Podmínky pro zpracování bankovních operací prostřednictvím portálu firemního bankovnictví a služby HBCI/FinTS

(Stav k 30. září 2016)

1. Rozsah služeb

1) Klient může používat portál firemního bankovnictví a provádět bankovní operace v rozsahu nabízeném bankou. Provedení transakcí podléhá podmínkám pro příslušné bankovní operace (například Všeobecné podmínky pro poskytování platebních služeb). Klient má rovněž přístup k informacím od banky.

2) Klient a oprávněná osoba budou dále v tomto dokumentu označováni jako „**účastník**“ nebo „**uživatel**“. Tento termín podle Podmínek pro dálkový přenos dat zahrnuje také „**uživatele**“, který používá dálkový přenos dat zpřístupněný prostřednictvím firemního portálu banky. Účet a vklad jsou dále označovány jako „**účet**“.

3) Klient a banka se mohou dohodnout na zvláštních limitech pro limity určitých služeb.

2. Nezbytné podmínky pro používání portálu firemního bankovnictví a služby HBCI/FinTS

Provedení bankovních operací vyžaduje, aby účastník/uživatel prokázal svou totožnost jako oprávněný účastník/uživatel (viz bod č. 3) a autorizoval příkazy (viz bod č. 4) prostřednictvím individuálních bezpečnostních prvků a ověřovacích nástrojů dohodnutých s bankou. Každý účastník/uživatel se může s bankou dohodnout na tom, jaký individuální bezpečnostní prvek a ověřovací nástroj bude používat.

2.1 Individuální bezpečnostní prvky

Individuální bezpečnostní prvky, které mohou být také v alfanumerické podobě, jsou:

- osobní identifikační číslo (PIN),
- jednorázové autorizační číslo operace (photoTAN)
- podpisový PIN a data osobního elektronického klíče pro elektronický podpis.

2.2 Ověřovací nástroje

PhotoTAN může být účastníkovi/uživateli vygenerován a zpřístupněn prostřednictvím mobilního nebo čtecího zařízení. Účastník/uživatel může k autorizaci operací používat i další ověřovací nástroje:

- čipovou kartu s podpisovou funkcí nebo
- jiný ověřovací nástroj obsahující klíč včetně uložení elektronického podpisového klíče v technickém prostředí poskytnutém bankou (nebo poskytovatelem služeb schváleným bankou), které je chráněno proti neoprávněnému přístupu,
- softwarovou aplikaci, kterou banka pro účastníka/uživatele personalizuje v procesu počátečního nastavení programu.

3. Přístup k portálu firemního bankovnictví

Účastníku/uživateli je umožněn přístup do portálu firemního bankovnictví, pokud

- účastník/uživatel obdržel účastnické číslo / registrační jméno a PIN,
- ověření tohoto údaje bankou prokázalo, že účastník/uživatel má oprávnění k přístupu a
- přístup nebyl zablokován (viz bod 9.1 a 10). Poté, co mu byl umožněn přístup do portálu firemního bankovnictví, může účastník/uživatel vyhledat informace nebo zadat příkazy.

4. Provedení příkazů

4.1 Zadání příkazů a autorizace

Autorizace realizování jednotlivých operací (například kreditní převod, termínované vklady) proběhne podle zvoleného typu služby sjednaného individuálními bezpečnostními prvky, tj.:

- photoTAN,
- podpisový PIN.

4.2 Dodatečná nařízení pro dálkový přenos dat ve standardu EBICS při používání postupu photoTAN

4.2.1 Klient instruuje banku, aby uložila osobní klíč účastníka/uživatele v technickém prostředí, které je chráněno proti neoprávněnému přístupu. Banka musí také zajistit náležité poučení spolehlivého poskytovatele služeb. Kódové slovo nutné k autorizaci osobního klíče musí být v postupu photoTAN nahrazeno heslem TAN.

