Raiffeisen BANK
Banka inspirovaná klienty

PRODUKTOVÉ PODMÍNKY SLUŽEB PŘÍMÉHO BANKOVNICTVÍ

(dále také jen „Produktové podmínky")

1. Dostupnost Služeb přímého bankovnictví

1.1. Služby přímého bankovnictví jsou poskytovány na základě Smlouvy o službách uzavřené mezi Klientem a Bankou. Smlouva o službách může být rovněž součástí ujednání o jiných službách poskytovaných Bankou Klientovi. ~~Smlouva o službách je sjednávána v souvislosti s dalšími Bankovními službami poskytovanými Bankou Klientovi.~~ Po dobu, kdy Banka Klientovi poskytuje jiné Bankovní služby, nelze závazky ze Smlouvy o službách samostatně ukončit nebo zrušit. Toto ujednání je stanovením vzájemné závislosti služeb poskytovaných Bankou, na které odkazují některé Smlouvy uzavřené mezi Bankou a Klientem. V případě, že Banka neposkytuje Klientovi žádné Bankovní služby kromě Služeb přímého bankovnictví, může Klient Služby přímého bankovnictví nadále využívat, především za účelem přístupu k informacím a dokumentům předaným prostřednictvím Služeb přímého bankovnictví. Pakliže Banka neposkytuje Klientovi jiné Bankovní služby a Uživatel se po dobu 6 měsíců k některé Službě přímého bankovnictví nepřihlásí, je Banka oprávněna prostředky a údaje pro přístup ke Službám přímého bankovnictví takovému Uživateli zablokovat. Pokud lze závazky ze Smlouvy o službách vypovědět, může tak Banka učinit ve výpovědní době 2 měsíců, není-li ve výpovědi stanovena doba delší a Klient ve výpovědní době 14 dnů. ~~závazky sjednané Smlouvou o službách zanikají, a to ke dni, kdy Banka přístup ke Službám přímého bankovnictví Klientovi ukončí. Banka tak učiní v přiměřené době po zjištění, že Klientovi jsou dostupné Služby přímého bankovnictví, ačkoliv mu již jiné Bankovní služby poskytovány nejsou.~~ Po dobu trvání závazků ze Smlouvy o službách je Klient oprávněn požádat Banku o poskytnutí obsahu Smlouvy o službách a o informace, které je mu Banka povinna poskytnout před jejím uzavřením.

1.2. V případě, že ke Službám přímého bankovnictví přistupuje jménem Klienta jiný Uživatel, určuje Klient rozsah jeho oprávnění prostřednictvím Podpisového vzoru. Podpisový vzor může být výslovně označen jiným způsobem, například jako protokol o nastavení přístupových práv. Zajištění dostupnosti některých Služeb přímého bankovnictví pak vyžaduje kromě uzavření Smlouvy o službách rovněž další součinnost Banky a Klienta či Uživatele. Ke zřízení, změně a zrušení Podpisového vzoru je oprávněn Klient, jiná osoba pak na základě oprávnění uděleného Podpisovým vzorem nebo plnou mocí s úředně ověřeným podpisem Klienta nebo podpisem Klienta učiněným před pracovníkem Banky.

1.3. Při sjednání Služeb přímého bankovnictví Banka určí Uživateli Klientské číslo pro přihlášení ke Službám přímého bankovnictví, případně si jej Uživatel zvolí.

1.4. Klient určí, jaký Elektronický klíč bude Uživatel používat. Dle zvoleného Elektronického klíče poskytne Banka pro jeho získání a užívání potřebnou součinnost. Zpravidla je potřebná také součinnost Uživatele či rovněž Klienta. ~~Pokud určí Mobilní Elektronický klíč, Banka zajistí registraci telefonního čísla Mobilního zařízení Uživatele v systému Banky. Pokud určí Osobní Elektronický klíč (OEk), Banka ho vydá Uživateli. Pokud určí Smartphone Elektronický klíč, Banka zpřístupní Uživateli možnost aktivace Mobilního bankovnictví v Internetovém bankovnictví na základě společného Pokynu Klienta a Uživatele.~~

1.5. Podmínkou využívání Internetového bankovnictví je přístup Uživatele k počítači připojenému k internetu, zároveň musí být Uživatel držitelem Mobilního zařízení aktivovaného v síti libovolného Mobilního operátora. ~~případně Mobilního zařízení aktivovaného v síti Mobilního operátora poskytujícího služby elektronických komunikací v ČR a zajišťujícího službu GSM SIM Toolkit, a SIM karty podporující GSM SIM Toolkit společně s údaji BPIN a BPUK dodanými Mobilním operátorem.~~

1.6. Podmínkou aktivace a využívání Mobilního bankovnictví je, aby Uživatel splňoval předpoklady pro přístup k Internetovému bankovnictví a byl držitelem Mobilního zařízení s operačním systémem iOS nebo Android a připojením k internetu.

