COMMERZBANK
Banka po Vašom boku

PODMIENKY

pre dialkový prenos dát

Obsah

1. Rozsah služieb

(1) Banka je svojmu klientovi (majiteľovi účtu) k dispozícii na diaľkový prenos dát elektronickou cestou, ďalej ako „diaľkový prenos dát“. Diaľkový prenos dát zahŕňa predkladanie a odvolávanie súborov (predovšetkým zasielanie príkazov a odvolávanie informácií).

(2) Banka oznámi klientovi druhy služieb, ktoré môže tento v rámci diaľkového prenosu dát využívať. Pre využívanie diaľkového prenosu dát platia dostupné limity dohodnuté s bankou.

(3) Diaľkový prenos dát je možný prostredníctvom napojenia na EBICS (príloha 1a až 1c).

(4) Štruktúra viet a súborov na zasielanie príkazov a vyvolávanie informácií je dohodnutá v špecifikácii dátových formátov (príloha č. 3) alebo bude dohodnutá osobitne.

2. Užívatelia a účastníci, autorizačné a zabezpečovacie médiá

(1) Príkazy podáva prostredníctvom napojenia na EBICS klient alebo jeho zástupca splnomocnený na disponovanie účtom. Klienti a osoby splnomocnené na disponovanie účtom sa jednotne označujú ako „užívatelia“. Na autorizáciu dát z príkazov zaslaných formou diaľkového prenosu dát užívateľ využíva individuálne a bankou aktivované autorizačné médiá. Požiadavky na autorizačné médiá sú definované v prílohe č. 1. Ak je to dohodnuté s bankou, môžu byť dáta z príkazov zaslaných formou diaľkového prenosu dát autorizované na základe podpísaného sprievodného lístka/hromadného príkazu.

(2) Za účelom výmeny dát prostredníctvom napojenia na EBICS môže klient okrem splnomocnených osôb vymenovať aj „technických účastníkov“, ktorí musia byť fyzické osoby a ktorí budú oprávnení na výmenu dát. Užívatelia a technickí účastníci sú ďalej označovaní ako „účastníci“. Na zabezpečenie výmeny dát potrebuje každý účastník individuálne a bankou aktivované zabezpečovacie médiá. Požiadavky na zabezpečovacie médiá sú definované v prílohe č. 1a.

3. Ustanovenia o postupe

(1) Pre postup prenosu dohodnutý medzi klientom a bankou platia požiadavky uvedené v prílohe č. 1a ako aj v dokumentácii technického rozhrania (Príloha č. 1b) a špecifikácii formátu dát (Príloha č. 3).

(2) Klient musí zabezpečiť, aby všetci účastníci dodržiavali postup pre diaľkový prenos dát a špecifikácie.

(3) Obsadzovanie dátových polí sa riadi podľa smerníc pre obsadzovanie a kontrolu platných pre príslušný formát (Príloha č. 3).

(4) Užívateľ je povinný uvádzať identifikačné údaje klienta príjemcu platby príp. platiteľa podľa príslušných osobitných podmienok. Poskytovatelia platobných služieb zapojení do vykonávania platobných príkazov sú oprávnení vykonávať spracovávanie výhradne podľa identifikačných údajov klientov. Chybné údaje môžu viesť k chybnému prenosu údajov o príkaze. Za škody a nedostatky, ktoré v dôsledku toho vzniknú, zodpovedá klient. Úprava platí primerane, ak sa formou diaľkového prenosu dát zasielajú iné príkazy (iné než platobné príkazy).

(5) Pred prenosom údajov o príkaze do banky musí byť vyhotovený súpis prenášaných súborov spolu s ich úplným obsahom ako aj súpis dát prenesených za účelom autorizácie. Tento súpis musí mať klient k dispozícii po dobu najmenej 30 kalendárnych dní odo dňa vykonania (pri prevodoch) príp. odo dňa splatnosti (pri inkasách) uvedeného v súbore alebo v prípade viacerých termínov od neskoršieho termínu, a to v takej forme, aby bolo možné súbor na žiadosť banky krátkodobo opakovane poskytnúť k dispozícii, ak nebude dohodnuté inak.

(6) Okrem toho musí za každé podanie a vyvolanie súborov vyhotoviť strojový protokol, ktorý obsahovo zodpovedá ustanoveniam kapitoly 10 Špecifikácie pre napojenie na EBICS (Príloha č. 1b), uložiť ho medzi svoje spisy a na požiadanie predložiť banke.