4.2.2 Podmínky pro dálkový přenos dat se doplňují takto:

- V článku 4, odstavec 2 Podmínek pro dálkový přenos dat se povoluje uložení elektronického klíče v technickém prostředí poskytnutém bankou (nebo poskytovatelem služeb schváleným bankou) (viz článek 2.1.1, odst. 5 Přílohy 1a Podmínek pro dálkový přenos dat).
- V článku 7, odstavec 3 se sjednává, že banka může ověřit, zda bylo zadáno správné photoTAN.

4.2.3 Příloha 1a Podmínek pro dálkový přenos dat se doplňují takto:

- Ověřovací podpis v bodě 1.2 může být poskytnut také ve formě photoTAN v technickém prostředí banky nebo oprávněného poskytovatele služeb. Banka, popř. poskytovatel služeb, provede nutné ověření klienta.
- K článku 2.2 odstavec 5 se sjednává, že místo kódového slova se použije photoTAN, pokud banka uložila bezpečnostní médium účastníka v technickém prostředí, které je chráněno proti neoprávněnému přístupu.
- Autorizace příkazů v souladu s článkem 3 může být poskytnuta zadáním photoTAN, které se zobrazí na mobilním nebo čtecím zařízení, a elektronickým podpisem následně vygenerovaným v bezpečném technickém prostředí.
- V případě rozděleného elektronického podpisu podle článku 3.1 odstavec 1 může souhlas a autorizace druhým bankovním podpisem proběhnout použitím photoTAN nebo autorizací příkazu s použitím softwarové aplikace poskytnuté bankou.

4.3 Odvolání příkazů

Odvolatelnost příkazu se řídí zvláštními podmínkami platnými pro příslušný typ příkazu. Příkazy je možné odvolat mimo portál firemního bankovnictví a služby HBCI/FinTS, pokud banka výslovně neposkytne možnost příkaz odvolat na portálu firemního bankovnictví nebo ve službě HBCI/FinTS.

5. Zpracování příkazů bankou

1) Příkazy zadané v rámci portálu firemního bankovnictví se zpracovávají podle nařízení platných pro zpracování příslušného typu příkazu (například převod nebo příkaz týkající se cenných papírů).

2) Platební příkazy (převody, přímé inkaso) se řídí zvláštními nařízeními uvedenými dále. Banka provede příkaz, pokud budou splněny následující podmínky:
   - účastník/uživatel prokázal svou totožnost prostřednictvím svého individuálního bezpečnostního prvku,
   - byla ověřena autorizace účastníka/uživatele pro příslušný typ příkazu,
   - je dodržen datový formát pro sjednaný typ služby,
   - není překročen samostatně sjednaný limit čerpání pro typ služby nebo standardní limit,
   - jsou splněny nezbytné podmínky pro provedení příkazu podle příslušných zvláštních podmínek platných pro příslušný typ příkazu,
   - na účtu je k dispozici dostatečné krytí (kreditní zůstatek nebo poskytnutý úvěr).

   Pokud budou dodrženy nezbytné podmínky pro provedení příkazu podle věty 1 výše, banka platební příkaz provede. Toto provedení nesmí být v rozporu s jakýmikoliv jinými zákonnými ustanoveními.

3) Pokud nebudou splněny nezbytné podmínky pro provedení příkazu podle odstavce 2, věta 1, odrážky 1–5 výše, banka platební příkaz neprovede. Banka bude

účastníka/uživatele informovat online nebo jiným způsobem o neprovedení příkazu a, pokud to bude možné, o důvodech neprovedení a také o možnostech opravy chyb, které neprovedení příkazu způsobily. Toto ustanovení neplatí, pokud je oznámení důvodů v rozporu s jakýmkoliv jiným zákonným ustanovením. Pokud banka provede příkaz v případě nedostatečného krytí na účtu, vznikne povolené přečerpání, které bude podléhat zvýšené úrokové sazbě.

