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. 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 již neposkytuje Klientovi žádné Bankovní služby kromě Služeb přímého bankovnictví, závazky ze Smlouvy o službách, včetně závazků z doplňkových služeb dle čl. 5 těchto Produktových podmínek, zanikají. Povinnosti upravené v čl. 4 Produktových podmínek však trvají po dobu, kdy je Uživateli umožněno Elektronických identifikační prostředek používat. Klient může Služby přímého bankovnictví i po zániku závazků ze Smlouvy o službách nadále za účelem přístupu k informacím a dokumentům předaným prostřednictvím Služeb přímého bankovnictví. Pokud se však po zániku závazků ze Smlouvy o službách 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. 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. Banka umožní vybraným Klientům určení úvodního rozsahu oprávnění Uživatele, změnu stávajícího rozsahu oprávnění Uživatele či zrušení role Uživatele (tedy zřízení, změnu či zrušení Podpisového vzoru) prostřednictvím Služeb přímého bankovnictví (zejména Internetového a Mobilního bankovnictví). Správa uživatelských oprávnění bude tímto způsobem umožněna především Klientům, kteří jsou právnickými osobami, a u nichž lze očekávat potřebu zřízení většího počtu Uživatelů a vyšší frekvenci změn jejich oprávnění. Uvedená funkcionalita pak bude dostupná výhradně Uživatelům, které k tomu Klient výslovně prostřednictvím Podpisového vzoru zmocnil (takové zmocnění ovšem nebude možné udělit prostřednictvím Internetového bankovnictví). Klientům, kteří jsou fyzickými osobami, však Banka umožní dle tohoto ustanovení správu uživatelských oprávnění i v případě, že si jako Uživatelé takové oprávnění výslovně nezřídili. Vytvoření či změna Podpisového vzoru prostřednictvím Internetového bankovnictví se bude moci týkat pouze Uživatele, u něhož již došlo k řádné identifikaci Bankou ve smyslu čl. 2 VOP.

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

1.5. 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.

1.6. 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.

1.7. 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.

1.8. Pro využívání Telefonního bankovnictví je třeba, aby byl Uživatel držitelem Mobilního zařízení aktivovaného v síti libovolného Mobilního operátora.

1.9. Pro využití služby označené jako Premium API je třeba, aby byl Uživatel oprávněn získat prostřednictvím Internetového bankovnictví příslušný certifikát Premium API a měl zajištěn přístup k nezbytným nástrojům (zejména softwarovému vybavení) třetích stran, které je přizpůsobeno k datové komunikaci s Bankou prostřednictvím rozhraní Premium API.

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, službách poskytovaných třetími osobami, jež s Bankou spolupracují, dále jako doručovací místo pro zprávy nebo právní jednání Banky či třetích osob, jež s Bankou spolupracují, adresované Klientovi a jako 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 jednající smluvní strany. Smlouvou se pro účely tohoto ustanovení Produktových podmínek může rozu-

mět 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 pří mého bankovnictví. Internetové nebo Mobilní 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. Ujednání v tomto čl. 2.3 se pak obdobně uplatní pro případné sjednání služeb mezi Klientem a třetími osobami, které Banka zastupuje.

2.4. Služby přímého bankovnictví mohou být použity také jako prostředek komunikace na dálku za účelem předání vybraných dokumentů v elektronické podobě ze strany Uživatele Bance. Přehled dokumentů, které mohou být tímto způsobem Bance předány, zpřístupní Banka Uživateli Vhodným způsobem, zejména prostřednictvím vymezené části Internetového nebo Mobilního bankovnictví, stejně tak informace o podporovaných formátech dokumentů, jejich maximální velikosti a případných dalších technických či jiných podmínkách, jejichž dodržení je pro úspěšné předání dokumentu Bance nezbytné. Banka se může s Klientem na podmínkách předání určitého dokumentu v elektronické podobě také zvlášť dohodnout. Dokument, který není uveden v přehledu Bankou akceptovaných dokumentů nebo jehož předání nebylo mezi Bankou a Klientem zvlášť ujednáno, případně který nebyl Bance předán v souladu s ujednanými či zpřístupněnými podmínkami, není Banka povinna přijmout. Dostupnost této funkcionality pro konkrétního Klienta či Uživatele může být závislá na obchodní nabídce Banky a rozsahu dalších sjednaných Bankovních služeb.