(7) Ak banka poskytuje klientovi údaje o platobných postupoch, ktoré neboli definitívne spracované, predstavujú len nezáväzné informácie. Tieto údaje sú osobitne označené.

(8) Dáta z príkazov doručené formou diaľkového prenosu dát musia byť podľa dohody s bankou autorizované prostredníctvom elektronického podpisu alebo podpísaného sprievodného lístka / hromadného príkazu. Tieto dáta z príkazov sú účinné ak príkaz

a) pri doručení s elektronickým podpisom, ak

- boli počas dohodnutej lehoty doručené všetky nevyhnutné elektronické podpisy užívateľov formou diaľkového prenosu dát a
- elektronické podpisy bolo možné úspešne prekontrolovať pomocou dohodnutých kľúčov, alebo

b) pri doručení sprievodného lístka / hromadného príkazu, ak

- sprievodný lístok / hromadný príkaz bol do banky doručený v dohodnutej lehote a
- sprievodný lístok / hromadný príkaz bol podpísaný podľa splnomocnenia k účtu.

4. Povinnosti spočívajúce v správaní a starostlivom zaobchádzaní s médiami na autorizáciu príkazu

(1) Klient je v závislosti od postupov prenosu dohodnutých s bankou povinný zabezpečiť, aby všetci užívatelia dodržiavali autorizačné postupy popísané v Prílohe č. 1a.

(2) Pomocou autorizačných médií aktivovaných bankou môže užívateľ zadávať príkazy. Klient zabezpečí, aby sa každý užívateľ postaral o to, aby sa autorizačné médium nedostalo do rúk inej osoby alebo aby sa iné osoby nedozvedeli heslo slúžiace na jeho ochranu. Každá iná osoba, ktorá získa do svojej držby médium alebo jeho duplikát, môže v spojení s príslušným heslom zneužiť dohodnuté služby. Za účelom utajenia autorizačných médií je potrebné dodržiavať nasledovné podmienky:

- Dáta, ktoré autorizujú užívateľa, musia byť chránené pred neoprávneným prístupom a musia byť bezpečne uchovávané
- Heslo slúžiace na ochranu autorizačného média nesmie byť zaznamenané ani elektronicky uložené bez zabezpečenia.
- Pri zadávaní hesla je potrebné zabezpečiť, aby ho iné osoby nemohli vypátrať.

5. Povinnosti spočívajúce v správaní a starostlivom zaobchádzaní so zabezpečovacími médiami na výmenu dát

Klient je v rámci napojenia na EBICS povinný zabezpečiť, aby všetci užívatelia dodržiavali zabezpečovacie postupy popísané v Prílohe č. 1a. Pomocou zabezpečovacích médií aktivovaných bankou môže užívateľ zabezpečovať výmenu dát. Klient je povinný zabezpečiť, aby sa každý užívateľ postaral o to, aby sa zabezpečovacie médium nedostalo do rúk inej osoby alebo aby ho iné osoby používali. Najmä v prípade uloženia v technickom systéme musí byť zabezpečovacie médium účastníka uložené v takom technickom prostredí, ktoré je chránené pred neoprávneným prístupom. Každá iná osoba, ktorá získa do svojej držby zabezpečovacie médium alebo jeho duplikát, môže zneužiť výmenu dát.

6. Zablokovanie autorizačných a zabezpečovacích médií

(1) Ak sa autorizačné alebo zabezpečovacie médiá stratia, ak sa o nich dozvedia iné osoby alebo ak existuje podozrenia z ich zneužitia, musí účastník bezodkladne zablokovať svoj prístup k diaľkovému prenosu dát v banke alebo zabezpečiť jeho zablokovanie. Bližšie údaje sú uvedené v Prílohe č. 1a. Účastník môže banke kedykoľvek doručiť oznámenie o zablokovaní aj prostredníctvom osobitne oznámených kontaktných údajov.

(2) Klient môže mimo postupu pre diaľkový prenos dát zabezpečiť zablokovanie používania autorizačných a zabezpečovacích médií účastníka alebo celý prístup k diaľkovému prenosu dát prostredníctvom funkcie na zablokovanie, ktorú poskytla banka.

(3) Banka zablokuje celý diaľkový prenos dát, ak existuje podozrenie zo zneužitia diaľkového prenosu dát. Banka bude o tom klienta informovať mimo postupu pre diaľkový prenos dát. Toto zablokovanie nie je možné zrušiť prostredníctvom diaľkového prenosu dát.

7. Spracovanie prichádzajúcich dát z príkazov zo strany banky

(1) Dáta z príkazov doručené banke prostredníctvom postupu pre diaľkový prenos dát sa spracovávajú v rámci bežného pracovného režimu.