6. Oznámení klientovi o pohybech

Banka oznámí klientovi pohyby provedené prostřednictvím portálu firemního bankovnictví nebo služby HBCI/FinTS ve formě sjednané pro informace o účtu a v souladu s podmínkami platnými pro příkaz.

7. Povinnosti účastníka/uživatele

7.1 Technické připojení

Účastník/uživatel je povinen zřídit si technické připojení k portálu firemního bankovnictví pouze prostřednictvím přístupových kanálů portálu firemního bankovnictví (například internetové adresy) sdělených samostatně bankou. Klient odpovídá za zálohování příslušných dat pro své vlastní systémy a za přijetí dostatečných preventivních opatření proti virům a jiným škodlivým programům (například trojský kůň, červ atd.) a aktualizování těchto systémů. Softwarové aplikace banky je možné získat od poskytovatele aplikace, kterého banka sdělí klientovi. Klient odpovídá za dodržování specifických ustanovení pro užívání internetu v dané zemi.

7.2 Uchovávání individuálních bezpečnostních prvků v tajnosti a pečlivé bezpečné uložení ověřovacích nástrojů

1) Účastník/uživatel musí
   - uchovávat v tajnosti své individuální bezpečnostní prvky (viz článek 2.1) a přeposílat je do banky pouze prostřednictvím přístupových kanálů portálu firemního bankovnictví sdělených bankou samostatně nebo prostřednictvím softwarových aplikací vydaných bankou a
   - uchovávat svůj ověřovací nástroj v bezpečí (viz článek 2.1), aby zabránil třetím osobám k jeho přístupu.

   Toto opatření má zabránit tomu, aby žádná osoba, která vlastní ověřovací nástroj, nemohla zneužít portál firemního bankovnictví v kombinaci se souvisejícím individuálním bezpečnostním prvkem.

2) Na ochranu individuálního bezpečnostního prvku a ověřovacího nástroje je třeba především dodržovat dále uvedené body:
   - Individuální bezpečnostní prvek PIN a podpisový PIN nesmí účastník/uživatel uchovávat elektronicky (například v systému klienta). Osobní elektronický klíč vygenerovaný účastníkem/uživatelem bude výhradně pod kontrolou účastníka/uživatele nebo v technickém prostředí zpřístupněném bankou (nebo

poskytovatelem služby pověřeným bankou), které je chráněno proti neoprávněnému přístupu.

- Pokud se během plně automatizovaného přenosu dat používá „technický uživatel“, musí být elektronicky uložený podpis veden v bezpečném a přiměřeně vhodném technickém prostředí. „Technický uživatel“ není oprávněn autorizovat příkazy. Může pouze připravovat příkazy.
- Při zadávání individuálního bezpečnostního prvku musí být zajištěno, že se ho nemůže zmocnit žádná jiná osoba.
- Individuální bezpečnostní prvky nesmí být zadávány mimo samostatně sjednané internetové stránky nebo softwarové aplikace než ty, které vlastní banka (například nikoliv na internetové stránky obchodníků).
- Individuální bezpečnostní prvky nesmí být přenášeny mimo portál firemního bankovnictví nebo službu HBCI/FinTS, například nikoliv e-mailem.
- Podpisový PIN pro elektronický podpis nesmí být uchováván společně s ověřovacím nástrojem.
- Pro autorizaci příkazu nesmí účastník/uživatel použít více než jeden photoTAN.

7.3 Zabezpečení systému klienta

Účastník/uživatel musí dodržovat bezpečnostní upozornění na internetových stránkách banky, především opatření k ochraně používaného hardwaru a softwaru, a instalovat aktuální stávající antivirovou ochranu a ochranné systémy (firewalls). Především nesmí upravovat nebo deaktivovat operační systém a bezpečnostní opatření mobilního zařízení.