1.7. Pro využívání Telefonního bankovnictví je třeba, aby byl Uživatel držitelem Mobilního zařízení aktivovaného v síti libovolného Mobilního operátora. ~~, případně Mobilního zařízení aktivovaného v síti Mobilního operátora poskytujícího služby elektronických komunikací v ČR a zajišťujícího službu GSM SIM Toolkit, a SIM karty podporující GSM SIM Toolkit společně s údaji BPIN a BPUK dodanými Mobilním operátorem.~~

2. Rozsah Služeb přímého bankovnictví

2.1. Služby přímého bankovnictví představují soubor Internetového, Telefonního a Mobilního bankovnictví, který slouží především jako komunikační prostředek Banky a Klienta o stávajících službách Banky poskytovaných Klientovi, budoucích službách a podmínkách jejich poskytování včetně sjednávání smluv, dále jako doručovací místo pro zprávy nebo právní jednání Banky adresované Klientovi a komunikační prostředek pro předávání Klientových Pokynů či Pokynů ke smlouvě Bance. Rozsah Internetového, Telefonního a Mobilního bankovnictví dostupný Klientovi je přitom také závislý na dalších službách poskytovaných Bankou Klientovi. V případě Uživatele, který zároveň není Klientem, je pak rozsah Služeb přímého bankovnictví dostupný Uživateli vymezen Klientem prostřednictvím Podpisového vzoru.

2.2. Banka průběžně vyvíjí a upravuje služby a jejich funkce dostupné prostřednictvím Služeb přímého bankovnictví. Kromě jiného také za účelem zvýšení bezpečnosti vzájemné komunikace vyvíjí a přijímá potřebná opatření, jež mohou ovlivnit dostupnost Služeb přímého bankovnictví či přístup Klienta ke Službám přímého bankovnictví nebo způsob, jakým Klient Služby přímého bankovnictví využívá. Vyžaduje-li to povaha nově zařazených služeb, odebraných služeb nebo upravených funkcí služeb, Banka o přijatých opatřeních Klienta informuje Vhodným způsobem.

2.3. Klient je srozuměn s tím, aby byly Služby přímého bankovnictví použity jako prostředek komunikace na dálku za účelem uzavírání Smluv. Smlouvy, které musí být uzavřeny v písemné formě, budou opatřeny Elektronickým podpisem Banky a Uživatele. Smlouvou se pro účely tohoto ustanovení Produktových podmínek může rozumět také jen návrh Smlouvy nebo přijetí návrhu Smlouvy. Smlouva uzavřená prostřednictvím Služeb přímého bankovnictví v písemné formě je Bankou archivována a na žádost Klienta mu její znění bude poskytnuto; uzavřená Smlouva je pak rovněž zpravidla prostřednictvím Internetového bankovnictví dostupná Uživateli. Klient a Banka se dohodli, že návrh Smlouvy či jeho přijetí mohou být Bankou doručeny Klientovi rovněž prostřednictvím Služeb přímého bankovnictví. Příslušná aplikace Služeb přímého bankovnictví je pak pro

tyto účely korespondenční adresou Klienta; Banka může Klientovi zaslat příslušnou reakci (například odmítnutí či přijetí návrhu) jinou Službou přímého bankovnictví, než kterou ji Klient kontaktoval (např. přijetí návrhu Smlouvy, jenž Klient podal pomocí Mobilního bankovnictví, může být Klientovi doručeno pomocí Internetového bankovnictví), nebo zcela odlišným komunikačním prostředkem.

2.4. Autentizační či Certifikační kód nebo Mobilní klíč může být v souvislosti s poskytováním služeb Bankou Klientovi použit rovněž ve vybraných situacích (například při výběru hotovosti) při jednání Klienta a Banky na Obchodním místě jako podpůrný prostředek ověření totožnosti Uživatele nebo pro potvrzení Pokynu Uživatele.

3. Podmínky provozu Služeb přímého bankovnictví

3.1. Banka provozuje Služby přímého bankovnictví 24 hodin denně. Ačkoliv jsou obvykle technické prostředky nezbytné pro využití Služeb přímého bankovnictví Uživateli stále dostupné, Banka se nezavazuje umožnit jejich využití bez přerušení a nepřetržitě. Banka je oprávněna přerušit nebo omezit poskytování Služeb přímého bankovnictví na dobu nezbytnou k údržbě zařízení potřebných k jejich provozu.

3.2. Klient je povinen seznámit Uživatele s podmínkami Služeb přímého bankovnictví.

3.3. Banka není povinna kontrolovat věcnou správnost údajů uváděných Uživatelem prostřednictvím Služeb přímého bankovnictví.

3.4. Zadáním příslušného Certifikačního kódu, PINu či hesla ~~T-PIN, I-PIN, S-PIN či~~ nebo jiného Elektronického identifikačního prostředku nebo jejich kombinací vyjadřuje Uživatel souhlas s provedením příslušného úkonu (zejména Pokynu či Pokynu ke Smlouvě), u kterého jsou Certifikační kód, PIN, ~~PIN, I-PIN, S-PIN,~~ heslo či jiný Elektronický identifikační prostředek nebo jejich kombinace vyžadovány. Uživatel může vyjádřit souhlas s provedením vybraných Pokynů (například příkazů k odchozí úhradě mezi Účty vedenými Bankou pro téhož Klienta) či Pokynů ke smlouvě potvrzením ve formě kliknutí či poklepání na odpovídající tlačítko zobrazené ve Službě přímého bankovnictví či Mobilním klíči. Uživatel může rovněž vyjádřit svůj souhlas s provedením Pokynu či Pokynu ke smlouvě tak, že úspěšně ověří svou identitu pomocí otisku prstu nebo jiných biometrických údajů prostřednictvím senzoru biometrických údajů svého Mobilního zařízení. Způsob vyjádření souhlasu Uživatele s provedením příslušného úkonu závisí na technickém řešení zvoleném Bankou, které je v době vyjádření souhlasu Uživateli dostupné. ~~Banka a Klient se dohodli, že Certifikační kód, údaje uvedené v tomto odstavci výše v kombinaci s Elektronickými klíči, Certifikačním kódem nebo jiným Elektronickým identifikačním prostředkem nebo samotné použití jiného Elektronického identifikačního prostředku představují Elektronický podpis Uživatele nebo k vytvoření Elektronického podpisu Uživatele vedou.~~

3.5. Banka informuje Klienta Vhodným způsobem o všech relevantních skutečnostech, které souvisejí s provozem a dostupností Služeb přímého bankovnictví.

