Podmienky diaľkového prenosu dát (DPD) Oberbank AG pobočka zahraničnej banky v Slovenskej republike

ku dňu: 15.08.2019

Oberbank AG so sídlom Untere Donaulände 28, A-4020 Linz, Rakúska republika, zapísaná v obchodnom registri (Firmenbuch) Krajského súdu Linz (Landesgericht Linz) pod číslom FN 79063w, organizačná zložka: **Oberbank AG pobočka zahraničnej banky v Slovenskej republike** so sídlom: Prievozská 4/A, 821 09 Bratislava, IČO 36 861 146, DIČ:4020139662, zapísaná v Obchodnom registri Okresného súdu Bratislava I, oddiel: Po, vložka č. 1660/B

(ďalej len „Banka“ alebo „Oberbank AG“)

vydáva nasledovné podmienky diaľkového prenosu dát (ďalej len „DPD“):

1. ROZSAH PLNENIA

1.1 Banka umožňuje svojim klientom zasielanie dát elektronickou cestou - diaľkový prenos dát (DPD). DPD zahŕňa zadávanie, ako aj výmenu údajov (prenos príkazov a sťahovanie informácií o obratoch na účte).

1.2 Banka oznámi klientovi typy služieb, ktoré môže v rámci DPD využívať. Ak banka pre dispozície zadávané prostredníctvom DPD nastaví v systéme určitý limit, bude o tom klienta informovať.

1.3 Diaľkový prenos dát je možný dvoma spôsobmi, cez rozhranie EBICS (príloha 1a až 1c) alebo rozhranie MCFT (príloha 2a až 2b). Klient a banka sa dohodnú na definitívnom spôsobe prenosu.

2. VŠEOBECNÉ PODMIENKY PREVÁDZKY

2.1 Užívateľ je povinný aplikovať postupy pre prenos a zabezpečenie dát dohodnuté s bankou, ako i rešpektovať dohodnuté rozhrania.

2.2 Klient je povinný používať software schválený bankou. Ak sa požiadavky na software zmenia, oznámi banka včas túto skutočnosť klientovi a oznámi termín, od ktorého k zmene dôjde. Je potrebné rešpektovať užívateľské ovládanie špecifické pre túto službu.

2.3 Dáta klienta musia ohľadom ich štruktúry dávky a dátových súborov, ako i ohľadom špecifikácii zodpovedať údajom uvedeným v prílohe 3.

2.4 Pred zaslaním dát do banky je potrebné zaznamenať (zálohovať) zasielané dáta s ich úplným obsahom vrátanie dát nevyhnutných na kontrolu preukázania totožnosti, ak tieto nie sú tajné. Ak nie je stanovené inak, je klient povinný tieto dáta preukázateľne uschovať odo dňa zaslania dát do banky po dobu 14 pracovných dní pri tuzemských príkazoch na úhradu, a po dobu 30 pracovných dní v prípade zahraničných príkazov, a to v takej forme, aby súbor mohol byť na výzvu banky v krátkej dobe odoslaný znovu, ak nie je dojednané nič iné.

2.5 Ak banka užívateľovi poskytne dáta o platobných operáciách, ktoré ešte nie sú s konečnou platnosťou spracované (predbežné položky), potom predstavujú tieto dáta len nezáväznú informáciu. Takéto dáta sú vždy zvlášť označené.

2.6 Príkazné údaje predložené prostredníctvom DPD je podľa dohody s bankou potrebné autorizovať elektronickým podpisom. Príkazné údaje sa považujú za platný príkaz ak všetky potrebné elektronické podpisy používateľov boli doručené DPD v dohodnutej lehote a elektronické podpisy bolo možné úspešne overiť za pomoci dohodnutých kľúčov.

3. IDENTIFIKAČNÉ MÉDIÁ A PREUKAZOVANIE TOTOŽNOSTI, OPRÁVNENÍ UŽÍVATELIA

3.1 Príkazy môže prostredníctvom rozhrania EBICS, resp. MCFT zadávať len klient alebo ním poverený disponent k účtu. Klient a disponent sa ďalej budú súhrnne označovať ako „používateľ“. Na autorizáciu príkazných údajov prenášaných DPD potrebuje každý používateľ individuálne identifikačné médiá aktivované bankou. Požiadavky na identifikačné médiá sú opísané v prílohe 1a resp. v prílohe 2a.

3.2 V prípade výmeny dát prostredníctvom rozhrania EBICS môže klient okrem splnomocneného disponenta určiť aj „technických účastníkov“, ktorí sú oprávnení len na vykonávanie výmeny údajov (prenos príkazov a sťahovanie informácií o obratoch na účte). Používatelia a technickí účastníci sa ďalej budú spoločne označovať pojmom „účastníci“. Ochrana výmeny dát si vyžaduje, aby každý účastník mal individuálne,

bankou aktivované bezpečnostné médiá. Požiadavky na bezpečnostné médiá sú opísané v prílohe 1a.

3.3 V prípade výmeny dát prostredníctvom rozhrania MCTF potrebuje každý používateľ heslo na diaľkový prenos dát, ktoré mu sprístupní banka. Požiadavky na heslo na diaľkový prenos dát sú opísané v prílohe 2a.

4. POVINNOSTI PRI ZAOBCHÁDZANÍ S IDENTIFIKAČNÝMI MÉDIAMI PRE AUTORIZÁCIU PRÍKAZOV A BEZPEČNOSTNÝMI MÉDIAMI PRE VÝMENU ÚDAJOV

4.1 Na základe postupu prenosu dohodnutého s bankou je klient povinný zabezpečiť, aby všetci používatelia dodržiavali identifikačné postupy uvedené v prílohe 1a, resp. prílohe 2a.