(2) Banka na základe podpisov vyhotovených účastníkmi pomocou zabezpečovacích médií skontroluje, či je odosielateľ oprávnený vykonať výmenu dát. Ak z tejto kontroly vyplynú nezrovnalosti, banka príslušný príkaz nespracuje a bezodkladne doručí klientovi príslušnú informáciu.

(3) Banka skontroluje autorizáciu užívateľa príp. užívateľov a autorizáciu dát z príkazov zaslaných formou diaľkového prenosu dát na základe elektronických podpisov vyhotovených užívateľmi pomocou autorizačných médií alebo podľa zaslaného sprievodného lístka/hromadného príkazu ako aj súlad dátových viet z príkazu s ustanoveniami podľa Prílohy č. 3. Ak z tejto kontroly vyplynú nezrovnalosti, banka príslušný príkaz nespracuje a bezodkladne doručí klientovi príslušnú informáciu. Banka je oprávnená po uplynutí osobitne oznámeného časového limitu vymazať neúplne autorizované dáta z príkazov.

(4) Ak banka počas kontrol súborov alebo dátových viet podľa Prílohy č. 3 zistí chyby, banka vhodným spôsobom preukáže chybné súbory alebo dátové vety a bude o nich bezodkladne informovať užívateľa. Banka je oprávnená vylúčiť chybné súbory alebo dátové vety z ďalšieho spracovania, ak nie je možné zabezpečiť riadne vykonanie príkazu.

(5) Banka je povinná zadokumentovať vyššie uvedené postupy (viď Prílohu č. 1a) a odoslanie príkazov na spracovanie v klientskom spise. Klient je povinný pravidelne nahliadať do svojho spisu a informovať sa o stave spracovania príkazu. V prípade nezrovnalostí sa má spojiť s bankou.

8. Odvolanie

(1) Pred autorizáciou dát z príkazu môže klient stornovať súbor. Zmeny jednotlivých údajov z príkazov sú možné len na základe stornovania celého súboru a jeho opätovného predloženia. Banka môže rešpektovať stornovanie len vtedy, ak jej bude oznámené včas natoľko, aby ho banka mohla zohľadniť v rámci riadneho pracovného postupu.

(2) Možnosť odvolania príkazu sa riadi podľa platných osobitných podmienok (napr. podmienky pre platobné služby). Odvolanie príkazu je možné mimo diaľkového prenosu dát, ak bolo dohodnuté s klientom, podľa ustanovení kapitoly 11 Prílohy č. 3. Za týmto účelom musí klient banke oznámiť podrobnosti pôvodného príkazu.

9. Vykonanie príkazov

(1) Banka vykoná príkazy, ak boli splnené všetky nižšie uvedené podmienky pre ich vykonanie:

- dáta z príkazov predložené formou diaľkového prenosu dát boli autorizované podľa bodu 3 ods. 8
- stanovený formát dát bol dodržaný
- dostupný limit nebol presiahnutý
- boli splnené podmienky pre vykonanie príkazov podľa osobitných podmienok platných pre príslušný typ príkazu
- vykonanie príkazu nesmie odporovať ostatným právnym predpisom

(2) Jestliž(2) Ak neboli podmienky pre vykonanie príkazov podľa odseku 1 splnené, banka príkaz nevykoná a bude o tom bezodkladne informovať klienta dohodnutým spôsobom. Ak je to možné, oznámi banka klientovi dôvody a chyby, ktoré viedli k nevykonaniu, ako aj oznámi možnosti na opravu týchto chýb. To neplatí, ak uvedenie dôvodov odporuje ostatným právnym predpisom.

10. Bezpečnosť systému klienta

Klient je povinný zabezpečiť dostatočnú ochranu systémov, ktoré používa na diaľkový prenos dát. Bezpečnostné požiadavky platné pre postup EBICS sú popísané v Prílohe č. 1c.

11. Zodpovednosť

11.1 Ručenie banky v prípade neautorizovaného pokynu na diaľkový prenos dát a nevykonaného, chybne alebo oneskorene vykonaného pokynu na diaľkový prenos dát

Ručenie banky v prípade neautorizovaného pokynu na diaľkový prenos dát a nevykonaného, chybne alebo oneskorene vykonaného pokynu na diaľkový prenos dát sa riadi podľa osobitných podmienok (napr. podmienky pre platobné služby).