3.6. V návaznosti na úpravu Technických podmínek, čl. 1.8.4. Maximální výdajové limity, se pro Platební transakce, k nimž je dán Platební příkaz prostřednictvím Služeb přímého bankovnictví, vztahují následující omezení:
Použitím senzoru biometrických údajů Mobilního zařízení lze vyjádřit souhlas s provedením Platební transakce do částky maximálně 5 000 Kč včetně. V případě Platební transakce v jiné měně jsou pro přepočet využity směnné kurzy vyhlášené Bankou v Kurzovním lístku. Banka je však oprávněna vyžádat vyjádření souhlasu s provedením Platební transakce i do částky 5 000 Kč jiným způsobem, než použitím senzoru biometrických údajů Mobilního zařízení.
Dle ujednání v Technických podmínkách je Banka oprávněna při důvodném závěru o existenci rizika vzniku škody na straně Klienta změnit výše uvedené limity jednostranně (zejména snížit je až na hodnotu 0) a o přijatých opatřeních Klienta informovat Vhodným způsobem.

3.7 ~~5~~ Služba Informuj mě zahrnuje zasílání různých zpráv na základě požadavku Uživatele. Zprávy o Platebních transakcích a karetních blokacích jsou zasílány pouze v případě, že částka Platební transakce přesahuje limit stanovený Uživatelem. Zprávy nejsou rovněž zasílány v případě, že není možné zaúčtovat poplatek za zaslání zprávy (např. z důvodu nedostatku peněžních prostředků na příslušném Účtu).

3.8.~~6~~ Provoz Internetového bankovnictví
Banka umožňuje Uživatelům Internetového bankovnictví komunikovat s Bankou prostřednictvím veřejné datové sítě Internet. Adresa pro přihlášení do Internetového bankovnictví je uvedena na Veřejných stránkách a podle Uživatelem používaného typu Elektronického klíče se může lišit.

3.9.~~7~~ Provoz Mobilního bankovnictví
Banka umožňuje Uživatelům Mobilního bankovnictví komunikovat s Bankou prostřednictvím aplikace v Mobilním zařízení, která využívá datové připojení k síti Internet. Aplikace je k dispozici ke stažení v obchodech s aplikacemi App Store (pro mobilní zařízení s operačním systémem iOS) a Google Play (pro mobilní zařízení s operačním systémem Android) nebo prostřednictvím služeb, které je nahradí, pod názvem Raiffeisenbank CZ – Mobilní eKonto či názvem, který jej nahradí a o kterém Banka informuje Klienta Vhodným způsobem.

3.10.~~8~~ Provoz Telefonního bankovnictví
Banka umožňuje Uživatelům Telefonního bankovnictví komunikovat s Bankou prostřednictvím veřejné telefonní sítě. Telefonní bankovnictví je přístupné prostřednictvím infolinky uvedené na Veřejných stránkách, přičemž náklady telefonického spojení na tuto infolinku nese při hovorech v rámci České republiky Banka. V případě volání ze zahraničí je Telefonní bankovnictví přístupné na infolince uvedené rovněž na Veřejných stránkách a náklady telefonického spojení při hovorech ze zahraničí nese Uživatel.

4. Bezpečnost Služeb přímého bankovnictví

4.1. Obecné bBezpečnostní zásady:

a) Uživatel může mít určeno pouze jedno Klientské číslo. Na žádost Uživatele nebo při podezření na možné zneužití Klientského čísla je Banka oprávněna provést změnu Klientského čísla; tuto změnu Banka Uživateli neprodleně oznámí. Uživatel volí především takové Klientské číslo, které není přímo spojeno s jeho identitou;

b) Uživatel může disponovat pouze jedním Elektronickým klíčem od každého typu. ~~a nemůže mít zároveň Mobilní Elektronický klíč SIM Toolkit a Mobilní Elektronický klíč SMS.~~ Výjimkou je Smartphone Elektronický klíč, který je unikátní pro každé mobilní zařízení, jímž Uživatel přistupuje ke službě Mobilního bankovnictví, a kterých může Uživatel získat maximálně pět (5);

c) Elektronické identifikační prostředky jsou nepřenosné a nesmí být žádným způsobem poskytnuty osobě, která není jejich oprávněným držitelem;

d) Elektronické identifikační prostředky jsou vydávány výhradně za účelem použití v souvislosti se službami poskytovanými Bankou, zejména pak Službami přímého bankovnictví;

e) Banka je z bezpečnostních důvodů oprávněna zablokovat jakýkoliv Elektronický identifikační prostředek, zejména při podezření na

ztrátu, odcizení, zneužití, neautorizované použití nebo podvodné použití Elektronického identifikačního prostředku, např. pokud zjistí použití nebo hrozící použití Elektronického klíče jinou osobou než oprávněným Uživatelem;