4.2 Za pomoci médií dohodnutých s bankou sa užívateľ identifikuje a preukáže totožnosť voči banke a môže zadávať príkazy. Užívateľ je povinný zaistiť, aby nepovolaná tretia osoba nezískala prístup k médiám slúžiacim na identifikáciu a preukazovanie totožnosti a nedozvedela sa heslo, ktoré slúži na ich ochranu, pretože akákoľvek osoba, ktorá drží médiá alebo ich duplikáty, môže využívať dojednané služby. Za účelom utajenia prostriedkov na identifikáciu a preukazovanie totožnosti je potrebné dbať najmä na nasledovné skutočnosti:

4.2.1 údaje, ktoré užívateľa identifikujú, nesmú byť ukladané mimo bezpečnostných médií, napr. na pevnom disku počítača;

4.2.2 médiá na identifikáciu a preukazovanie totožnosti je potrebné po použití DPD vyňať z čítacej jednotky a uschovať na bezpečnom mieste;

4.2.3 heslo slúžiace na ochranu médií na identifikáciu a preukazovanie totožnosti nesmie byť nikde poznamenané ani uložené v elektronickej podobe;

4.2.4 pri zadávaní hesla je potrebné zabezpečiť, aby ho žiadna tretia osoba nemohla vysledovať.

5. ZABLOKOVANIE IDENTIFIKAČNÝCH A BEZPEČNOSTNÝCH MÉDIÍ

5.1 V prípade straty identifikačných alebo bezpečnostných médií, v prípade, ak sa o nich dozvie iná osoba alebo v prípade, že existuje podozrenie na ich zneužitie, musí účastník bezodkladne zabezpečiť, aby banka zablokovala prístup k DPD. Podrobnejšie upravené v prílohe 1a ako aj v prílohe 2a. Klient môže mimo DPD nechať zablokovať identifikačné alebo bezpečnostné médiá účastníka alebo celkový prístup k diaľkovému prenosu dát prostredníctvom bankou oznámeného nástroja na zablokovanie.

5.2 Ak užívateľ banke doručil žiadosť o zablokovanie prístupu, nesie banka zodpovednosť od okamihu doručenia tejto správy za všetky škody, ktoré vzniknú ich nerešpektovaním.

5.3 V prípade troch po sebe nasledujúcich pokusov o zaslanie príkazu banke za pomoci nesprávneho identifikačného média, alebo o vykonanie výmeny údajov za pomoci nesprávneho bezpečnostného média, banka zablokuje prístup k DPD príslušného účastníka. Blokovanie nie je možné zrušiť prostredníctvom DPD. Ak klient chce zrušiť toto blokovanie, musí kontaktovať svoju banku.

5.4 Banka zablokuje celkový prístup k DPD v prípade, že existuje podozrenie na zneužívanie prístupu k DPD. Klienta o tom informuje inou formou ako prostredníctvom DPD. Blokovanie nie je možné zrušiť prostredníctvom DPD.

6. SPRACOVANIE DÁT ZASLANÝCH BANKE UŽÍVATEĽOM

6.1 Príkazy zadané banke prostredníctvom DPD sú spracované v rámci riadneho pracovného postupu. Banka je oprávnená, avšak nie povinná vykonávať príkazy na ťarchu účtu aj pri nedostatočnom krytí. Príkazy, ktoré nebudú vykonané z dôvodu nedostatočného krytia, budú klientovi telefonicky alebo písomne oznámené.

6.2 Banka kontroluje totožnosť odosielateľa a súlad dátových súborov s ustanoveniami podľa prílohy 1 a 2.

6.3 Pokiaľ budú pri kontrole totožnosti zistené nezrovnalosti, banka príslušný súbor nespracuje a klientov o tom bezodkladne informuje.

6.4 Ak sa vyskytnú chyby pri bankovej kontrole dátových súborov, banka zdokladuje chybné dátové súbory vrátane ich úplného obsahu a oznámi to bezodkladne užívateľovi. Banka je oprávnená chybné dátové súbory vylúčiť z ďalšieho spracovania, pokiaľ nebude možné zaistiť riadne vykonanie príkazu.

6.5 Stanovenie termínu na prijatie dátového súboru nepredstavuje prísľub termínu na vykonanie príkazu.

6.6 Klient je povinný bezchybne zadávať smerový kód banky príjemcu/BIC a číslo účtu/IBAN príjemcu. Banky, ktoré sú zapojene do vybavenia príkazu na úhradu, sú oprávnené spracovať ho len na základe týchto údajov. Chybné údaje môžu mať za následok zaslanie platby nesprávnemu príjemcovi. Škody a nevýhody, ktoré z toho vzniknú, idú na ťarchu klienta.

6.7 Banka vykoná príkazy za predpokladu, že sú splnené všetky nasledujúce podmienky vykonania:

- príkazné údaje dodané prostredníctvom DPD a boli autorizované,
- bol použitý stanovený dátový formát,
- bola dodržaná lehota na prijatie platobných príkazov,
- nebol prekročený limit na disponovanie.

6.8 V prípade, že podmienky vykonania neboli splnené, banka príkaz nevykoná a klienta o jeho nevykonaní bezodkladne informuje dohodnutým spôsobom.

7. ZODPOVEDNOSŤ

7.1 Klient znáša zodpovednosť za všetky škody, ktoré vzniknú nedodržiavaním týchto podmienok vrátane ich príloh alebo zneužitím médií, ktoré má k dispozícii na dátovú komunikáciu a preukazovanie totožnosti voči banke; to platí najmä vtedy, ak médiá sprístupnil tretím osobám. Klient znáša zodpovednosť tiež za škody, ktoré vzniknú vytváraním kópii z médií (kopírovanie software).

7.2 Klient je vo vzťahu k banke zodpovedný za všetky škody a nevýhody, ktoré vzniknú tým, že sa dáta s príkazmi alebo ďalšie dáta, ktoré zaslal banke, nenachádzajú v riadnom stave alebo sú nesprávne alebo neúplné, ibaže banka tento nedostatok mohla odhaliť v rámci svojej kontroly podľa bodu 6.7.

7.3 Banka zodpovedá v rámci svojho zavinenia len v takej miere, v akej prispela k vzniku škody v pomere k ostatným príčinám.