2.5. Autentizační či Certifikační kód nebo RB 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.

2.6 V případě, že je Uživatel oprávněn získat certifikát Premium API a učiní tak, je povinen nakládat s certifikátem Premium API jako s jiným Elektronickým identifikačním prostředkem. Certifikát Premium API je vázán na Uživatele a je nepřenosný. Přístup k certifikátu Premium API je chráněn heslem, které si Uživatel zvolí. Uživateli pak dovoluje předat Bance jen takové požadavky, k nimž je oprávněn příslušným Podpisovým vzorem. Certifikát Premium API dovoluje Uživateli předat Bance požadavek výhradně prostřednictvím softwaru, který byl jeho zhotovitelem uzpůsoben ke komunikaci s Bankou prostřednictvím Premium API. Banka proto nezaručuje, že Uživatel může získaný certifikát Premium API využít ani neodpovídá za to, že příslušný software zajistí bezchybnou komunikaci a přenos dat prostřednictvím Premium API. Klient je povinen ověřit, že software, jehož prostřednictvím bude Uživatel předávat Bance požadavky, u nichž bude identita Uživatele ověřována prostřednictvím certifikátu Premium API, je takové datové komunikaci vhodně přizpůsoben a poskytuje Klientovi a rovněž Uživateli adekvátní míru bezpečnosti a ochrany údajů, které na vyžádání Uživatele Banka touto formou komunikace předá. Banka rovněž neodpovídá za bezpečnost a důvěrnost dat, která jsou předána z rozhraní Premium API. Rozsah požadavků, které může Uživatel Bance prostřednictvím rozhraní Premium API předat, je omezen aktuální obchodní nabídkou Banky.

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 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, 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 RB 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.

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. 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. 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. 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 prostřednictvím distribučních služeb dle operačního systému nebo výrobce Mobilního zařízení pod názvem Raiffeisenbank CZ – Mobilní eKonto či názvem, který jej nahradí a o kterém Banka informuje Klienta Vhodným způsobem.

3.10. 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. V případě volání ze zahraničí je Telefonní bankovnictví přístupné na infolince uvedené rovněž na Veřejných stránkách.

4. Bezpečnost Služeb přímého bankovnictví

4.1. Obecné bezpečnostní 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. 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, či službami na jejichž poskytování či zprostředkování se Banka podílí;

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, je-li na takové zneužití Uživatelem upozorněna, nebo pokud je prokazatelně obeznámena se skutečností, že Uživatel zemřel nebo byl prohlášen za mrtvého;

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

g) Uživatel je dále povinen nezaznamenávat svá hesla a PINy ve snadno rozeznatelné podobě a nesdělovat je třetím osobám, chránit své Elektronické identifikační prostředky před odcizením nebo zneužitím jakoukoliv osobou;

h) 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 prostřednictvím kontaktních údajů uvedených Bankou na Veřejných stránkách;

i) V případě, že je Uživatel osloven výzvou či podnětem k zadání jakýchkoliv Elektronických identifikačních prostředků zprávou elektronické pošty, SMS nebo jinou formou elektronického sdělení, pak podle takové výzvy či podnětu nepostupuje a je povinen kontaktovat Banku především telefonicky prostřednictvím kontaktních údajů uvedených Bankou na Veřejných stránkách a reakci na takovou výzvu či podnět s Bankou konzultovat; je povinen Banku kontaktovat rovněž v případě, že chová jakékoliv pochybnosti, zda komunikuje s Bankou či zástupcem Banky a také v případě, pokud jej k tomu Banka vyzve v souvislosti s jakoukoliv aktivitou, o které si není jist, že je záměrným a chtěným výsledkem jeho předcházející činnosti;