~~f)~~ ~~Uživatel je povinen ihned po převzetí změnit čtyřmístný číselný kód (PIN) chránící Osobní Elektronický klíč;~~

f) ~~g)~~ Uživatel je povinen měnit pravidelně (alespoň jedenkrát za tři [3] měsíce) číselné kódy ~~I-PIN a T-PIN~~ PIN pro zachování maximální bezpečnosti realizovaných Pokynů a Pokynů ke ~~S~~smlouvě a Uživatel je rovněž povinen změnit číselné kódy ~~I-PIN a T-PIN~~ PIN, pokud jej k tomu Banka vyzve;

g) ~~h)~~ Uživatel je povinen učinit veškerá opatření k zajištění bezpečnosti užívání Služeb přímého bankovnictví, zejména nezaznamenávat svá hesla a PINy ~~kódy~~ ve snadno rozeznatelné podobě a nesdělovat je třetím osobám, chránit své Elektronické identifikační prostředky před odcizením nebo zneužitím jakoukoliv osobou;

h) ~~i)~~ v případě odcizení, zneužití, ztráty, neautorizovaného použití nebo podezření na odcizení, zneužití, ztrátu nebo neautorizované použití Elektronických identifikačních prostředků je Uživatel povinen jakoukoliv tuto skutečnost neprodleně oznámit vhodným způsobem Bance (zejména na infolince 800 900 900 při hovoru v rámci České republiky nebo na infolince +420 417 941 444 při hovoru ze zahraničí, případně osobně na nejbližším Obchodním místě);

i) ~~j)~~ Uživatel je v případě podezřelých dotazů povinen obrátit se na Banku prostřednictvím infolinky 800 900 900, zejména v případě, kdy si není jist, že komunikuje se zástupcem Banky;

j) ~~k)~~ Uživatel je povinen chovat se na internetu obezřetně, zejména nevyužívat pro přístup ke Službám přímého bankovnictví veřejně přístupná technická zařízení nebo technické zařízení, jehož bezpečné použití pro přístup ke Službám přímého bankovnictví Uživatel neověřil nebo ověřit nemohl; ~~Další informace o bezpečném využití Služeb přímého bankovnictví jsou zpřístupněny na Veřejných stránkách;~~

k) využívá-li Klient pro přístup ke Službám přímého bankovnictví Mobilní zařízení, je povinen zamezit jiným osobám použít Mobilní zařízení a aplikace, které pro přístup ke Službám přímého bankovnictví využívá, dále je povinen neumožnit jiné osobě registrovat v Mobilním zařízení jakékoliv bezpečnostní prostředky, které mohou být pro přístup ke Službám přímého bankovnictví a vyjádření souhlasu s Pokynem či Pokynem ke smlouvě využity (například číselné a jiné kódy, biometrické údaje), nesdělovat údaje a prostředky pro přístup ke Službám přímého bankovnictví a pro vyjádření souhlasu s Pokynem či Pokynem ke smlouvě jiné osobě a chránit je rovněž před zjištěním jinými osobami, dále pak oznámit Bance neprodleně ztrátu, odcizení, poškození či zneužití nebo podezření na zneužití Mobilního zařízení či SIM karty v Mobilním zařízení; ~~Klient uzavřením jakékoliv smlouvy, jejíž součástí jsou tyto Produktové podmínky, prohlašuje, že se seznámil a je srozuměn s doporučeními týkajícími se bezpečnosti Služeb přímého bankovnictví, které jsou uvedeny v dokumentu „Bezpečnost Služeb přímého bankovnictví, zásady a doporučení pro jejich používání“. Tento dokument je zpřístupněn na Veřejných stránkách. Klient se zavazuje s obsahem dokumentu seznámit každého Uživatele a zajistit, že každý Uživatel bude postupovat v souladu s informacemi a doporučeními, které jsou v něm uvedeny.~~

l) Banka sděluje Klientovi svá aktuální doporučení, která se týkají zajištění bezpečnosti Služeb přímého bankovnictví, zprávou předanou Službami přímého bankovnictví nebo jiným kontaktním údajem, jinak především prostřednictvím Veřejných stránek, a to jejich částí označenou jako „Bezpečné bankovnictví“. Klient je povinen obsah části Veřejných stránek označenou jako Bezpečné bankovnictví pravidelně sledovat a při využívání Služeb přímého bankovnictví respektovat doporučení a pokyny Banky obsažené zde nebo v přímém sdělení zaslaném Klientovi. Klient je dále povinen s obsahem doporučení a pokynů Banky seznámit každého Uživatele a zajistit, že každý Uživatel bude těchto doporučení a pokynů Banky dbát;

m) využití senzoru biometrických údajů Mobilního zařízení může být dočasně zamezeno zejména pro jeho opakované neúspěšné použití; pro přihlášení ke Službám elektronického bankovnictví či vyjádření souhlasu s provedením Pokynu či Pokynu ke smlouvě pak Uživatel musí využít například odpovídající PIN;

n) Uživatel je povinen zajistit pravidelné aktualizace operačního systému Mobilního zařízení, vybavit Mobilní zařízení funkčním a aktualizovaným antivirovým programem včetně pravidelné kontroly Mobilního zařízení;

o) Uživatel je povinen neinstalovat do Mobilního zařízení programové vybavení, které nepochází z důvěryhodných zdrojů; v případě programového vybavení, které do Mobilního zařízení instaluje, pak Uživatel věnuje pozornost oprávněním, jež programové vybavení požaduje získat a v případě důvodné pochybnosti, zda požadované oprávnění neznamená hrozbu pro bezpečné využití Mobilního bankovnictví, je odmítne udělit;

p) Uživatel není oprávněn použít pro přístup ke Službám přímého bankovnictví Mobilní zařízení, u kterého byly provedeny zákroky označované jako „root/jailbreak“ nebo jiné zásahy s cílem získat privilegovaný přístup k nastavení Mobilního zařízení a překonat omezení stanovená výrobcem.