7.4 Banka si vyhradzuje právo prechodne alebo trvalo zablokovať prístup k diaľkovému prenosu dát, pokiaľ je to zo závažného dôvodu nevyhnutné, napr. z technických dôvodov.

8. STORNOVANIE PRÍKAZOV

8.1 Stornovanie zaslaného súboru je vylúčené, akonáhle banka začala s jeho spracovaním. Banka však môže zrušiť príkaz za predpokladu, že správu o zrušení dostane natoľko včas, aby ju bolo možné v rámci obvyklého pracovného postupu zohľadniť. Zmena obsahu súboru je možná iba stornovaním a novým zaslaním súboru.

8.2 Stornovanie jednotlivých príkazov zo súborov je možné vykonať len mimo režimu DPD, ibaže by banka v rámci tohto režimu s takou možnosťou počítala. Užívateľ banke musí za týmto účelom oznámiť jednotlivé údaje z originálneho príkazu, a to smerový kód banky príjemcu /kód BIC, číslo účtu /IBAN a mená príjemcov /platiteľov, čiastku, smerový kód banky platiteľa /prvého inkasného miesta a číslo účtu a meno platiteľa /príjemcu platby, ako aj údaje v dátovom poli „účel použitia“ podľa prílohy 3.

Príloha 1a: Rozhranie EBICS
Príloha 1b: Špecifikácia pripojenia EBICS
Príloha 1c: Bezpečnostné požiadavky pre klientsky systém EBICS
Príloha 2a: Rozhranie MCFT
Príloha 2b: Bezpečnostné požiadavky pre klientsky systém MCFT
Príloha 3: Štruktúra a špecifikácia súborov s platobnými príkazmi
Príloha 4: Postúpenie údajov v prípade zmeny formátu

V dňa

Oberbank AG

Oberbank AG pobočka zahraničnej banky v Slovenskej republike

Príloha 1a: **Rozhranie EBICS**

1. IDENTIFIKAČNÉ A BEZPEČNOSTNÉ POSTUPY

Klient (majiteľ účtu) uvedie banke účastníkov a ich oprávnenia v rámci DPD.

V rámci rozhrania EBICS sa používajú nasledujúce identifikačné a bezpečnostné postupy:

- Elektronické podpisy
- Overovací podpis
- Šifrovanie

Účastník má pre každý identifikačný a bezpečnostný postup k dispozícii samostatnú dvojicu kľúčov, ktorá pozostáva zo súkromného a verejného kľúča. Verejné kľúče účastníkov je banke potrebné oznámiť prostredníctvom postupu opísaného v bode 2. Verejné bankové kľúče je potrebné chrániť pred neoprávnenými zmenami na základe postupu opísaného v bode 2. Dvojice kľúčov účastníkov je možné využiť aj pri komunikácii s inými bankami.

1.1 Elektronické podpisy

Pri elektronických podpisoch účastníkov je potrebné definovať tieto triedy podpisov:

Samostatný podpis (typ „E“)
Prvý podpis (typ „A“)
Druhý podpis (typ „B“)
Transportný podpis (typ „T“)

V bankovníctve používané elektronické podpisy sú podpisy označené ako typ „E“, „A“ alebo „B“. Bankové elektronické podpisy slúžia na autorizáciu príkazov. Príkazy si môžu vyžadovať viacero bankových elektronických podpisov rôznych používateľov (majiteľov účtov a ich disponentov). Pre každý podporovaný typ príkazu dohodne banka s klientom minimálny počet bankových elektronických podpisov.

Elektronické podpisy typu „T“, ktoré sa označujú ako transportné podpisy, sa nepoužívajú na bankové schvaľovanie príkazov, ale len na odosielanie príkazov do systému banky. „Technickým účastníkom“ (bod 2.2) môžu byť pridelené len elektronické podpisy typu „T“.

Program, ktorý používa klient, môže generovať rôzne správy (napr. tuzemské alebo zahraničné platobné príkazy, ale aj správy týkajúce sa inicializácie, stiahnutia protokolu alebo vyvolania informácií o účte a obratoch, atď.). Banka informuje klienta o tom, ktorý typ správy môže použiť a ktorý typ elektronického podpisu sa v danom prípade použije.

1.2 Overovací podpis

Na rozdiel od elektronického podpisu, ktorý sa používa na podpisovanie príkazných dát, overovací podpis sa vytvára pre jednotlivé správy EBICS na základe kontrolných a prihlasovacích údajov a v nich obsiahnutých elektronických podpisov. S výnimkou niekoľkých typov príkazov týkajúcich sa systému, ktoré sú definované v špecifikáciách pre rozhranie EBICS, poskytuje overovací podpis v každom kroku transakcie ako systém klienta, tak aj systém banky. Klient musí zabezpečiť, aby sa používal softvér, ktorý v súlade so špecifikáciami pre rozhranie EBICS (príloha 1b) overuje overovací podpis každej správy EBICS posielanej bankou, pri zohľadnení aktuálnosti a pravosti uložených verejných kľúčov banky.

1.3 Šifrovanie

Na zabezpečenie dôvernosti bankových údajov na úrovni aplikácie musí klient príkazné údaje zašifrovať v súlade so špecifikáciami pre rozhranie EBICS (príloha 1b), pri zohľadnení aktuálnosti a pravosti uložených verejných kľúčov banky.

Okrem toho je potrebné pri externých prenosových kanáloch medzi systémom klienta a systémom banky používať ešte aj transportné šifrovanie. Klient musí zabezpečiť, aby sa používal softvér, ktorý v súlade so špecifikáciami pre rozhranie EBICS (príloha 1b) overuje aktuálnosť a pravosť certifikátov pre server, ktorý banka používa.

2. INICIALIZÁCIA ROZHRANIA EBICS

2.1 Zriadenie komunikačného spojenia

Komunikačné spojenie sa zriadi prostredníctvom URL (Uniform Ressource Locator). Alternatívne je možné použiť aj IP-adresu príslušnej banky. URL alebo IP-adresa budú klientovi oznámené pri podpise zmluvy s bankou.

