

## Produktové podmínky služeb přímého bankovníctví

(dále také jen „Produktové podmínky“)

### 1. Dostupnost Služeb přímého bankovníctví

- 1.1. Služby přímého bankovníctví 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 bankovníctví, závazky sjednané Smlouvou o službách zanikají, a to ke dni, kdy Banka přístup ke Službám přímého bankovníctví Klientovi ukončí. Banka tak učiní v přiměřené době po zjištění, že Klientovi jsou dostupné Služby přímého bankovníctví, 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 informace, které je mu Banka povinna poskytnout před jejím uzavřením.
- 1.2. V případě, že ke Službám přímého bankovníctví 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 bankovníctví 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 bankovníctví Banka určí Uživateli Klientské číslo pro přihlášení ke Službám přímého bankovníctví, případně si jej Uživatel zvolí.
- 1.4. Klient určí, jaký Elektronický klíč bude Uživatel používat. 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 bankovníctví v Internetovém bankovníctví na základě společného Pokynu Klienta a Uživatele.
- 1.5. Podmínkou využívání Internetového bankovníctví 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 bankovníctví je, aby Uživatel splňoval předpoklady pro přístup k Internetovému bankovníctví a byl držitelem Mobilního zařízení s operačním systémem iOS nebo Android a připojením k internetu.
- 1.7. Pro využívání Telefonního bankovníctví 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 bankovníctví

- 2.1. Služby přímého bankovníctví představují soubor Internetového, Telefonního a Mobilního bankovníctví, 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 bankovníctví dostupný Klientovi je přitom také závislý na dalších službách poskytovaných Bankou Klientovi. V případě Uživatele, který zároveň není Klientem, je pak rozsah Služeb přímého bankovníctví dostupný Uživateli vymezen Klientem prostřednictvím Podpisového vzoru.
- 2.2. Banka průběžně vyvíjí a upravuje služby a jejich funkce dostupné prostřednictvím Služeb přímého bankovníctví. Kromě jiného také za účelem zvýšení bezpečnosti vzájemné komunikace vyvíjí a přijímá potřebná opatření, jež mohou ovlivnit dostupnost Služeb přímého bankovníctví či přístup Klienta ke Službám přímého bankovníctví nebo způsob, jakým Klient Služby přímého bankovníctví 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 bankovníctví 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 bankovníctví v písemné formě je Bankou archivována a na žádost Klienta mu její znění bude poskytnuto; uzavřená Smlouva je pak rovněž zpravidla prostřednictvím Internetového bankovníctví dostupná Uživateli. Klient a Banka se dohodli, že návrh Smlouvy či jeho přijetí mohou být Bankou doručeny Klientovi rovněž prostřednictvím Služeb přímého bankovníctví. Příslušná aplikace Služeb přímého bankovníctví je pak pro tyto účely korespondenční adresou Klienta; Banka může Klientovi zaslat příslušnou reakci (například odmítnutí či přijetí návrhu) jinou Službou přímého bankovníctví, než kterou ji Klient kontaktoval (např. přijetí návrhu Smlouvy, jež Klient podal pomocí Mobilního bankovníctví, může být Klientovi doručeno pomocí Internetového bankovníctví), nebo zcela odlišným komunikačním prostředkem.
- 2.4. Autentizační či Certifikační kód 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 bankovníctví

- 3.1. Banka provozuje Služby přímého bankovníctví 24 hodin denně. Ačkoliv jsou obvykle technické prostředky nezbytné pro využití Služeb přímého bankovníctví Uživateli stále dostupné, Banka se nezavazuje umožnit jejich využití bez přerušování a nepřetržitě. Banka je oprávněna přerušit nebo omezit poskytování Služeb přímého bankovníctví na dobu nezbytnou k údržbě zařízení potřebných k jejich provozu.
- 3.2. Klient je povinen seznámit Uživatele s podmínkami Služeb přímého bankovníctví.
- 3.3. Banka není povinna kontrolovat věcnou správnost údajů uváděných Uživatelem prostřednictvím Služeb přímého bankovníctví.