4.2. Elektronické klíče ~~Bezpečnost Internetového bankovnictví~~

Přístup ~~do~~ ke Službám elektronického bankovnictví je chráněn Elektronickými klíči, které představují bezpečnostní prostředek komunikace Banky a Klienta. Mobilní Elektronický klíč SMS dovoluje Uživateli přijímat unikátní Autentizační a Certifikační kódy prostřednictvím jeho Mobilního zařízení formou SMS zpráv. Jeho použití vyžaduje, aby Uživatel deklaroval svou totožnost prostřednictvím Klientského čísla, řádně vložil či sdělil Autentizační či Certifikační kód vygenerovaný Bankou a zpravidla připojil také příslušný PIN. Osobní Elektronický klíč zajišťuje generaci unikátních Autentizačních či Certifikačních kódů přímo. Smartphone Elektronický klíč je vytvářen prostřednictvím vazby na registrované Mobilního zařízení v Internetovém bankovnictví za účelem přístupu k Mobilnímu bankovnictví při aktivaci této služby. Mobilní klíč je aktivován prostřednictvím Internetového bankovnictví na registrovaném Mobilním zařízení a následně dovoluje Uživateli jeho prostřednictvím zpravidla ve spojení se zvoleným PINem, heslem či úspěšném použití senzoru biometrických údajů Mobilního zařízení přistupovat ke Službám přímého bankovnictví a vyjadřovat souhlas s provedením Pokynu či Pokynu ke smlouvě. Má-li být Uživateli zajištěn jiný či náhradní Elektronický klíč a pro jeho získání je nutná spolupráce s Bankou, provede Banka aktivaci takového Elektronického klíče do dvou Bankovních pracovních dnů od doručení takové žádosti (provedení aktivace může být podmíněno další součinností Uživatele či Klienta).

~~Internetového bankovnictví je chráněn Elektronickými klíči:~~

~~Mobilní Elektronický klíč SIM Toolkit nebo SMS:~~

~~pro přihlášení do Internetového bankovnictví Uživatel vždy použije své Klientské číslo a Autentizační kód vygenerovaný Bankou a zaslaný na Mobilní telefon Uživatele, který je registrován jako Mobilní Elektronický klíč (MEk). Kód zaslaný Bankou má omezenou časovou platnost. U Elektronického klíče MEk SIM Toolkit je kód zaslán šifrovanou SMS chráněnou klíčem na SIM kartě. U Elektro-~~

nického klíče MEk SMS je kód zaslán nešifrovanou SMS a je nutné k němu doplnit I-PIN;
pro podepsání Pokynů a Pokynů ke smlouvě Uživatel používá Certifikační kód, jenž je vygenerovaný Bankou a zaslaný na Mobilní telefon Uživatele, který je registrován jako Mobilní Elektronický klíč. Kód zaslaný Bankou má omezenou časovou platnost. U Elektronického klíče MEk SIM Toolkit je kód zaslán šifrovanou SMS chráněnou klíčem na SIM kartě. U Elektronického klíče MEk SMS je kód zaslán nešifrovanou SMS a je nutné k němu doplnit I-PIN;
v případě, že Uživatel oznámí Bance ztrátu, zapomenutí, vyzrazení třetí osobě, neautorizované nebo podvodné použití nebo požádá o blokaci I-PINu, Banka vydá nový I-PIN na základě žádosti Uživatele, případně vytvoření nového I-PINu v součinnosti s Uživatelem zajistí;
z bezpečnostních důvodů Banka provede automaticky blokaci I-PINu po třech neplatných pokusech zadat I-PIN. Banka vydá nový I-PIN na základě písemné žádosti Uživatele;
v případě zničení, ztráty, blokace Mobilního telefonu, SIM karty nebo jiné změny na telefonním čísle používaném pro zasílání Autentizačních a Certifikačních kódů je Uživatel povinen tuto skutečnost Bance neprodleně oznámit. V takovém případě je Banka oprávněna provést blokaci příslušného Elektronického klíče a na základě žádosti Uživatele též přenastavení příslušného Elektronického klíče.
Osobní Elektronický klíč:
pro přihlášení do Internetového bankovnictví Uživatel vždy použije své Klientské číslo a online Autentizační kód vygenerovaný OEk. Tento Autentizační kód má časově omezenou platnost;
pro podepsání Pokynů a Pokynů ke smlouvě Uživatel používá Certifikační kód, jenž je vygenerovaný OEk po zadání údajů z Pokynu nebo Pokynu ke Smlouvě. Tento Certifikační kód má časově omezenou platnost;
v případě zničení, ztráty, poruchy nebo odcizení OEk je Uživatel povinen tuto skutečnost Bance neprodleně oznámit. V takovém případě je Banka oprávněna provést blokaci OEk a na základě písemné žádosti Uživatele vydat nový OEk.
Bezpečnost Mobilního bankovnictví
Přístup do Mobilního bankovnictví je chráněn zvoleným heslem (S-PIN) a Smartphone Elektronickým klíčem instalovaným v mobilním zařízení. Obojí Uživatel získá v průběhu aktivace služby Mobilního bankovnictví.
Smartphone Elektronický klíč
Uživatel si vytvoří Smartphone Elektronický klíč v prostředí Internetového bankovnictví, kam se přihlásí pomocí svého Klientského čísla a Autentizačního kódu vygenerovaného jedním z Elektronických klíčů, které slouží pro přístup do Internetového bankovnictví;