11.2 Ručenie klienta v prípade zneužitia autorizačných alebo zabezpečovacích médií

11.2.1 Ručenie klienta za neautorizované platobné postupy pred oznámením zablokovania

(1) Ručenie klienta – nespotrebiteľa
Ak pred oznámením o zablokovaní dôjde k neautorizovaným platbám na základe zneužitia autorizačných alebo zabezpečovacích médií, ručí klient voči banke za škodu, ktorá jej tým vznikla, ak účastník nedbanlivo alebo úmyselne porušil svoje povinnosti spočívajúce v správaní

a starostlivom zaobchádzaní. Ustanovenia § 675v Občianskeho zákonníka sa neuplatňujú.

(2) Ručenie klienta – spotrebiteľa

a) V prípadoch, v ktorých sú neautorizované platby pred oznámením o zablokovaní založené na použití strateného, odcudzeného alebo inak zmiznutého autorizačného alebo zabezpečovacieho média, ručí klient za banke vzniknutú škodu do čiastky 50 Eur, bez ohľadu na to, či je účastník vinný za stratu, odcudzenie a iné alebo za iné zneužitie autorizačného alebo zabezpečovacieho média.

b) Klient nie je povinný nahradiť škodu podľa ods. (2) a), ak

- nemal možnosť všimnúť si stratu, odcudzenie a pod. alebo iné zneužitie autorizačného alebo zabezpečovacieho média, alebo
- ak stratu autorizačného alebo zabezpečovacieho média spôsobil zamestnanec, agent, pobočka poskytovateľa platobných služieb alebo iný subjekt, na ktorý boli činnosti poskytovateľa platobných služieb vyčlenené.

c) Ak pred oznámením o zablokovaní dôjde k neautorizovaných platbám a ak účastník konal s podvodným úmyslom alebo úmyselne alebo hrubo nedbanlivo porušil svoje povinnosti spočívajúce v správaní a starostlivom zaobchádzaní, ručí klient v plnom rozsahu za takto spôsobenú škodu. O hrubú nedbanlivosť účastníka ide predovšetkým vtedy, ak

- si stratu, odcudzenie a pod. alebo iné zneužitie autorizačného alebo zabezpečovacieho média účastník neoznámi banke neodkladne potom, ako sa o tom dozvie (viď bod 6 odsek (1)),
- údaje na jeho autorizáciu nie sú chránené pred neoprávneným prístupom a nie sú bezpečne uchovávané,
- heslo slúžiace na ochranu autorizačného média bolo zaznamenané alebo elektronicky uložené bez zabezpečenia.

(3) Ručenie za škody, ktoré budú spôsobené počas obdobia, pre ktoré platí dostupný limit, je obmedzené na príslušný dohodnutý dostupný limit.

(4) Klient nie povinný nahradiť škodu podľa odsekov 1 a (2) a) a c), ak účastník nemohol podať hlásenie o zablokovaní podľa bodu 6 ods. (1), nakoľko banka neumožnila prijatie hlásenia o zablokovaní.

(5) Odseky (2) b), (3) a (4) sa neuplatňujú, ak účastník konal s podvodným úmyslom.

11.2.2 Ručenie klienta pri iných neautorizovaných postupoch pred oznámením zablokovania

Ak neautorizované postupy, ktoré nie sú platobnými operáciami, pred oznámením zablokovania spočívajú v použití strateného alebo odcudzeného autorizačného alebo zabezpečovacieho média alebo v zneužití autorizačného alebo zabezpečovacieho média a ak v dôsledku toho vznikla banke škoda, ručí klient a banka podľa zákonných ustanovení o spoluzavinení.

11.2.3 Ručenie banky od oznámenia zablokovania

Od momentu, v ktorom banka dostala oznámenie účastníka o zablokovaní, preberá všetky škody, ktoré následne vzniknú v dôsledku neautorizovaných príkazov. To neplatí, ak účastník konal s podvodným úmyslom.

11.3 Vylúčenie ručenia
Nároky z ručenia sú vylúčené, ak okolnosti odôvodňujúce nárok sú založené na nezvyčajnej a nepredvídateľnej udalosti, ktorú nemohla strana odvolávajúca sa na udalosť nijako ovplyvniť, a ktorej dôsledkom nemohla napriek uplatneniu starostlivého prístupu zabrániť.

12. Záverečné ustanovenia

Prílohy uvedené v týchto podmienkach tvoria súčasť dohody uzatvorenej s klientom.