7.4 Ověření údajů na příkazu prostřednictvím údajů zobrazených bankou

Pokud banka zobrazí účastníkovi/uživateli k potvrzení údaje obsažené v jeho příkazu na portálu firemního bankovnictví (například účet, číslo účtu příjemce, identifikační číslo cenných papírů) v systému klienta nebo prostřednictvím jiného zařízení účastníka/uživatele (například photoTAN čtečka, photoTAN aplikace), je účastník/uživatel povinen před potvrzením transakce ověřit, zda zobrazené údaje odpovídají údajům zamýšlené operace.

7.5 Další povinnosti klienta

Klient musí zajistit, aby byly povinnosti klienta vyplývající z této smlouvy dodržovány také jeho oprávněnými osobami (tj. všemi účastníky/uživateli).

8. Šifrovací technologie v zahraničí

V zemích, kde existuje omezení používání nebo importní a exportní omezení týkající se šifrovacích technik, nesmí být použit online přístup, který banka umožňuje. V případě potřeby musí účastník zařídit nutná povolení, oznámení nebo se musí postarat, aby byla přijata další nutná opatření. Účastník musí banku informovat o zákazech, povinnostech získat povolení a o oznamovacích povinnostech, o kterých se dozví.

9. Oznamovací a informační povinnost

9.1 Žádost o zablokování

1) Pokud účastník/uživatel zjistí
   - ztrátu nebo krádež ověřovacího nástroje,
   - zneužití nebo
   - jiné neoprávněné použití svého ověřovacího nástroje nebo individuálního bezpečnostního prvku, sdělí tuto skutečnost neprodleně bance. Účastník/uživatel může banku požádat o zablokování prostřednictvím oddělení klientské podpory v úředních hodinách.

2) Účastník/uživatel musí policii bez zbytečného prodlení nahlásit jakoukoliv krádež nebo zneužití.

3) Pokud má účastník/uživatel podezření, že nějaká jiná osoba
   - získala do vlastnictví jeho ověřovací nástroj, a to neoprávněně, nebo jinak získala povědomí o jeho individuálním bezpečnostním prvku nebo
   - použila ověřovací nástroj nebo individuální bezpečnostní prvek, musí rovněž požádat o zablokování.

9.2 Oznámení o neautorizovaných nebo nesprávně provedených příkazech

Klient bude banku informovat o neautorizovaném nebo nesprávně provedeném příkazu okamžitě poté, co to zjistí.

10. Blokování přístupu

10.1 Zablokování přístupu na žádost účastníka/uživatele

Na žádost účastníka/uživatele, především v případě žádosti o zablokování podle článku 9.1 výše, banka zablokuje:
- danému účastníku/uživateli přístup na portál firemního bankovnictví a, pokud o to účastník/uživatel požádá, přístup pro všechny účastníky/uživatele klienta nebo
- ověřovací nástroj účastníka/uživatele.

10.2 Zablokování přístupu na žádost banky

1) Banka může účastníku/uživateli zablokovat přístup na portál firemního bankovnictví, pokud
   - je banka z podstatného důvodu oprávněna vypovědět Smlouvu o spolupráci v oblasti Commerzbank Transaction Services,
   - je k tomu oprávněna z objektivních důvodů v souvislosti se zabezpečením ověřovacího nástroje nebo individuálního bezpečnostního prvku nebo
   - existuje podezření z neoprávněného nebo podvodného použití ověřovacího nástroje nebo individuálního bezpečnostního prvku.

2) Pokud to bude možné, sdělí banka klientovi příslušné důvody pro zablokování přístupu předtím, než bude přístup zablokován, ale nejpozději bezprostředně po zablokování.

10.3 Odblokování přístupu

Banka odblokuje přístup nebo změní individuální bezpečnostní prvek nebo ověřovací nástroj, pokud již dále neplatí důvody pro zablokování přístupu. Banka bude klienta o této skutečnosti neprodleně informovat.

10.4 Automatické zablokování

1) Čipová karta s podpisovou funkcí se zablokuje, pokud byl podpisový PIN pro elektronický podpis zadán třikrát po sobě nesprávně. Čipovou kartu nemůže banka odblokovat.