a) v aplikaci Mobilního bankovnictví si v průběhu aktivace uživatel zvolí S-PIN (čtyř až osmimístné číslo);
b) pro podepsání Pokynů a Pokynů ke Smlouvě Uživatel použije S-PIN, který společně se Smartphone Elektronickým klíčem vytvoří Elektronický podpis, a to na základě správně zadaného S-PINu;
c) z bezpečnostních důvodů Banka provede automaticky blokaci S-PINu po pěti (5) neplatných pokusech zadat S-PIN. Banka umožní vytvoření nového S-PINu na základě žádosti Uživatele v Internetovém bankovnictví, která bude podepsána Certifikačním kódem získaným pomocí Elektronického klíče, jenž slouží Uživateli pro přístup do Internetového bankovnictví a pro jeho obsluhu;
d) v případě zničení, ztráty, blokace nebo jiného důvodu ukončení používání mobilního zařízení, na němž byl vytvořen Smartphone Elektronický klíč, je Uživatel povinen provést blokaci takového Elektronického klíče v Internetovém bankovnictví.

4.3. Bezpečnost Telefonního bankovnictví
Využití služeb Telefonního bankovnictví je chráněno Elektronickými klíči:
4.3.1. Mobilní Elektronický klíč SIM Toolkit nebo SMS:
a) pro ověření totožnosti je Uživatel povinen sdělit telefonnímu bankéři své Klientské číslo nebo číslo Účtu nebo číslo telefonním bankéřem určené platební karty.
Poté telefonní bankéř vygeneruje a odešle Autentizační kód na Mobilní zařízení Uživatele, které je registrováno jako Mobilní Elektronický klíč. Tento Autentizační kód zaslaný Bankou má omezenou časovou platnost. Uživatel Autentizační kód sdělí telefonnímu bankéři. U Elektronického klíče MEk SIM Toolkit je kód zaslán šifrovanou SMS chráněnou klíčem na SIM kartě. U Elektronického klíče MEk SMS je kód zaslán nešifrovanou SMS a je nutné k němu doplnit T-PIN;
b) v případě, že Uživatel oznámí Bance ztrátu, zapomenutí, vyzrazení třetí osobě, neautorizované nebo podvodné použití nebo požádá o blokaci T-PIN, Banka vydá nový T-PIN na základě písemné žádosti Uživatele;
c) z bezpečnostních důvodů Banka provede automaticky blokaci T-PINu po třech (3) neplatných pokusech zadat T-PIN. Banka vydá nový T-PIN na základě písemné žádosti Uživatele;
d) v případě zničení, ztráty, blokace Mobilního zařízení, SIM karty nebo jiné změny na telefonním čísle používaném pro zasílání Autentizačních kódů je Uživatel povinen tuto skutečnost Bance neprodleně oznámit. V takovém případě je Banka oprávněna provést blokaci příslušného Elektronického klíče.
4.3.2. Osobní Elektronický klíč:
a) pro ověření totožnosti musí Uživatel sdělit telefonnímu bankéři své Klientské číslo nebo číslo Účtu nebo číslo platební karty nebo číslo OEk. Poté telefonnímu bankéři sdělí online Autentizační kód vygenerovaný OEk. Kód má časově omezenou platnost;
b) v případě zničení, ztráty, poruchy nebo odcizení OEk je Uživatel povinen tuto skutečnost Bance neprodleně oznámit. V takovém případě je Banka oprávněna provést blokaci OEk a na základě písemné žádosti Uživatele vydat nový OEk.

4.4. V případě, že Uživatel požádá Banku o vydání/nastavení nového nebo náhradního Elektronického klíče kteréhokoliv druhu s výjimkou Smartphone Elektronického klíče, Banka provede aktivaci takového Elektronického klíče do dvou (2) Bankovních pracovních dnů od doručení takové žádosti Klienta Bance. Lhůta neběží po dobu, v níž Služba přímého bankovnictví, ke které se Elektronický klíč vztahuje, není funkční z důvodu mimo kontrolu Banky či údržby nebo úprav systémů Banky.

5. Odpovědnost za škodu

5.1. Banka neodpovídá za škodu vzniklou z důvodů a v rozsahu dohodnutém v příslušných ustanoveních VOP, zejména pak za škodu vzniklou dočasnou nedostupností Služeb přímého bankovnictví, poruchami telefonní sítě, sítě datové nebo poruchami na straně mobilního operátora nebo poskytovatele internetového připojení. V případě, že prostřednictvím Služeb přímého bankovnictví dochází k poskytování Platebních služeb, řídí se odpovědnost za škodu Banky a Klienta úpravou obsaženou v Technických podmínkách.