Prílohy:

Príloha č. 1a: Napojenie EBICS

Príloha č. 1b: Špecifikácia napojenia EBICS

Príloha č. 1c: Bezpečnostné požiadavky na systém klienta EBICS

Príloha č. 2: momentálne neobsadené

Príloha č. 3: Špecifikácia formátu dát

COMMERZBANK
Banka po Vašom boku

Príloha č. 1a: Napojenie na EBICS

1. Postup autorizácie a zabezpečenia

Klient (majiteľ účtu) oznámi finančnej inštitúcii účastníkov a ich oprávnenia v rámci diaľkového prenosu dát.

V napojení na EBICS sa používajú nasledovné autorizačné a zabezpečovacie postupy:

- elektronické podpisy
- autorizačný podpis
- šifrovanie

S ohľadom na každý autorizačný a zabezpečovací postup má účastník individuálny pár kľúčov, ktorý pozostáva zo súkromného a verejného kľúča. Verejné kľúče účastníka musia byť finančnej inštitúcii oznámené podľa postupov uvedených v bode 2. Verejné kľúče banky musia byť chránené podľa postupov uvedených v bode 2 pred neoprávneným pozmeňovaním. Páry kľúčov patriace účastníkovi je možné využívať aj na komunikáciu s inými finančnými inštitúciami.

1.1 Elektronické podpisy

1.1.1 Elektronické podpisy účastníkov

Pre elektronické podpisy (EU) účastníkov sú definované nasledovné triedy podpisov:

- – individuálny podpis (typ „E")
- – prvotný podpis (typ „A")
- – druhý podpis (typ „B")
- – prenosný podpis (typ „T")

Ako odborný bankový elektronický podpis sa označuje elektronický podpis typu „E", „A" alebo „B". Odborný bankový elektronický podpis slúži na autorizáciu príkazov. Príkazy si môžu vyžadovať odborné bankové elektronické podpisy, ktoré musia zadať rôzni užívatelia (majitelia účtov a ich splnomocnenci). Pre každý podporovaný druh príkaz sa medzi finančnou inštitúciou a klientom dohodne minimálny počet bankových elektronických podpisov.

Bankové elektronické podpisy typu „T", ktoré sa označujú za prenosné podpisy, sa nepoužívajú na schvaľovanie príkazov, ale len na ich prenos do bankových systémov. „Technickým účastníkom" (viď bod 2.2) je možné prideliť len elektronický podpis typu „T".

V programe, ktorý používa klient, je možné vyhotovovať rôzne správy (napr. príkazy pre domáce a zahraničné platby, ale aj pre inicializáciu, vyvolanie protokolu a získanie informácií o účte a obrate). Finančná inštitúcia klientovi oznámi, aké druhy správ môže používať a aký elektronický podpis má byť pre tento účel použitý.

1.2 Autorizačný podpis

Na rozdiel od elektronického podpisu, ktorý podpisuje údaje z príkazov, sa autorizačný podpis vytvára pomocou jednotlivej správy EBICS, vrátane riadiacich a prihlasovacích dát a obsiahnutého elektronického podpisu. S výnimkou niektorých systémových druhov príkazov definovaných v špecifikácii EBICS sa autorizačný podpis vykonáva pri každom kroku transakcie zo strany systému klienta ako aj bankového systému. Klient musí zabezpečiť, aby bol použitý softvér, ktorý kontroluje autorizačný podpis každej správy EBICS zasielanej finančnou inštitúciou pri zohľadnení aktuálnosti a pravosti uložených verejných kľúčov finančnej inštitúcie podľa ustanovení špecifikácie EBICS (viď Príloha č. 1b).

1.3 Šifrovanie

Na zabezpečenie utajenia bankových dát na užívateľskej úrovni musia byť dáta z príkazov klientom zašifrované pri zohľadnení aktuálnosti a pravosti uložených verejných kľúčov finančnej inštitúcie podľa ustanovení špecifikácie EBICS (viď Príloha č. 1b).

Okrem toho musí byť na externých prenosových trasách medzi systém klienta a bankovým systémom vykonané šifrovanie prenosu. Klient musí musí zabezpečiť, aby bol použitý softvér, ktorý kontroluje aktuálnosť a pravosť používaných certifikátov servera finančnej inštitúcie podľa ustanovení špecifikácie EBICS (viď Príloha č. 1b).

2. Inicializácia napojenia na EBICS

2.1 Vytvorenie komunikačného spojenia

Na vytvorenie komunikačného spojenia sa používa URL (Uniform Resource Locator). Alternatívne môže byť použitá aj IP adresa príslušnej finančnej inštitúcie. URL alebo IP adresa budú oznámené klientovi pri uzatvorení zmluvy s finančnou inštitúciou.