Pre inicializáciu rozhrania EBICS poskytne banka účastníkom, ktorých určí klient, nasledujúce údaje:

- URL alebo IP-adresa banky
- názov banky
- hostiteľské ID
- povolená(é) verzia(e) protokolu EBICS a bezpečnostných postupov
- partnerské ID (ID klienta)
- používateľské ID
- systémové ID (pre technických účastníkov)
- ďalšie špecifické údaje o oprávneniach klienta a účastníkov.

Účastníkom priradeným ku klientovi pridelí banka jedno používateľské ID, ktoré účastníka jednoznačne identifikuje. Pokiaľ má klient priradených jedného alebo viacerých technických účastníkov (systém s viacerými používateľmi), banka okrem používateľského ID priradí aj systémové ID. V prípade, že nie je určený žiadny technický účastník, je systémové ID a používateľské ID rovnaké.

2.2 Inicializácia kľúčov

Okrem všeobecných podmienok opísaných v bode 1 musí dvojica kľúčov používaná pre bankové elektronické podpisy, šifrovanie príkazných údajov a overovací podpis zodpovedať aj týmto požiadavkám:

- Dvojice kľúčov musia byť priradené výlučne a jednoznačne účastníkovi.
- V prípade, že účastník svoje kľúče generuje sám, súkromné kľúče musia byť vygenerované takým spôsobom, ktorý je výhradne pod kontrolou účastníka.
- V prípade, že kľúče sprístupnila tretia strana, je potrebné zabezpečiť, že účastník je jediným vlastníkom súkromných kľúčov.
- Pokiaľ ide o súkromné kľúče, ktoré sa používajú na identifikáciu, každý používateľ musí pre každý kľúč stanoviť heslo, ktoré bude zabezpečovať prístup k príslušnému súkromnému kľúču.
- Pokiaľ ide o súkromné kľúče, ktoré sa používajú na zabezpečenie výmeny dát, každý účastník stanoví pre každý kľúč heslo, ktoré bude zabezpečovať prístup k príslušnému súkromnému kľúču. Toto heslo nemusí byť použité v prípade, že bezpečnostné médium účastníka je uložené v technickom prostredí, ktoré je chránené pred neoprávneným prístupom.

Inicializácia účastníka zo strany banky si vyžaduje prenos verejných kľúčov účastníkov do systému banky. Na tento účel účastník zašle svoje verejné kľúče banke prostredníctvom dvoch navzájom nezávislých komunikačných kanálov:

- prostredníctvom rozhrania EBICS za pomoci typov príkazov, ktoré systém na tento postup poskytuje,
- prostredníctvom inicializačného listu podpísaného majiteľom účtu alebo disponentom účtu.

Na účel aktivácie účastníka overí banka pravosť verejných účastníckych kľúčov zaslaných prostredníctvom rozhrania EBICS na základe inicializačných listov podpísaných majiteľom účtu alebo disponentom účtu.

Pre každý verejný účastnícky kľúč musí inicializačný list obsahovať nasledujúce údaje:

- Účel použitia verejného účastníckeho kľúča
- Elektronický podpis
- Overovací podpis/ Šifrovanie
- Príslušnú podporovanú verziu pre každú dvojicu kľúčov
- Určenie dĺžky exponenta
- Hexadecimálny zápis exponenta verejného kľúča
- Určenie dĺžky modulu
- Hexadecimálny zápis modulu verejného kľúča
- Hexadecimálny zápis hašovacej hodnoty verejného kľúča (údajová štruktúra)

Banka overí podpis majiteľa účtu resp. disponenta účtu v inicializačnom liste ako aj zhodnosť hašovacích hodnôt verejného účastníckeho kľúča prenášaných prostredníctvom rozhrania EBICS s hodnotami zaslanými písomne. V prípade pozitívneho výsledku banka príslušnému účastníkovi aktivuje dohodnuté typy príkazov.

2.3 Inicializácia bankových kľúčov

Účastník získa verejný kľúč banky prostredníctvom typu príkazu, ktorý systém na tento účel špeciálne poskytuje.

Hašovaciu hodnotu verejného bankového kľúča banka dodatočne sprístupní prostredníctvom druhého komunikačného kanálu, ktorý s klientom dohodne osobitne.

Pred prvým použitím EBICS účastník musí overiť pravosť verejných bankových kľúčov, ktoré mu boli zaslané diaľkovým prenosom dát tak, že porovná ich hašovacie hodnoty s hašovacími hodnotami, ktoré mu banka oznámi prostredníctvom osobitne dohodnutého komunikačného kanála.

Klient musí zabezpečiť, aby sa používal softvér, ktorý overuje platnosť certifikátov serveru používaného v súvislosti s transportným šifrovaním pomocou certifikačného kanálu, ktorý banka oznámi osobitne.

3. ZADÁVANIE PRÍKAZU BANKE

Používateľ overí správnosť príkazných údajov a zabezpečí, aby práve tieto údaje boli elektronicky podpísané. Po nadviazaní komunikácie banka najskôr overí oprávnenie týkajúce sa účastníka, ako napríklad autorizácia typu príkazu, alebo prípadne možné dohodnuté limity. Výsledky dodatočných overení zo strany banky, ako napríklad overenie limitu, alebo overenie oprávnenia disponovať s účtom, sa klientovi oznámia neskôr v protokole klienta. Výnimku tvorí on-line overenie príkazných údajov zo strany banky, ktoré si klient dohodol na voliteľnej báze.

Príkazné údaje, ktoré sa zašlú do systému banky, môžu byť autorizované nasledovne:

1. Všetky potrebné bankové elektronické podpisy sa prenášajú spolu s príkaznými údajmi.
2. Ak sa s klientom dohodlo používanie distribuovaného elektronického podpisu pre príslušný typ príkazu a zasielané elektronické podpisy nepostačujú na schválenie bankou, príkaz sa uloží v systéme banky, až kým nebudú použité všetky požadované elektronické podpisy.