j) Uživatel je povinen chovat se na internetu obezřetně, zejména je povinen:
1) 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;
2) zdržet se návštěv internetových stránek, které jsou nedůvěryhodné, mohou představovat riziko pro bezpečné užívání Služeb přímého bankovnictví (zejména internetové stránky s jakýmkoliv nelegálním obsahem);
3) věnovat pozornost zasílaným emailovým, SMS zprávám, nebo jiným formám komunikace na dálku, neotevírat nevyžádaná sdělení, a pokud tak již učiní pro nutné ověření povahy zprávy, neotvírat či nespouštět jakékoliv podezřelé přílohy takových zpráv nebo odkazy, které obsahují;
4) vždy ověřit, zda je internetová stránka, na které zadává Elektronické identifikační prostředky provozována Bankou, a to podle obsahu adresního řádku prohlížeče, který odpovídá adrese „https://www.rb.cz" a podle bezpečnostního certifikátu – zobrazením jeho detailu při pokliku na zámek v adresním řádku prohlížeče („view/show certificate"), držitelem (subjektem) certifikátu musí být Raiffeisenbank a.s. (bližší popis dostupný na Bezpečném bankovnictví); jako bezpečné řešení přístupu na Veřejné stránky za účelem přihlášení ke službě Internetového bankovnictví volí Uživatel ruční zadání adresy uvedené výše do příslušného řádku prohlížeče;
5) nezadávat žádné Elektronické identifikační prostředky jinde než do příslušné aplikace Mobilního bankovnictví, aplikace RB klíč, případně jiných komunikačních prostředků sjednaných s Bankou, nebo internetových stránek, které jsou provozovány Bankou, a nereagovat na výzvy k zadání jakýchkoliv Elektronických identifikačních prostředků jakoukoliv elektronickou zprávou;
6) neumožnit žádné osobě obsluhu Technického zařízení na dálku, když využívá nebo přistupuje ke službě Internetového bankovnictví nebo Mobilního bankovnictví;
7) pozorně sledovat popis Pokynu či Pokynu ke smlouvě, ke kterému se váže zaslaný Certifikační kód, vyžádané potvrzení v aplikaci Mobilní klíč či RB klíč, a pokud neodpovídá chtěným a zamýšleným záměrům Uživatele, pak takový Certifikační klíč nepoužít nebo potvrzení neučinit;
8) využívá-li služby Mobilního bankovnictví a Internetového bankovnictví současně, použít k tomu dvě různá Technická zařízení;

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;

l) Banka sděluje Klientovi své aktuální pokyny, která se týkají zajištění bezpečnosti Služeb přímého bankovnictví, hrozeb, kterým může Uživatel Služeb přímého bankovnictví čelit zprávou předanou Službami přímého bankovnictví nebo jiným kontaktním údajem (například emailem či SMS zprávou, notifikací v aplikaci Mobilního zařízení), jinak především prostřednictvím Bezpečného bankovnictví Klient je povinen se s těmito pokyny vždy seznámit, obsah Bezpečného bankovnictví pravidelně sledovat a při využívání Služeb přímého bankovnictví respektovat a následovat pokyny Banky a rovněž zohlednit Bankou poskytované informace o aktuálních hrozbách. Klient je dále povinen s obsahem pokynů Banky seznámit každého Uživatele a zajistit, že každý Uživatel bude rovněž těchto doporučení 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 Technického zařízení, vybavit Technického zařízení funkčním a aktualizovaným antivirovým programem včetně pravidelné kontroly Technického zařízení jeho prostřednictvím, dále pak chránit Technické zařízení nástrojem pro řízení navazované komunikace (firewall); dále je Uživatel povinen sledovat doporučení a upozornění výrobců či distributorů softwaru či Technického zařízení o hrozbách a rizicích a přizpůsobit jim užívání Technického zařízení či jeho softwarového vybavení;

o) Uživatel je povinen neinstalovat do Technického zařízení softwarového vybavení, které nepochází z důvěryhodných zdrojů (v případě Mobilních zařízení pak z příslušných oficiálních zdrojů dle operačního systému Mobilního zařízení) nebo o němž si není jistý, že neobsahuje viry či jiný obdobný závadný obsah, který by představoval hrozbu pro Uživatele a bezpečné užívání Služeb přímého bankovnictví; v případě softwarového vybavení, které do Mobilního zařízení instaluje, pak Uživatel věnuje pozornost oprávněním, jež softwarové vybavení požaduje získat a v případě důvodné pochybnosti, zda požadované oprávnění neznamená hrozbu pro bezpečné využití Služeb přímého bankovnictví, je odmítne udělit; výše uvedené povinnosti Uživatele platí rovněž v případě, že Mobilní zařízení využívá pouze pro potřeby MEk SMS;