Finančná inštitúcia oznámi účastníkom oznámeným klientom za účelom vytvorenia napojenia na EBICS nasledovné údaje:

- URL alebo IP adresa finančnej inštitúcie
- označenie finančnej inštitúcie
- Host-ID
- prípustná(é) verzia(e) pre protokol EBICS a postup zabezpečenia
- IP partnera (ID klienta)
- ID užívateľa
- ID systému (pre technických účastníkov)
- ďalšie technické údaje o oprávneniach klienta a účastníka

Pre účastníkov pridelených klientovi priradí finančná inštitúcia ID užívateľa, ktoré jednoznačne identifikuje účastníka. Ak sú ku klientovi priradený jeden alebo viacerí účastníci (systém s viacerými užívateľmi), pridelí finančná inštitúcia dodatočne k ID užívateľa aj ID systému. Ak nie je stanovený technický účastník, sú ID systému a ID užívateľa zhodné.

2.2 Inicializácia kľúčov

2.2.1 Nová inicializácia kľúčov účastníka

Páry kľúčov, ktoré účastník používa na bankový elektronický podpis, šifrovanie údajov z príkazov a autorizačný podpis musia okrem podmienok uvedených v bode 1 spĺňať aj nasledovné všeobecné požiadavky:

(1.) Páry kľúčov sú priradené výhradne a jednoznačne účastníkovi.

(2.) Ak účastník generuje svoje kľúče samostatne, musia byť súkromné kľúče vyhotovené prostriedkami, ktoré dokáže účastník sám kontrolovať.

(3.) Ak kľúče poskytuje tretia osoba, musí byť zabezpečené, aby sa súkromné kľúče dostali do výhradnej držby účastníka.

(4.) S ohľadom na súkromné kľúče používané na autorizáciu musí účastník definovať pre každý kľúč heslo, ktoré zabezpečí prístup k príslušným súkromným kľúčom.

(5.) S ohľadom na súkromné kľúče používané na výmenu dát musí účastník definovať pre každý kľúč heslo, ktoré zabezpečí prístup k príslušným súkromným kľúčom. Od definovania hesla je možné upustiť, ak je zabezpečovacie médium účastníka uložené v technickom prostredí, ktoré je chránené pred neoprávneným prístupom.

Na inicializáciu účastníka vo finančnej inštitúcii je nevyhnutný prenos verejných kľúčov účastníka do systému banky. Za týmto účastník účastník odošle do finančnej inštitúcie svoje verejné kľúče pomocou dvoch od seba nezávislých komunikačných ciest:

- cez napojenie na EBICS prostredníctvom predpokladaných systémových druhov príkazov
- na základe inicializačného listu podpísaného majiteľom účtu alebo splnomocnencom k účtu.

Za účelom aktivovania účastníka finančná inštitúcia skontroluje na základe inicializačných listov podpísaných majiteľom účtu alebo splnomocnencom k účtu autenticitu verejných kľúčov účastníka odoslaný prostredníctvom EBICS.

Ku každému verejnému kľúču účastníka bude inicializačný list obsahovať nasledovné údaje:

- účel použitia verejného kľúča účastníka
- elektronický podpis
- autorizačný podpis
- šifrovanie
- podpora verzia páru kľúčov
- uvedenie dĺžky exponenta
- exponent verejného kľúča v hexadecimálnom zobrazení
- uvedenie dĺžky modulu
- modulus verejného kľúča v hexadecimálnom zobrazení
- hodnota hash verejného kľúča v hexadecimálnom zobrazení

Finančná inštitúcia skontroluje podpis majiteľa účtu príp. splnomocnenca k účtu na inicializačnom liste ako aj zhodu medzi hodnotami hash zaslanými prostredníctvom napojenia na EBICS a písomne odoslanými hodnotami hash verejného kľúča účastníka. V prípade pozitívneho výsledku kontroly finančná inštitúcia aktivuje príslušného účastníka pre dohodnuté druhy príkazy.

2.3 Inicializácia bankových kľúčov
Účastník vyzdvihne verejný kľúč finančnej inštitúcie pomocou na to určeného systémového druhu príkazu.

Finančná inštitúcia poskytuje hodnotu hash verejného bankového kľúča dodatočne prostredníctvom druhej komunikačnej cesty osobitne dohodnutej s klientom.

Pred prvým využitím EBICS musí skontrolovať pravosť verejných bankových kľúčov odoslaných formou diaľkového prenosu tým, že porovná hodnoty hash s hodnotami hash, ktoré oznámila finančná inštitúcia prostredníctvom komunikačnej cesty osobitne dohodnutej s klientom.