6. Mimosoudní řešení sporů

6.1. K rozhodování sporů mezi Bankou a Klientem, který je Spotřebitelem, při poskytování služeb, na které se vztahují tyto Produktové podmínky, pokud je jinak k rozhodnutí takového sporu dána pravomoc českému soudu, je rovněž příslušný finanční arbitr. Pokud Kli-

ent, který je Spotřebitelem, není s postupem Banky při poskytování služeb, na které se vztahují tyto Produktové podmínky, srozuměn, může se obrátit se svou stížností na finančního arbitra, působícího na adrese Legerova 69, 110 00 Praha 1. Více informací a kontaktních údajů je k dispozici na internetových stránkách finančního arbitra www.finarbitr.cz.

7. Závěrečná ustanovení

7.1. Banka je oprávněna navrhnout změnu těchto Produktových podmínek, a to za podmínek a způsobem dohodnutým v článku I VOP.

~~7.2. Klient a Banka se dohodli, že práva a povinnosti ze Smlouvy o službách uzavřené před nabytím účinnosti zákona č. 89/2012 Sb., občanského zákoníku (dále jen „Občanský zákoník"), se od 1. 1. 2014 řídí tímto právním předpisem.~~

7.2.~~3~~ Tyto Produktové podmínky nabývají účinnosti dne 1. 5~~3~~. 201~~9~~8 a nahrazují Produktové podmínky služeb přímého bankovnictví, které nabyly účinnosti dne 1~~3~~. 1~~4~~. 201~~8~~7.

8. Vymezení pojmů

Pojmy označené velkými písmeny nevymezené v těchto Produktových podmínkách jsou vymezeny ve VOP.

~~**Autentizace** znamená ověření totožnosti Uživatele.~~

Autentizační kód znamená číselný kód sloužící k ověření totožnosti Uživatele v rámci Služeb přímého bankovnictví. Tento kód může mít omezenou či neomezenou dobu platnosti, avšak vždy jde o jednorázový kód, který nelze použít opakovaně.

~~**Certifikace** znamená podpis Pokynu nebo Pokynu ke smlouvě Certifikačním kódem.~~

Certifikační kód znamená číselný kód sloužící k podpisu Pokynu nebo Pokynu ke smlouvě a je vytvářen prostřednictvím Elektronického klíče. Tento kód může mít omezenou dobu platnosti (tzv. online Certifikační kód) nebo neomezenou dobu platnosti (tzv. offline Certifikační kód). V obou případech se jedná o jednorázový kód, který nelze použít opakovaně.

Elektronické identifikační prostředky znamenají veškeré ~~typy prostředků pro vytváření Elektronického podpisu nebo pro ověření autora Pokynu či Pokynu ke smlouvě, např. Elektronické klíče, T-PINu, I-PINu nebo S-PINu.~~ nástroje a údaje, které jsou určeny pro ověření totožnosti Uživatele a vyjádření souhlasu s Pokynem či Pokynem ke smlouvě. Jde jak o Certifikační a Autentizační kódy, PINy, hesla, tak rovněž o Mobilní klíč či Mobilní zařízení (především jeho hardwarové a softwarové vybavení), využije-li Uživatel pro přihlášení ke Službě přímého bankovnictví nebo vyjádření souhlasu s Pokynem či Pokynem ke smlouvě například své biometrické údaje.

Elektronické klíče znamenají prostředky umožňující Uživateli ~~provedení~~ ověření jeho totožnosti vůči Bance či odsouhlasení Pokynu či Pokynu ke smlouvě. ~~jeho Autentizace nebo Certifikace prostřednictvím Autentizačních a Certifikačních kódů.~~ Varianty Elektronických klíčů dostupné Uživateli jsou závislé na technickém a bezpečnostním řešení vzájemné komunikace zvoleném Bankou a rovněž její obchodní nabídce. Elektronické klíče jsou ve smluvní dokumentaci, především Podpisových vzorech, označeny také jako bezpečnostní prostředky.

~~**Elektronický podpis** znamená podpis, který používá Banka a Uživatel při vzájemné komunikaci. Za Elektronický podpis považují Banka a Klient především Certifikační kódy vytvářené prostřednictvím Elektronických klíčů a Certifikační kódy doplněné dalšími Elektronickými identifikačními prostředky.~~

Informační zpráva znamená SMS zprávu zasílanou na určené telefonní číslo nebo textovou zprávu zasílanou na e-mailovou adresu Uživatele, případně notifikační zprávu aplikace Mobilního bankovnictví, jejímž prostřednictvím může být Uživatel informován o zůstatku a pohybech na Účtu nebo o jiných skutečnostech. Doručení notifikační zprávy je podmíněno funkčním přenosem dat Mobilního zařízení, které Uživatel pro přístup k Mobilnímu bankovnictví využívá; v případě nedostupného datového přenosu nebude notifikační zpráva předána.

Informuj mě znamená službu zasílání Informačních zpráv.