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

Přístup ke Službám přímého 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 Mobilní zařízení registrované v Internetovém bankovnictví za účelem přístupu k Mobilnímu bankovnictví při aktivaci této služby. RB klíč je aktivován prostřednictvím Internetového bankovnictví, či jinou formou součinnosti Banky a Uživatele, na registrovaném Mobilním zařízení a následně dovoluje Uživateli jeho prostřednictvím zpravidla ve spojení se zvoleným PINem, heslem či úspěšným použitím 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).

5. Doplňkové služby

5.1. Banka prostřednictvím Služeb přímého bankovnictví umožňuje sjednat další služby, jež rozvíjejí dosavadní Bankovní služby, a to například novými způsoby předávání informací o využívaných Bankovních službách, nebo které představují samostatné Bankovní služby.

5.2. Otevřené bankovnictví

a) Prostřednictvím Internetového či Mobilního bankovnictví může být sjednána služba informování o platebním účtu, která je součástí funkcionalit označených jako „Otevřené bankovnictví". Službu může pro svou potřebu sjednat každý Uživatel služby Internetového bankovnictví, a v takovém případě je pro Banku Klientem, jenž vystupuje svým jménem.

b) Služba informování o platebním účtu dovoluje soustředit v Internetovém a Mobilním bankovnictvím informace o platebních účtech vedených jinými poskytovateli platebních služeb. Tyto informace zahrnují také údaje o transakcích provedených na platebních účtech. Rozsah informací, které budou v Internetovém a Mobilním bankovnictví dostupné, závisí především na tom, jaké údaje zpřístupnil poskytovatel platebních služeb, který platební účet vede. Banka přitom nemůže nijak ovlivnit, zda informace o určitém účtu jiný poskytovatel platebních služeb zpřístupní či nikoliv. V Internetovém a Mobilním bankovnictví lze soustředit informace o platebních účtech vedených poskytovateli, u nichž je Banka získání a předání těchto informací schopna zajistit. Obchodní nabídka Banky se v tomto ohledu může měnit.

c) Pro účet, který do služby informování o účtu Klient zahrne, zajistí Banka rovněž aktualizaci údajů včetně souvisejících transakcí i bez součinnosti Klienta. Taková aktualizace však může být provedena jen v omezené frekvenci. Pokud Banka provede aktualizaci údajů v maximální možné frekvenci, pro případnou další aktualizaci v průběhu příslušného období (zpravidla jeden den) je nutný výslovný pokyn Klienta (především prostřednictvím Internetového a Mobilního bankovnictví). Banka poskytne dle rozvoje technické intrastruktury Klientovi možnost zprostředkované informace o platebních účtech dále strukturovat a různým způsobem zobrazovat.

d) Údaje, které pro Klienta získá Banka při poskytování služby informování o platebním účtu o účtech vedených jinými poskytovateli platebních služeb a souvisejících platebních transakcích, jsou využity výhradně k poskytnutí služby informování o platebním účtu, pokud se Banka a Klient nedohodnou na něčem jiném, případně pokud Klient k jinému využití údajů neudělí souhlas.

e) Poskytování služby informování o platebním účtu je podmíněno trváním Smlouvy o službách.

5.3. RB identita

a) Využití služeb RB identity je možné výhradně prostřednictvím RB klíče. Pro jiné varianty Elektronických klíčů nejsou služby RB identity dostupné.

b) Za účelem využití RB klíče v rámci RB identity zajistí Banka, aby Uživatelé měli možnost využít tento Elektronický klíč jako prostředek elektronické identifikace či k dalším účelům nejen pro potřeby služeb

Národního bodu, ale rovněž v rámci jiných vztahů se třetími osobami, jež hodlají na služby zajišťované Bankou v rámci RB identity spoléhat. Rozsah těchto služeb je závislý na obchodní nabídce Banky a připravenosti třetích osob či zprostředkujících poskytovatelů identifikačních služeb využívat služby RB identity. Banka je však povinna zajistit Uživatelům možnost použít RB klíč především jako prostředek elektronické identifikace pro služby Národního bodu.