Klient musí zabezpečiť, aby bol používaný softvér, ktorý kontroluje platnosť certifikátov servera používaných v rámci šifrovania prenosu na základe certifikačnej cesty osobitne oznámenej finančnou inštitúciou.

3. Udelenie príkazu banke

Užívateľ kontroluje správnosť dát z príkazov a zabezpečí, aby boli elektronicky podpísané presne tieto dáta. Pri spustení komunikácie finančná inštitúcia najprv vykonáva kontroly oprávnení na strane účastníka, napr. oprávnenie na isté druhy príkazov alebo dohodnuté kontroly limitov. Výsledky ďalších bankových kontrol, napr. kontrol limitov alebo kontrol oprávnení k účtu, sa oznamujú klientovi vo forme protokolu, ktorý sa zasiela neskôr.

Príkazy zasielané do systému banky môžu byť autorizované nasledovne:

(1.) Všetky nevyhnutné bankové elektronické podpisy sa prenášajú spoločne s dátami z príkazov.

(2.) Ak bol s klientom pre príslušný druh príkaz dohodnutý rozdelený elektronický podpis (VEU) a ak nie sú odoslané elektronické podpisy pre banku a schválenie dostatočné, bude príkaz až do odovzdania všetkých nevyhnutných elektronických podpisov uložený v systéme banky.

(3.) Ak sa klient a Banka dohodnú, že autorizácia dát z príkazov a príkazov zasielaných formou diaľkového prenosu dát je možná na základe osobitne zaslaných

sprievodných lístkov/hromadných príkazov, musí byť namiesto bankového elektronického podpisu vykonaný prenosový podpis (typ „T“) za účelom technického zabezpečenia dát z príkazov. Za týmto účelom musí byť súbor označený špeciálnym symbolom, ktorý uvádza, že okrem prenosového podpisu (typ „T“) neexistuje k tomuto príkaz iný elektronický podpis. Schválenie príkazu je možné po úspešnej kontrole podpisu užívateľa na sprievodnom lístku/hromadnom príkaze zo strany finančnej inštitúcie.

3.1 Udelenie príkazu pomocou rozdeleného elektronického podpisu (VEU)
Spôsob, akým sa používa rozdelený elektronický podpis klientom, musí byť dohodnutý s finančnou inštitúciou.

Rozdelený elektronický podpis (VEU) sa musí použiť vtedy, ak má byť autorizácia príkazov vykonávaná nezávisle od prenosu dát z príkazu príp. aj zo strany viacerých účastníkov.

Ak ešte nie sú k dispozícii všetky bankové elektronické podpisy nevyhnutné na autorizáciu, môže byť príkaz vymazaný oprávneným užívateľom. Ak bol príkaz v plnom rozsahu autorizovaný, je možné len odvolanie podľa odseku 8 Podmienok pre prenos dát.

Finančná inštitúcia je za týmto účelom oprávnená vymazať neúplne autorizované príkazy po uplynutí časového limitu osobitne oznámeného bankou.

3.2 Kontrola autorizácie zo strany banky
Prijatý príkaz banka vykoná až potom, ako boli prijaté nevyhnutné bankové elektronické podpisy príp. podpísaný sprievodný ôístok/ hromadný príkaz a ak boli pozitívne skontrolované.

3.3 Protokoly klientov
Banka zaznamenáva v protokoloch nasledovné postupy:

- prenos dát z príkazov do systému banky
- prenos informačných súborov zo systému banky do systému klienta
- výsledok každej kontroly autorizácie príkazov klienta zadaných do systému banky
- ďalšie spracovanie príkazov, ak sa dotýkajú kontroly podpisu a oznámenia dát z príkazov.

Účastník sa musí po vyvolaní protokolu klienta informovať o výsledku kontrol vykonaných na strane finančnej inštitúcie.

Účastník musí tento protokol, ktorý obsahovo zodpovedá ustanoveniam kapitoly 10 Prílohy č. 1b, vložiť do svojich záznamov a na požiadanie ich predložiť finančnej inštitúcii.

4. Zmena kľúčov účastníka s automatickou aktiváciou

Ak je platnosť autorizačných a zabezpečovacích médií používaných účastníkom časovo obmedzená, musí účastník banke predložiť nové verejné kľúče účastníka ešte pred uplynutím platnosti. Po ukončení doby platnosti starých kľúčov musí byť vykonaná nová inicializácia.

Ak účastník sám generuje svoje kľúče, musí okrem toho v momente dohodnutom s finančnou inštitúciou obnoviť kľúče účastníka pri použití na to určených systémových druhov príkazov a odoslať ich včas pred uplynutím platnosti starých kľúčov.