Internetové bankovnictví znamená službu (systém) provozovanou prostřednictvím klientské aplikace, která se spouští v prostředí internetového prohlížeče a komunikuje se serverem Banky. ~~, existuje ve dvou jazykových verzích (české a anglické), případně dalších jazykových verzích, které Banka zpřístupní.~~

~~**I-PIN** znamená čtyřmístný číselný kód pro podepsání Pokynu nebo Pokynu ke smlouvě v Internetovém bankovnictví v kombinaci s Mobilním Elektronickým klíčem SMS.~~

Klientské číslo znamená jednoznačné číselné označení identity Uživatele pro Služby přímého bankovnictví, které neslouží k ověření jeho totožnosti.

~~**Mobilní Elektronický klíč SIM Toolkit nebo též MEk SIM Toolkit** umožňuje Uživateli příjem online Autentizačních a Certifikačních kódů formou šifrované SMS na Mobilním zařízení.~~

Mobilní Elektronický klíč SMS nebo též MEk SMS umožňuje Uživateli příjem online Autentizačních a Certifikačních kódů formou běžné SMS zprávy na Mobilním zařízení. Kódy takto doručené lze použít v kombinaci s T-PINem prostřednictvím Telefonního bankovnictví a v kombinaci s I-PINem prostřednictvím Internetového bankovnictví.

Mobilní klíč znamená aplikaci, jež slouží k zajištění bezpečné komunikace Uživatele a Banky při využívání Služeb přímého bankovnictví. Aplikace je k dispozici ke stažení v obchodech s aplikacemi App Store (pro mobilní zařízení s operačním systémem iOS) a Google Play (pro mobilní zařízení s operačním systémem Android) nebo prostřednictvím služeb, které je nahradí, pod názvem Mobilní klíč či názvem, který jej nahradí a o kterém Banka informuje Klienta Vhodným způsobem. Mobilní klíč umožňuje Uživateli ověření jeho totožnosti vůči Bance nebo vyjádření souhlasu s provedením Pokynu či Pokynu ke smlouvě. Pro obsluhu Mobilního klíče je nezbytné stanovení PINu či hesla, případně úspěšné použití biometrického senzoru Mobilního zařízení.

Mobilní bankovnictví znamená službu provozovanou prostřednictvím klientské aplikace v Mobilním zařízení, která komunikuje se serverem Banky. ~~, existuje ve dvou jazykových verzích (české a anglické).~~

Mobilní operátor znamená poskytovatele služeb elektronických komunikací.

Mobilní zařízení znamená mobilní telefon nebo jiné mobilní zařízení (tablet) vybavené SIM kartou aktivovanou v síti Mobilního operátora.

Osobní Elektronický klíč nebo též OEk znamená hardwarové zařízení, které umožňuje Uživateli generovat online i offline Autentizační a Certifikační kódy ~~pro přímé bankovnictví~~. Jeho použití je chráněno ~~čtyřmístným číselným kódem~~ (PIN~~em~~).

PIN znamená vícemístný číselný kód, který používá Uživatel pro odsouhlasení Pokynu či Pokynu ke smlouvě. PIN je určen pro použití v Internetovém, Mobilním či Telefonním bankovnictví a je pro potřeby těchto jednotlivých Služeb přímého bankovnictví označen jako I-PIN, T-PIN, nebo S-PIN. PIN je zároveň jedním z bezpečnostních prvků pro odsouhlasení Pokynu či Pokynu ke smlouvě prostřednictvím Mobilního klíče či pro použití OEk. Při opakovaném

neúspěšném zadání PINu je Banka oprávněna jeho další použití blokovat. Počet těchto neúspěšných pokusů je pro jednotlivé druhy PINů odlišný. Dojde-li k blokaci PINu, Uživatel pro obnovení přístupu ke Službám přímého bankovnictví požádá Banku o potřebnou součinnost.

Služby přímého bankovnictví znamenají služby Internetového, Mobilního a Telefonního bankovnictví.

Smartphone Elektronický klíč nebo též SPEk znamená funkčnost v rámci aplikace Mobilního bankovnictví, která ve spojení s kódem S-PIN slouží k ochraně komunikace Uživatele a Banky ~~a pro podepsání Pokynu nebo Pokynu ke smlouvě~~.

Smlouva o službách znamená smlouvu mezi Bankou a Klientem, kterou jsou sjednávány Služby přímého bankovnictví.

~~**Stavová zpráva** znamená informační SMS zprávu nebo e-mail o stavu zpracování transakce (zejména Platební transakce) zadané prostřednictvím Služeb přímého bankovnictví.~~

~~**S-PIN** znamená čtyř až osmimístný číselný kód, který ve spojení se Smartphone Elektronickým klíčem slouží k ochraně komunikace Uživatele a Banky a pro podepsání Pokynu nebo Pokynu ke smlouvě.~~

Telefonní bankovnictví znamená službu umožňující Uživateli komunikaci se zástupcem Banky – telefonním bankéřem – zahrnující jak informace o poskytovaných službách Banky, tak přímo využití některých služeb Banky.

~~**T-PIN** znamená čtyř nebo šestimístný číselný kód pro podepsání Pokynu nebo Pokynu ke smlouvě nebo pro potvrzení Pokynu nebo Pokynu ke smlouvě prostřednictvím Telefonního bankovnictví v kombinaci s Mobilním Elektronickým klíčem SMS.~~

Uživatel znamená Klienta nebo jinou fyzickou osobu oprávněnou Klientem přistupovat ke Službám přímého bankovnictví a využívat v zastoupení Klienta jejich prostřednictvím další služby poskytované Bankou Klientovi v rozsahu, který Klient určí.