3.1 Zadávanie príkazu prostredníctvom distribuovaného elektronického podpisu

S bankou je potrebné dohodnúť spôsob, akým bude klient používať distribuovaný elektronický podpis.

Distribuovaný elektronický podpis sa používa v prípadoch, keď majú byť príkazy schválené nezávisle od prenosu príkazných údajov a prípadne aj viacerými účastníkmi.

Príkaz môže vymazať používateľ, ktorý je na to oprávnený, avšak len pokiaľ ešte neboli použité všetky bankové elektronické podpisy potrebné na autorizáciu. Ak bol príkaz už plne autorizovaný, je možné ho už len odvolať podľa bodu 8 týchto podmienok pre diaľkový prenos dát.

Banka je oprávnená príkazy, ktoré neboli v plnej miere autorizované, vymazať po uplynutí bankou osobitne oznámenej lehoty.

3.2 Overenie identifikácie zo strany banky

Príkazné údaje doručené diaľkovým prenosom dát vykoná banka ako príkaz až vtedy, keď dostane potrebný bankový elektronický podpis a overí ho s pozitívnym výsledkom.

3.3 Protokoly klienta

V protokoloch klienta dokumentuje banka nasledovné procesy:

- prenos príkazných údajov do systému banky,
- prenos informačných súborov z bankového systému do systému klienta,
- výsledok všetkých overení identifikácie pre príkazy od klienta pre bankový systém,
- ďalšie spracovanie príkazov, ak sa týkajú overenia podpisov a zobrazenia príkazných údajov,
- chyby pri dekomprimácii.

Účastník je povinný sa informovať o výsledku overenia, ktoré vykonala banka a to prostredníctvom stiahnutia protokolu klienta.

Účastník je povinný tento protokol, ktorého obsah zodpovedá ustanoveniam bodu 10 prílohy 1b, zahrnúť do svojich podkladov a na žiadosť ho predložiť banke.

4. ZMENA ÚČASTNÍCKEHO KĽÚČA S AUTOMATICKOU AKTIVÁCIOU

V prípade, že platnosť identifikačných a bezpečnostných médií, ktoré účastník používa, je obmedzená, účastník musí odoslať do banky nové verejné účastnícke kľúče včas pred dátumom uplynutia platnosti. Po dátume uplynutia platnosti starých kľúčov je potrebné vykonať novú inicializáciu.

V prípade, že si účastník generuje kľúče sám, musia byť tieto účastnícke kľúče obnovené za pomoci typov príkazov, ktoré na tento účel poskytuje systém v deň dohodnutý s bankou. Okrem toho musia byť kľúče odoslané zavčasu pred uplynutím platnosti starých kľúčov.

Pri automatickej aktivácii nových kľúčov bez obnovenia inicializácie účastníka sa použitú tieto typy príkazov:

- Aktualizácia verejného bankového kľúča (PUB) a
- Aktualizácia verejného overovacieho kľúča a verejného šifrovacieho kľúča (HCA)

Typy príkazov PUB a HCA si na tento účel vyžadujú platný bankový elektronický podpis užívateľa. Po úspešnej zmene sa musia používať už len nové kľúče.

Ak nebolo možné pozitívne overiť elektronický podpis, postupuje sa podľa ustanovení bodu 6.3 týchto podmienok pre DPD.

Kľúče je možné zmeniť až po spracovaní všetkých príkazov. V opačnom prípade bude potrebné zadať ešte nespracované príkazy znovu za pomoci nového kľúča.

5. ZABLOKOVANIE ÚČASTNÍCKYCH KĽÚČOV

V prípade podozrenia zo zneužitia účastníckych kľúčov je účastník povinný zablokovať svoje prístupové oprávnenie ku všetkým bankovým systémom, pri ktorých sa využíva(jú) kompromitovaný(é) kľúč(e).

V prípade, že účastník má k dispozícii platné identifikačné a bezpečnostné médiá, môže zablokovať prístupové oprávnenia prostredníctvom rozhrania EBICS. Zaslaním správy s príkazom typu „SPR“ sa prístup zablokuje pre príslušného účastníka, ktorého používateľské ID bolo pre odoslanie správy použité. Po zablokovaní nemôže účastník zadávať žiadne ďalšie príkazy prostredníctvom rozhrania EBICS, a to až dovtedy, kým sa prístup opäť neinicializuje v súlade s bodom 2.

V prípade, že účastník už nemá k dispozícii platné identifikačné a bezpečnostné médiá, môže požiadať o zablokovanie identifikačného a bezpečnostného média aj mimo postupu diaľkového prenosu dát prostredníctvom bankou oznámeného nástroja na zablokovanie. Okrem prostredníctvom diaľkového prenosu dát môže klient nechať zablokovať identifikačné alebo bezpečnostné médiá účastníka alebo celkový prístup k diaľkovému prenosu dát prostredníctvom bankou oznámeného nástroja na zablokovanie.

Príloha 1b: **Špecifikácia pripojenia EBICS**

Špecifikácie je zverejnená na webovej stránke www.ebics.de.

Príloha 1c: **Bezpečnostné požiadavky pre klientsky systém EBICS**

Okrem bezpečnostných opatrení opísaných v prílohe 1a, musí klient dodržiavať aj nasledujúce požiadavky:

- Softvér, ktorý klient používa pri postupe EBICS, musí zodpovedať požiadavkám opísaným v prílohe 1a.
- Klientsky systém EBICS nesmie byť používaný bez firewallu. Firewall je aplikácia, ktorá sleduje všetky prichádzajúce a odchádzajúce správy a povoľuje len známe alebo autorizované spojenia.
- Je potrebné nainštalovať antivírusový program, ktorý musí byť pravidelne aktualizovaný tak, aby obsahoval najnovšie definície vírusov.
- Klientsky systém EBICS musí byť nakonfigurovaný tak, aby sa účastník pred jeho použitím musel prihlásiť. Prihlásenie musí vykonať ako bežný používateľ a nie ako administrátor, ktorý je napr. oprávnený vykonávať inštaláciu programov.
- Interné komunikačné IT kanály pre nešifrované bankové údaje alebo pre nešifrované správy EBICS je potrebné chrániť pred zachytávaním údajov a manipuláciou.
- V prípade, že sú k dispozícii aktualizácie týkajúce sa zabezpečenia používaného operačného systému alebo iného softvéru súvisiaceho s bezpečnosťou, používané klientske systémy EBICS by mali byť príslušne aktualizované.