Na automatickú aktiváciu nových kľúčov bez opätovnej inicializácie účastníka musia byť použité nasledovné druhy príkazov:

- aktualizácia verejného bankového kľúča (PUB)
- aktualizácia verejného autorizačného kľúča a verejného šifrovacieho kľúča (HCA)
- aktualizácia všetkých troch vyššie uvedených kľúčov (HCS)

Druhy príkazov PUB a HCA príp. HCS musia byť za týmto účelom opatrené platným bankovým elektronickým podpisom užívateľa. Po úspešnej zmene je možné používať už len nové kľúče.

Ak nebolo možné úspešne skontrolovať elektronický podpis, postupuje sa podľa bodu 7 ods. 3 Podmienok pre diaľkový prenos dát.

Zmena kľúčov je možná až po spracovaní všetkých príkazov. V opačnom prípade musia byť ešte nevykonané príkazy udelené s novým kľúčom.

5. Zablokovanie kľúčov účastníka

Ak existuje podozrenie zo zneužitia kľúčov účastníka, je účastník za týmto účelom povinný zablokovať svoje prístupové právo ku všetkým bankovým systémom, ktoré používajú príslušný/é skompromitovaný/é kľúč/e.

Ak účastník disponuje platnými autorizačnými a zabezpečovacími médiami, môže svoje prístupové právo zablokovať aj prostredníctvom napojenia na EBICS. Pritom bude zaslaním správy s druhom príkazu „SPR“ zablokovaný prístup pre účastníka, pod ktorého ID užívateľa bola správa zaslaná. Po zablokovaní nemôže tento účastník do novej inicializácie popísanej v bode 2 zadávať príkazy prostredníctvom napojenia na EBICS.

Ak účastník nedisponuje platnými autorizačnými a zabezpečovacími médiami, môže mimo postupu pre diaľkový prenos dát zabezpečiť zablokovanie svojich autorizačných a zabezpečovacích médií prostredníctvom blokovacieho zariadenia, ktoré bolo osobitne oznámené zo strany banky.

Klient kann môže mimo postupu pre diaľkový prenos dát zabezpečiť zablokovanie autorizačných a zabezpečovacích médií účastníka alebo celkový prístup k diaľkovému prenosu dát prostredníctvom blokovacieho zariadenia, ktoré bolo osobitne oznámené zo strany banky.

COMMERZBANK
Banka po Vašom boku

Príloha č. 1b: Špecifikácia napojenia na EBICS

Špecifikácia je zverejnená na internetovej stránke: http://www.ebics.de

COMMERZBANK
Banka po Vašom boku

Príloha č. 1c: Bezpečnostné požiadavky na systém EBICS

Okrem bezpečnostných opatrení popísaných v Prílohe č. 1a bod 5 musí klient zohľadňovať nasledovné požiadavky:

- softvér používaný klientom pre postup EBICS musí spĺňať požiadavky popísané v Prílohe č. 1a
- systémy EBICS nie je možné používať bez firewall. Firewall je zariadenie, ktoré monitoruje celú výmenu prichádzajúcich a odchádzajúcich správ a ktoré povoľuje len známe alebo autorizované spojenia.
- je potrebné nainštalovať antivírový program, ktorý musí byť pravidelne aktualizovaný
- systém EBICS musí byť vyhotovený tak, že sa účastník musí pred jeho používaním prihlásiť. Prihlásenie musí byť ako bežný užívateľ, a nie ako správca príp. oprávnená osoba vykonávajúca inštaláciu programov.
- Interné IT komunikačné cesty pre nešifrované bankové dáta alebo nešifrované správy EBICS musia byť chránené pred odpočúvaním a manipuláciou.
- Ak existujú bezpečnostné aktualizácie používaného operačného systému a ďalších softvérov týkajúce sa bezpečnosti, musia byť používané systémy EBICS aktualizované.

Za splnenie týchto požiadaviek zodpovedá výhradne klient.

COMMERZBANK
Banka po Vašom boku

Príloha č. 2:

V súčasnej dobe sa nepoužíva

COMMERZBANK
Banka po Vašom boku

Príloha č. 3: Špecifikácia formátov dát

Špecifikácia je zverejnená na internetovej stránke: http://www.ebics.de.

Vaša pobočka Commerzbank:

COMMERZBANK Aktiengesellschaft,

pobočka zahraničnej banky, Bratislava
Rajská 15/A
811 08 Bratislava

Telefón: +421 257 103 111
Fax: +421 257 103 116

www.commerzbank.sk