klíče (HCA),
- aktualizace všech tří výše uvedených klíčů (HCS).

Uživatel může poskytnout platný bankovní elektronický podpis pro typy příkazu PUB, HCA a HCS. Po úspěšné změně klíčů mohou být používány pouze klíče nové. Pokud nebylo možné elektronický podpis pozitivně ověřit, použijí se ustanovení uvedená v článku 7 odstavec 3 Podmínek pro dálkový přenos dat. Klíče mohou být změněny pouze poté, co budou zpracovány všechny příkazy. Jinak budou muset být příkazy, které ještě nebyly zpracovány, zadány znovu s použitím nového klíče.

5. Pozastavení účastnických klíčů

Pokud bude existovat podezření ze zneužití účastnických klíčů, musí účastník pozastavit přístupové oprávnění ke všem bankovním systémům, které kompromitovaný klíč (kompromitované klíče) používají. Pokud účastník vlastní platná identifikační a bezpečnostní média, může pozastavit přístupové oprávnění prostřednictvím rozhraní EBICS. Pokud se odesílá zpráva s příkazem typu „SPR“, přístup bude pozastaven pro příslušného účastníka, jehož uživatelské ID bylo pro odeslání zprávy použito. Po pozastavení nemůže účastník zadávat žádné další příkazy prostřednictvím rozhraní EBICS, a to až do doby, než bude přístup opět inicializován, jak je popsáno v článku 2. Pokud již účastník platná identifikační a bezpečnostní média nevlastní, může požádat o pozastavení identifikačního a bezpečnostního média mimo postup dálkového přenosu dat prostřednictvím zařízení pro pozastavení, které mu sdělí banka. Mimo proces dálkového přenosu dat může klient požádat o pozastavení identifikačního nebo bezpečnostního média účastníka nebo o pozastavení úplného přístupu k dálkovému přenosu dat prostřednictvím zařízení pro pozastavení sděleného bankou.

COMMERZBANK
Banka po Vašem boku

Příloha 1b: Specifikace pro rozhraní EBICS

Specifikace je zveřejněna na internetových stránkách: http://www.ebics.com

Příloha 1c: Bezpečnostní požadavky na klientský systém EBICS

Kromě bezpečnostních opatření popsaných v Příloze 1a, článek 5, je klient povinen dodržovat tyto požadavky:

- Software používaný klientem pro postup EBICS musí odpovídat požadavkům popsaným v Příloze 1a.
- Klientský systém EBICS nesmí být používán bez firewallu. Firewall je aplikace, která monitoruje všechny přicházející a odcházející zprávy a povoluje pouze známá nebo autorizovaná spojení.
- Musí být nainstalován antivirový program, který bude pravidelně aktualizován a bude obsahovat soubory s nejnovějšími definicemi virů.
- Klientský systém EBICS musí být nastaven tak, aby se účastník musel přihlásit před jeho použitím jako běžný Uživatel, a nikoliv jako administrátor, který je například oprávněný provádět programové instalace.
- Interní komunikační IT kanály pro nešifrované bankovní údaje nebo pro nešifrované zprávy EBICS musí být chráněny proti zachycení a manipulaci.
- Jestliže jsou k dispozici důležité bezpečnostní aktualizace pro aktuálně používaný operační systém nebo pro jiné nainstalované softwarové programy související se zabezpečením, musí být tyto aktualizace použity v klientských systémech EBICS.

Odpovědnost za splnění těchto požadavků nese výhradně klient.

Příloha 2:

V současné době se nepoužívá.

Příloha 3: Specifikace datového formátu

Specifikace je zveřejněna na internetových stránkách: http://www.ebics.com.

Vaše pobočka Commerzbank:

Commerzbank Aktiengesellschaft

pobočka Praha
Jugoslávská 934/1, Vinohrady
120 00 Praha 2

Telefon: +420 221 193 111
Fax: +420 221 193 699

www.commerzbank.cz