Klient je výlučne zodpovedný za realizáciu týchto požiadaviek.

Príloha 2a: **Rozhranie MCFT**

1. IDENTIFIKAČNÉ A BEZPEČNOSTNÉ POSTUPY

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

V rámci pripojenia prostredníctvom rozhrania MCFT sa používajú nasledujúce identifikačné a bezpečnostné postupy:

- Elektronické podpisy
- Heslo pre diaľkový prenos dát
- Komprimácia Šifrovanie

1.1 Elektronické podpisy

Pri rozhraní MCFT sa v rámci identifikačného postupu využíva elektronický podpis. Definované sú nasledujúce druhy elektronických podpisov:

„E“ = samostatný podpis
„A“ = prvý podpis
„B“ = druhý podpis
„N“ = transportné oprávnenie (len na zaslanie, vyvolanie a inicializáciu)

Program, ktorý používa klient, môže generovať rôzne správy (napr. tuzemské alebo zahraničné platobné príkazy, ale aj správy týkajúce sa inicializácie, stiahnutia protokolu alebo vyvolania informácií o účte a obratoch, atď.). Banková inštitúcia informuje klienta o tom, ktorý typ správy môže použiť a pri ktorých typoch môže použiť elektronický podpis.

Účastník má pre elektronický podpis k dispozícii dvojicu kľúčov, ktorá pozostáva zo súkromného a verejného kľúča. Súkromný kľúč je potrebné chrániť pred neoprávneným prečítaním a zmenami. Verejný kľúč je potrebné bankovej inštitúcii oznámiť v súlade s postupom podľa bodu 2.2. Dvojice kľúčov účastníka je možné využiť aj pri komunikácii s inými bankovými inštitúciami.

1.2 Heslo pre diaľkový prenos dát

Pri využití rozhrania MCFT sa výmena údajov medzi klientom a bankovou inštitúciou zabezpečuje prostredníctvom hesla pre DPD. Každý používateľ na tento účel dostane osobitné heslo, ktoré mu banková inštitúcia oznámi v rámci inicializácie rozhrania MCFT (bod 2.1). Používateľ je povinný toto heslo v priebehu inicializácie zmeniť.

Klient zabezpečí, aby každý používateľ dbal na to, aby žiadna tretia osoba nezískala jeho heslo pre DPD. Každá tretia osoba, ktorá pozná heslo pre diaľkový prístup, môže vykonať výmenu údajov s bankovou inštitúciou.

Ak chce používateľ vykonať výmenu údajov, zadá svoje heslo pre diaľkový prenos dát.

2. INICIALIZÁCIA ROZHRANIA MCFT

2.1 Zriadenie komunikačného spojenia

Banková inštitúcia zašle klientovi pre každého uvedeného používateľa prostredníctvom DPD, poštou alebo e-mailom údaje potrebné na zriadenie spojenia vo forme súboru s bankovými parametrami. Ide pritom o:

- ID klienta
- názov hostiteľa
- IP adresa vrátane čísla portu
- typ hostiteľa
- číslo účastníka
- prvé heslo pre diaľkový prenos dát

Klient načíta súbor s bankovými parametrami pre bankovú inštitúciu do svojho softvéru. Pre každý typ príkazu klient definuje potrebný minimálny počet elektronických podpisov.

Každý používateľ vykoná vo svojom programe zmenu svojho hesla pre diaľkový prenos údajov a vygeneruje kľúče pre elektronické podpisy („INI“).

2.2 Inicializácia kľúčov

Okrem všeobecných podmienok opísaných v bode 1 musí dvojica kľúčov zodpovedať aj týmto požiadavkám:

1. Dvojica kľúčov musí byť priradená výlučne a jednoznačne používateľovi.
2. V prípade, že používateľ svoje kľúče generuje sám, súkromné kľúče musí vygenerovať spôsobom, ktorý je výhradne pod jeho kontrolou.
3. V prípade, že dvojicu kľúčov poskytla tretia strana, je potrebné sa uistiť, že používateľ je jediným vlastníkom súkromného kľúča.
4. Pre používanie súkromného kľúča stanoví každý používateľ heslo, ktoré bude zabezpečovať prístup k súkromnému kľúču.

Inicializácia používateľa v bankovej inštitúcii si vyžaduje prenos verejného kľúča používateľa do systému banky. Na tento účel používateľ zašle svoj verejný kľúč bankovej inštitúcii prostredníctvom dvoch navzájom nezávislých komunikačných kanálov:

- prostredníctvom rozhrania MCFT za pomoci typov príkazov, ktoré systém na tento postup poskytuje,
- prostredníctvom inicializačného listu, ktorý podpísal účastník v súlade s plnou mocou k elektronickému bankovníctvu (príp. potrebný aj druhý podpis) na adresu: Oberbank AG, Electronic Banking Support, resp. mailom na EBSupport_SK@oberbank.sk. Pre aktiváciu používateľa overí banková inštitúcia na základe inicializačného listu podpísaného účastníkom v súlade s plnou mocou k elektronickému bankovníctvu (príp. potrebný aj druhý podpis) pravosť verejného kľúča zaslaného prostredníctvom MCFT.