2) Přenášený podpis se zablokuje, pokud byl podpisový PIN pro elektronický podpis zadán třikrát po sobě nesprávně. Účastník/uživatel musí vygenerovat nový elektronický podpis, přeposlat jej znovu do banky a vypořádat jej s bankou inicializačním dopisem („INI-Brief“).

3) PIN se zablokuje, pokud byl zadán třikrát po sobě nesprávně.

4) Účastníkovi bude zablokováno používání photoTAN, pokud bude TAN zadán pětkrát po sobě nesprávně.

5) Účastník/uživatel může kontaktovat banku za účelem obnovení funkčnosti firemního klientského portálu. Banka bude klienta neprodleně informovat o zablokování účtu a sdělí mu důvody tohoto kroku, ledaže by tím byla porušena objektivně oprávněná bezpečnostní kritéria nebo by to představovalo porušení zákonů Evropské unie nebo mezinárodních nařízení nebo úředních soudních nebo administrativních příkazů.

11. Odpovědnost při používání individuálních bezpečnostních prvků anebo ověřovacích nástrojů

11.1 Odpovědnost klienta za neautorizované platební operace před podáním žádosti o zablokování

1) Pokud budou před podáním žádosti o zablokování provedeny neautorizované platební operace v důsledku použití ověřovacího nástroje, který se ztratil nebo byl odcizen nebo se jinak postrádá, nebo v důsledku zneužití individuálního bezpečnostního prvku nebo ověřovacího nástroje, bude klient odpovědný za ztrátu vzniklou bance, pokud ztrátu, krádež nebo nedostupnost nebo zneužití individuálního bezpečnostního prvku nebo ověřovacího nástroje zavinil účastník/uživatel. Klient bude rovněž odpovědný, pokud nebyl pečlivý při výběru kteréhokoliv ze svých jmenovaných účastníků anebo pokud pravidelně neprověřoval, zda účastníci dodržují povinnosti podle těchto podmínek. Pokud ke vzniku ztráty přispěla svým vlastním pochybením banka, podle principů nedbalostního spoluzavinění bude stanoven rozsah ztráty, kterou banka a klient ponesou.

2) Klient nebude odpovědný za náhradu ztráty podle odstavce 1 a 2 výše, pokud nebyl účastník/uživatel schopen podat žádost o zablokování podle článku 9.1, protože banka nezajistila, aby mohla žádost o blokaci obdržet, a ztráta vznikla v důsledku tohoto selhání.

3) Odpovědnost za ztráty způsobené během období, na které se vztahuje standardní limit nebo limit čerpání prostřednictvím portálu firemního bankovnictví sjednaný s klientem, bude omezena na výši příslušného limitu.

11.2 Odpovědnost za neautorizované platební transakce nebo za jiné typy služeb před podáním žádosti o zablokování

Pokud dojde před podáním žádosti o zablokování k neautorizovaným platebním operacím pro sjednaný typ služby v důsledku použití ověřovacího nástroje, který se ztratil nebo byl odcizen nebo se jinak postrádá, nebo v důsledku zneužití individuálního bezpečnostního prvku nebo ověřovacího nástroje a banka tímto utrpěla ztrátu, bude klient odpovídat za výslednou ztrátu vzniklou bance, pokud ztrátu, krádež nebo zneužití individuálního bezpečnostního prvku nebo ověřovacího nástroje zavinil účastník/uživatel. Klient bude rovněž odpovědný, pokud nebyl pečlivý při výběru kteréhokoliv ze svých jmenovaných účastníků anebo pokud pravidelně neprověřoval, zda účastníci dodržují povinnosti podle těchto podmínek. Pokud ke vzniku ztráty přispěla svým vlastním pochybením banka, podle principů nedbalostního spoluzavinění bude stanoven rozsah ztráty, kterou banka a klient ponesou.