c) Využití RB klíče v rámci služeb RB identity především pro potřeby služeb Národního bodu vyžaduje, aby se stal prostředkem pro elektronickou identifikaci v rámci systému elektronické identifikace ve smyslu zákonných povinností, jimž Banka jako správce takového systému podléhá. Tyto povinnosti Bance ukládají, aby informaci o RB klíči, který je k dispozici konkrétnímu Uživateli, předala společně s informací o úrovni záruky, tj. s označením míry důvěry, kterou může třetí strana chovat k prokázání totožnosti prostřednictvím RB klíče, evidenci Národnímu bodu. Dále je Banka povinna ověřit totožnost držitele RB klíče prostřednictvím Národního bodu.

d) K ověření totožnosti Uživatele prostřednictvím Národního bodu dochází pomocí čísla a druhu dokladu Uživatele, které mohou být pro jednoznačné ztotožnění doplněny o jméno a příjmení, adresu pobytu, datum a místa narození. Druh dokladu totožnosti Uživatele musí být předmětem evidence registru obyvatel. Ověření totožnosti prostřednictvím Národního bodu však nebude možné provést, pokud údaj o čísle a druh dokladu Uživatele, kterým Banka disponuje, neodpovídá dokladu, jenž má v době, kdy ověření probíhá, v držení Uživatel a Banka bez součinnosti Uživatele nemůže aktuální údaje o čísle a druhu dokladu totožnosti zjistit. RB identitu nelze bez úspěšného ověření totožnosti Uživatele prostřednictvím Národního bodu poskytnout.

e) Činnosti dle bodu 5.3 písm. c) a d) výše Banka provede již na základě ujednání v těchto Produktových podmínkách ve vztahu k Uživatelům, kteří jsou Klienty, uzavřeli tedy s Bankou Smlouvu o službách. Služby RB identity jim tak budou dostupné již na základě dohody obsažené v těchto Produktových podmínkách. To však neplatí v případě, kdy identifikace Klienta při sjednání Bankovních služeb neproběhla za jeho fyzické přítomnosti s dokladem totožnosti, který je předmětem evidence registru obyvatel, nebo elektronicky pomocí tzv. uznaného prostředku pro elektronickou identifikaci, který byl vydán jinou bankou či poskytovatelem identifikačních služeb. Jakmile budou Uživateli služby RB identity dostupné, ověří Uživatel bezodkladně prostřednictvím Služeb přímého bankovnictví, že jsou jeho identifikační údaje Bankou evidovány správně a jsou aktuální.

f) Služby RB identity pro Uživatele, kteří nejsou účastníky Smlouvy o službách, nebo nesplňují předpoklady dle bodu 5.3 písm. e), Banka zpřístupní na základě registrace RB klíče pro potřeby služeb RB identity zejména prostřednictvím Internetového bankovnictví. Úspěšná registrace však vyžaduje splnění podmínek uvedených v bodě 5.3 písm. e), tedy ověření totožnosti Uživatele za jeho fyzické přítomnosti prostřednictvím dokladu totožnosti, který je předmětem evidence registru obyvatel a následné úspěšné ověření totožnosti prostřednictvím Národního bodu. Banka rovněž umožní Uživatelům zrušení registrace RB klíče jako prostředku elektronické identifikace v rámci RB identity. Pro opětovnou registraci RB klíče nebo registraci nové aktivace RB klíče platí ujednání bodu 5.3 písm. f) obdobně.

g) Třetí osoby nebo zprostředkující poskytovatelé identifikačních služeb pak mohou stanovit pro Uživatele RB Identity také další doplňující podmínky, například minimální věk. Informace týkající se Uživatele však Banka předá třetím osobám pouze za předpokladu a v rozsahu, k němuž Uživatel poskytne souhlas. To neplatí v případě činností Banky dle odst. c) a d) výše vůči Národnímu bodu; tento postup Banka uplatní již na základě dohody o službách RB identity v čl. 5.3 Produktových podmínek.

h) Použití RB klíče pro účely RB identity podléhá stejným bezpečnostním zásadám, které jsou pro Služby přímého bankovnictví stanoveny v čl. 4 Produktových podmínek. Uživatel odpovídá za újmu způsobenou zneužitím RB identity, k níž došlo porušením těchto bezpečnostních zásad v důsledku nedbalosti Uživatele, a to do okamžiku oznámení dle čl. 4.1 písm. h) Produktových podmínek.