Pre verejný kľúč musí inicializačný list obsahovať nasledujúce údaje:

- Účel použitia „Elektronický podpis“ verejného kľúča
- Príslušné podporované verzie pre každú dvojicu kľúčov
- Určenie dĺžky exponenta
- Hexadecimálny zápis exponenta verejného kľúča Určenie dĺžky modulu
- Hexadecimálny zápis modulu verejného kľúča
- Hexadecimálny zápis hašovacej hodnoty verejného kľúča

Banková inštitúcia overí podpis účastníka v inicializačnom liste podľa plnej moci k elektronickému bankovníctvu (príp. potrebný aj druhý podpis), ako aj zhodnosť hašovacích hodnôt verejného kľúča používateľa prenášaných prostredníctvom rozhrania MCFT s hodnotami zaslanými písomne faxom. V prípade pozitívneho výsledku banková inštitúcia príslušnému používateľovi aktivuje dohodnuté typy príkazov.

3. ZADÁVANIE PRÍKAZU BANKOVEJ INŠTUTÚCI

3.1 Zadávanie príkazu prostredníctvom elektronického podpisu

Súbory s príkazmi a informácie o účtoch sa medzi klientom a systémom banky posielajú zásadne v zašifrovanej a komprimovanej forme.

Používateľ overí správnosť príkazných údajov a zabezpečí, aby práve tieto údaje boli elektronicky podpísané. Pri nadviazaní komunikácie sa najskôr zašle štartovací blok údajov. Ten obsahuje všetky informácie potrebné na overenie, t. j. ID klienta, č. účastníka, účet na zaťaženie, elektronický podpis a kontrolné súčty k celkovému súboru. Takto je možné zavčasu identifikovať chyby resp. manipulácie a prerušiť samotný prenos údajov.

Príkazy zaslané do bankového systému je možné autorizovať nasledovne:

Ak sa s klientom dohodlo používanie distribuovaného elektronického podpisu pre príslušný typ príkazu a zasielané elektronické podpisy nepostačujú na schválenie, príkaz sa uloží v systéme banky, až kým nebudú použité všetky požadované elektronické podpisy.

V prípade, že sa elektronické podpisy zasielajú prostredníctvom MCFT, štartovací blok obsahuje aj tzv. „odtlačok prsta“ k hlavnému súboru a aj samotný elektronický podpis. Výhodou je to, že elektronické podpisy (pokiaľ boli použité všetky potrebné podpisy), môžu byť overené už počas komunikácie. V štartovacom bloku je možné zaslať až do 6 podpisov.

Ak sa pri kontrole na strane banky zistí, že:

- niektorý podpis v štartovacom bloku nie je správny, diaľkový prenos dát sa pred prenosom hlavného súboru preruší;
- všetky podpisy sú správne, prenesie sa hlavný súbor. Po prenose hlavného súboru sa na strane banky skontroluje „odtlačok prsta“ a porovná sa so správnym odtlačkom zaslaným ako súčasť štartovacieho bloku. V prípade, že sa pri kontrole „odtlačku prstu“ zistí zhoda s prenesenými hodnotami, táto informácia sa systému klienta oznámi v koncovom bloku ako „OK“. V prípade, že kontrolovaný „odtlačok prsta“ nesúhlasí s odtlačkom preneseným v štartovacom bloku, hlavný súbor bude odmietnutý.

Záverečné správy sa odošlú buď pri ukončení komunikácie alebo dialógu. Obsahujú kódy odpovede, ktoré opisujú stav výsledku diaľkového prenosu dát. Kódy odpovede prijaté v systéme klienta sa vyhodnotia a zobrazia v príslušných protokoloch. Okrem toho si klient môže vyvolať protokol klienta, ktorý banková inštitúcia sprístupní s časovým odstupom.

Na vyžiadanie informácií o účte u bankovej inštitúcie je potrebné vytvoriť želané príkazy na vyvolanie a zaslať ich bankovej inštitúcii. Pri tom je potrebné zadať príslušné heslo používateľa na diaľkový prenos dát. Bankový elektronický podpis nie je na vyvolanie informácií potrebný.

3.2 Zadávanie príkazu prostredníctvom distribuovaného elektronického podpisu

S bankovou inštitúciou je potrebné dohodnúť spôsob, akým bude klient používať distribuovaný elektronický podpis.

Distribuovaný elektronický podpis sa používa v prípadoch, keď majú byť príkazy schválené nezávisle od prenosu príkazných údajov a prípadne aj viacerými účastníkmi.

Ak bol príkaz už plne autorizovaný, je možné ho už len odvolať podľa bodu 8 týchto podmienok pre diaľkový prenos dát.

Banková inštitúcia je oprávnená príkazy, ktoré neboli v plnej miere autorizované, vymazať po uplynutí 14-dňovej lehoty.

3.3 Overenie identifikácie zo strany bankovej inštitúcie

Prijatý súbor s príkazom vykoná banková inštitúcia až po prijatí potrebného počtu elektronických podpisov a ich pozitívnom overení.

3.4 Protokoly klienta

V protokoloch klienta dokumentuje banková inštitúcia nasledovné procesy:

- prenos príkazných údajov do systému banky,
- prenos informačných súborov z bankového systému do systému klienta,
- výsledok všetkých overení identifikácie pre príkazy od klienta pre bankový systém,
- ďalšie spracovanie príkazov, ak sa týkajú overenia podpisov a zobrazenia príkazných údajov,
- chyby pri dekomprimácii.

Používateľ je povinný sa informovať o výsledku overenia, ktoré vykonala banková inštitúcia a to prostredníctvom vyvolania protokolu klienta.

Účastník je povinný tento protokol zahrnúť do svojich podkladov a na žiadosť ho predložiť bankovej inštitúcii.

4. ZMENA KĽÚČA POUŽÍVATEĽA

4.1 Zmena kľúča s automatickou aktiváciou

V prípade, že si používateľ generuje kľúče sám, musia byť tieto účastnícke kľúče obnovené za pomoci typov príkazov, ktoré na tento účel poskytuje systém v deň dohodnutý s bankovou inštitúciou. Okrem toho musia byť kľúče odoslané zavčasu pred uplynutím platnosti starých kľúčov.

Pri automatickej aktivácii nového kľúča bez obnovenia inicializácie účastníka sa použije tento typ príkazov:
-Aktualizácia verejného kľúča (PUB)

Typ príkazu PUB si na tento účel vyžaduje platný elektronický podpis užívateľa. Po úspešnej zmene sa musí používať už len nový kľúč.