11.3 Odpovědnost banky po podání žádosti o zablokování

Jakmile banka obdrží žádost účastníka/uživatele o zablokování, ponese veškeré ztráty vzniklé po datu žádosti o zablokování vyplývající z neoprávněného čerpání. Toto ustanovení neplatí, pokud účastník/uživatel jednal s podvodným úmyslem.

12. Dostupnost

Banka se bude snažit, aby byly poskytované služby k dispozici v co nejširším možném rozsahu. Nezahrnuje to však zaručenou dostupnost. Především technické problémy, problémy s údržbou a sítěmi (například nedostupnost serveru třetí strany), nad nimiž nemá banka žádnou kontrolu, mohou způsobit občasné přerušení, které brání přístupu.

13. Odkazy na internetové stránky třetí strany

Pokud internetová stránka poskytuje přístup na webové stránky třetí strany, má tento přístup klientovi a uživateli umožnit snadnější přístup k informacím na internetu. Obsah těchto stránek nepředstavuje žádné interní stanovisko banky a není bankou kontrolován.

14. Užívací práva

Tato smlouva nedovoluje klientovi vytvářet odkazy nebo rámcové odkazy na webové stránky banky bez jejího předchozího písemného souhlasu. Klient se tímto zavazuje používat internetové stránky a jejich obsah pouze pro své vlastní účely. Klient především nemá právo bez souhlasu banky zpřístupňovat jejich obsah třetím stranám, zahrnovat je do jiných produktů nebo postupů nebo dešifrovat zdrojový kód jednotlivých internetových stránek. Klient nesmí odstranit nebo učinit nečitelnými oznámení o právech banky nebo třetích stran. Klient nebude používat názvy značek, názvy domén nebo jiné obchodní známky banky nebo třetích stran bez předchozího souhlasu banky. Podle těchto podmínek klient neobdrží žádná neodvolatelná, výlučná nebo převoditelná užívací práva.

15. Klientská podpora („Help Desk“)

Pro zpracování technických a provozních dotazů a dotazů ohledně funkčnosti poskytovaných služeb banka zřídí linku telefonické podpory. Banka zajistí obsluhování linky telefonické podpory v úředních hodinách banky v bankovních dnech platných pro český bankovní trh. Telefonní čísla a provozní doba budou sděleny běžnými informačními kanály (například www.commerzbank.cz, sekce Kontakt).

16. Různé

1) V zájmu řádné spolupráce si banka tímto vyhrazuje právo provádět změny technické nebo organizační povahy na základě obecné, standardní úpravy v technických standardech, ve specifikacích platných pro bankovnictví a v zákonných nebo regulatorních ustanoveních. Pokud jde o významné technické nebo organizační úpravy, které překročí tento rámec a budou mít významný dopad na práva a povinnosti klienta nebo banky, bude banka o těchto úpravách klienta informovat nejméně dva měsíce před navrhovaným datem, kdy mají úpravy vstoupit v platnost. Platí, že klient návrh změn přijal, jestliže klient před navrhovaným okamžikem účinnosti změny písemně neodmítne. Na tento důsledek jej banka ve svém návrhu zvlášť upozorní. Budou-li klientovi navrženy změny těchto obchodních podmínek, může Smlouvu o

spolupráci v oblasti Commerzbank Transaction Services, které se tato změna dotkne, před navrhovaným okamžikem účinnosti změn také okamžitě a bezplatně vypovědět. Na toto právo výpovědi jej banka ve svém návrhu zvlášť upozorní.

3) Pokud by tato smlouva obsahovala mezeru nebo pokud by se některé ustanovení této smlouvy stalo neplatným nebo nevymahatelným, neovlivní tato skutečnost platnost zbývajících ustanovení. V takovém případě smluvní strany tímto sjednávají, že se dohodnou na platném nebo vymahatelném ustanovení, které bude svým duchem a účelem co možná nejblíže ustanovení, které má být nahrazeno.

Commerzbank AG