6. Odpovědnost za škodu

6.1. 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.

7. Mimosoudní řešení sporů

7.1. 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 Klient, 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.

8. Závěrečná ustanovení

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

8.2. Tyto Produktové podmínky nabývají účinnosti dne 1. 9. 2021 a nahrazují Produktové podmínky služeb přímého bankovnictví, které nabyly účinnosti dne 1. 6. 2021.

9. Vymezení pojmů

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

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.

Bezpečné bankovnictví – znamená část Veřejných stránek označenou jako „Bezpečné bankovnictví", jež je dostupná prostřednictvím odkazů pod záložkou „Důležité informace" na Veřejných stránkách v jejich spodní části, případně přímo prostřednictvím adresy https://www.rb.cz/bezpecne-bankovnictvi.

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 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, certifikát Premium

API, tak rovněž o RB 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 ověření jeho totožnosti vůči Bance či odsouhlasení Pokynu či Pokynu ke smlouvě. 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.

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.

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

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 bankovnictví znamená službu provozovanou prostřednictvím klientské aplikace v Mobilním zařízení, která komunikuje se serverem Banky.

Mobilní operátor znamená poskytovatele služeb elektronických komunikací.

Mobilní zařízení znamená mobilní telefon nebo jiné mobilní zařízení (tablet). Pokud je pro použití Mobilního zařízení nezbytné využití služeb Mobilního operátora, je nutné, aby bylo vybaveno SIM kartou aktivovanou v síti Mobilního operátora.

Národní bod znamená Národní bod pro identifikaci a autentizaci, který slouží pro ověření totožnosti osob při užívání online služeb veřejné správy.

Osobní Elektronický klíč nebo též OEk znamená hardwarové zařízení, které umožňuje Uživateli generovat online i offline Autentizační a Certifikační kódy. Jeho použití je chráněno PIN.

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.

Premium API znamená rozhraní Banky, jehož prostřednictvím mohou být poskytovány Klientům vybrané Bankovní služby. Uživatelé, kteří disponují potřebným oprávněním, mohou získat a spravovat certifikát Premium API, jenž jim dovolí přistupovat k některým službám Banky prostřednictvím programového vybavení (softwaru) třetích stran (například pomocí účetního systému). Premium API zahrnuje především možnost získat tímto způsobem transakční historii Účtu Klienta. Pokud budou v budoucnu dostupné další funkcionality Premium API pro obsluhu či využití služeb Banky, budou o tom Klienti a Uživatelé vhodným způsobem informováni.

RB identita znamená Bankovní službu, jež představuje především elektronickou identifikaci či autentizaci Uživatele pomocí RB klíče prostřednictvím nebo za součinnosti Banky vůči třetím osobám. RB identita pak může také dovolit Uživateli právně jednat vůči třetím osobám, a to v rozsahu dle aktuální obchodní nabídky Banky nebo zprostředkujících poskytovatelů identifikačních služeb.

RB klíč znamená samostatnou aplikaci nebo doplňkovou funkci Mobilního bankovnictví, jež slouží k zajištění bezpečné komunikace Uživatele a Banky při využívání Služeb přímého bankovnictví. Samostatná aplikace je k dispozici ke stažení prostřednictvím distribučních služeb dle operačního systému nebo výrobce Mobilního zařízení. RB klíč umožňuje Uživateli ověření jeho totožnosti vůči Bance nebo vyjádření souhlasu s provedením Pokynu či Pokynu ke smlouvě. Pro obsluhu RB klíče je nezbytné stanovení PINu (v případě RB klíče jako funkce Mobilního bankovnictví je jím rovněž S-PIN) či hesla, případně úspěšné použití biometrického senzoru Mobilního zařízení.

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.

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

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.

Technické zařízení – Mobilní zařízení, počítač nebo notebook, kterým Uživatel přistupuje ke Službám přímého bankovnictví a využívá je.

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. V případě služby informování o platebním účtu je Uživatel osobou, která sjednává službu svým jménem a je tak vždy Klientem.

27100/06/2021