Ak nebolo možné pozitívne overiť elektronický podpis, postupuje sa podľa ustanovení bodu 6.3 týchto podmienok pre DPD.

Kľúče je možné zmeniť až po spracovaní všetkých príkazov. V opačnom prípade bude potrebné zadať ešte nespracované príkazy znovu za pomoci nového kľúča.

4.2 Zmena kľúčov s novou inicializáciou

Prostredníctvom diaľkového prenosu dát môže používateľa nahradiť svoju doterajšiu dvojicu kľúčov zaslaním nového verejného kľúča (typ príkazu „PUB“). Nová dvojica kľúčov bude v bankovej inštitúcii aktivovaná až po prijatí (faxom) k tomu vygenerovaného príslušného inicializačného protokolu. Až potom je možné vykonávať príkazy podpísané novým kľúčom.

Po aktivácii nového verejného kľúča v bankovej inštitúcii je potrebné príkazy, ktoré ešte neboli zaslané bankovej inštitúcii, znovu overiť pomocou novej dvojice kľúčov a zaslať bankovej inštitúcii.

5. ZABLOKOVANIE KĽÚČA POUŽÍVATEĽA

V prípade podozrenia zo zneužitia kľúča je používateľ povinný zablokovať svoje prístupové oprávnenie ku všetkým bankovým systémom, pri ktorých sa využíva kompromitovaný kľúč.

V prípade, že používateľ už nemá k dispozícii platné identifikačné médiá, môže bankovú inštitúciu požiadať o zablokovanie identifikačného a bezpečnostného média aj mimo postupu diaľkového prenosu dát.

Ďalšie informácie o zablokovaní ako aj odblokovaní sú uvedené v bode 5 týchto podmienok pre DPD.

Príloha 2b: **Bezpečnostné požiadavky pre klientsky systém MCFT**

Okrem bezpečnostných opatrení opísaných v prílohe 2a, musí klient dodržiavať aj nasledujúce požiadavky:

- Softvér, ktorý klient používa pri postupe MCFT musí zodpovedať požiadavkám opísaným v prílohe 2a.
- Klientsky systém MCFT nesmie byť používaný bez firewallu. Firewall je aplikácia, ktorá sleduje všetky prichádzajúce a odchádzajúce správy a povoľuje len známe alebo autorizované spojenia
- Je potrebné nainštalovať antivírusový program, ktorý musí byť pravidelne aktualizovaný tak, aby obsahoval najnovšie definície vírusov.
- Klientsky systém MCFT musí byť nakonfigurovaný tak, aby sa účastník pred jeho použitím musel prihlásiť.
- Prihlásenie musí vykonať ako bežný používateľ a nie ako administrátor, ktorý je napr. oprávnený vykonávať inštaláciu programov. Interné komunikačné IT kanály pre nešifrované bankové údaje alebo pre nešifrované správy MCFT je potrebné chrániť pred zachytávaním údajov a manipuláciou.
- V prípade, že sú k dispozícii aktualizácie týkajúce sa zabezpečenia používaného operačného systému alebo iného softvéru súvisiaceho s bezpečnosťou, používané klientske systémy MCFT by mali byť príslušne aktualizované.

Klient je výlučne zodpovedný za realizáciu týchto požiadaviek.

Príloha 3: **Štruktúra a špecifikácia súborov s platobnými príkazmi**

Ohľadom štruktúry a špecifikácie súborov so SEPA a zahraničnými príkazmi je potrebné používať najaktuálnejšiu verziu podľa príslušných noriem.

Príloha 4: **Postúpenie údajov v prípade zmeny formátu**

V prípade, že banka nie je schopná vykonať prevod, ktorý klient zadal prostredníctvom diaľkového prenosu dát - prevodného príkazu vo formáte „SEPA prevod“ ako prevod v tomto formáte preto, že poskytovateľ platobných služieb príjemcu platby, ktorého klient uviedol, tento formát ešte nepodporuje, a v prípade, že banka takýto prevodný príkaz neodmietne, vykoná banka tento prevod v jednom z formátov, ktorý poskytovateľ platobných služieb príjemcu platby podporuje.

1. Pri zmene formátu nie je možné zasielať nasledujúce dátové prvky*:

   - Odlišný príjemca platby (Payment Information „Credit Transfer Transaction Information“ Ultimate Creditor)
   - Odlišný platiteľ (Payment Information „Ultimate Debtor und Payment Information“ Credit Transfer Transaction Information“ Ultimate Debtor)
   - Identifikácia príjemcu platby (Payment Information „Credit Transfer Transaction Information“ Creditor " Identification) Identifikácia platiteľa (Payment Information „Debtor“ Identification)

2. Pri zmene formátu je možné zasielať nasledujúce dátové prvky len čiastočne*:

   - Adresa príjemcu platby (Payment Information „Credit Transfer Transaction Information“ Creditor " Postal Address) [prenáša sa prvých 66 z pôvodne možných 140 znakov]
   - Adresa platiteľa (Payment Information „Debtor“ Postal Address) [prenáša sa prvých 66 z pôvodne možných 140 znakov]
   - Názov príjemcu platby (Payment Information „Credit Transfer Transaction Information“ Creditor " Name) [prenáša sa prvých 66 z pôvodne možných 70 znakov]
   - Názov platiteľa (Payment Information „Debtor“ Name) [prenáša sa prvých 66 z pôvodne možných 70 znakov]
   - Účel použitia (Payment Information „Credit Transfer Transaction Information“ Remittance Information) [Referencia klienta a účel použitia sa prenášajú spolu, nemôžu však dohromady mať viac ako 130 znakov. Referencia klienta (End to End Identification) sa tu uvádza ako prvá a vždy v plnom rozsahu.]

(*Zoznamy, uvedené v bode 1 a 2 platia len pri uplatnení „Translation Rules MX pacs.008.001.01 to MT 103“ z júna 2007)