- 3.4. Zadaním příslušného Certifikačního kódu, T-PIN, I-PIN, S-PIN či 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, T-PIN, I-PIN, S-PIN či jiný Elektronický identifikační prostředek nebo jejich kombinace vyžadovány. 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 bankovníctví.
- 3.6. Služba Informuj mě zahrnuje zasílání různých zpráv na základě požadavku Uživatele. Zprávy o Platebních transakcích a karetních blokácích 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).
- 3.7. Provoz Internetového bankovníctví  
Banka umožňuje Uživatelům Internetového bankovníctví komunikovat s Bankou prostřednictvím veřejné datové sítě Internet. Adresa pro přihlášení do Internetového bankovníctví je uvedena na Veřejných stránkách a podle Uživatelem používaného typu Elektronického klíče se může lišit.
- 3.8. Provoz Mobilního bankovníctví  
Banka umožňuje Uživatelům Mobilního bankovníctví komunikovat s Bankou prostřednictvím aplikace v Mobilním zařízení, která využívá datové připojení k síti Internet. Aplikace je k dispozici ke stažení v marketech aplikací 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.
- 3.9. Provoz Telefonního bankovníctví  
Banka umožňuje Uživatelům Telefonního bankovníctví komunikovat s Bankou prostřednictvím veřejné telefonní sítě. Telefonní bankovníctví 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 bankovníctví přístupné na infolince uvedené rovněž na Veřejných stránkách a náklady telefonického spojení při hovorech ze zahraničí nese Uživatel.
- 4. Bezpečnost Služeb přímého bankovníctví**
- 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 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 bankovníctví, a kterých může Uživatel získat maximálně pět (5);
- c) Elektronické identifikační prostředky jsou nepřenositelné 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 bankovníctví;
- 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;
- g) Uživatel je povinen měnit pravidelně (alespoň jedenkrát za tři [3] měsíce) číselné kódy I-PIN a T-PIN pro zachování maximální bezpečnosti realizovaných Pokynů a Pokynů ke Smlouvě a Uživatel je rovněž povinen změnit číselné kódy I-PIN a T-PIN, pokud jej k tomu Banka vyzve;
- h) Uživatel je povinen učinit veškerá opatření k zajištění bezpečnosti užívání Služeb přímého bankovníctví, zejména nezaznamenávat svá hesla a kódy ve snadno rozeznatelné podobě a nesdělovat je třetím osobám, chránit své Elektronické identifikační prostředky před odcizením nebo zneužitím jakoukoliv osobou;
- 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);
- j) Uživatel je povinen v případě podezřelých dotazů obrátit se na Banku prostřednictvím infolinky 800 900 900, zejména v případě, kdy si není jist, že komunikuje se zástupcem Banky;
- k) Uživatel je povinen chovat se na internetu obezřetně, zejména nevyužívat pro přístup ke Službám přímého bankovníctví veřejně přístupná technická zařízení nebo technické zařízení, jehož bezpečné použití pro přístup ke Službám přímého bankovníctví Uživatel neověřil nebo ověřit nemohl. Další informace o bezpečném využití Služeb přímého bankovníctví jsou zpřístupněny na Veřejných stránkách;
- l) Klient uzavřením jakékoliv smlouvy, jejíž součástí jsou tyto Produktové podmínky, prohlašuje, že se seznámil a je srozuměn s doporučeními týkajícími se bezpečnosti Služeb přímého bankovníctví, které jsou uvedeny v dokumentu „Bezpečnost Služeb přímého bankovníctví, 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.
- 4.2. Bezpečnost Internetového bankovníctví  
Přístup do Internetového bankovníctví je chráněn Elektronickými klíči.
- 4.2.1. Mobilní Elektronický klíč SIM Toolkit nebo SMS:
- a) pro přihlášení do Internetového bankovníctví Uživatel vždy použije své Klientské číslo a Autentizační kód vygenerovaný Bankou a zasláný na Mobilní telefon Uživatele, který je registrován jako Mobilní Elektronický klíč (MEK). Kód zasláný 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;
- b) pro podepsání Pokynů a Pokynů ke Smlouvě Uživatel používá Certifikační kód, jenž je vygenerovaný Bankou a zasláný na Mobilní telefon Uživatele, který je registrován jako Mobilní Elektronický klíč. Kód zasláný 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;
- c) v případě, že Uživatel oznámí Bance ztrátu, zapomenutí, vyzrazení

- třetí osobě, neautorizované nebo podvodné použití nebo požádá o blokadu I-PINu, Banka vydá nový I-PIN na základě žádosti Uživatele, případně vytvoření nového I-PINu v součinnosti s Uživatelem zajistí;
- d) z bezpečnostních důvodů Banka provede automaticky blokadu I-PINu po třech neplatných pokusech zadat I-PIN. Banka vydá nový I-PIN na základě písemné žádosti Uživatele;
- e) v případě zničení, ztráty, blokace Mobilního telefonu, SIM karty nebo jiné změny na telefonním čísle používaném pro zaslání Autentizačních a Certifikačních kódů je Uživatel povinen tuto skutečnost Bance neprodleně oznámit. V takovém případě je Banka oprávněna provést blokadu příslušného Elektronického klíče a na základě žádosti Uživatele též přenastavení příslušného Elektronického klíče.
- 4.2.2. Osobní Elektronický klíč:
- a) pro přihlášení do Internetového bankovníctví Uživatel vždy použije své Klientské číslo a online Autentizační kód vygenerovaný OEK. Tento Autentizační kód má časově omezenou platnost;
- b) 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;
- c) v případě zničení, ztráty, poruchy nebo odcizení OEK je Uživatel povinen tuto skutečnost Bance neprodleně oznámit. V takovém případě je Banka oprávněna provést blokadu OEK a na základě písemné žádosti Uživatele vydat nový OEK.
- 4.3. Bezpečnost Mobilního bankovníctví  
Přístup do Mobilního bankovníctví je chráněn zvoleným heslem (S-PIN) a Smartphone Elektronickým klíčem instalovaným v mobilním zařízení. Obojí Uživatel získá v průběhu aktivace služby Mobilního bankovníctví.
- 4.3.1. Smartphone Elektronický klíč
- a) Uživatel si vytvoří Smartphone Elektronický klíč v prostředí Internetového bankovníctví, kam se přihlásí pomocí svého Klientského čísla a Autentizačního kódu vygenerovaného jedním z Elektronických klíčů, které slouží pro přístup do Internetového bankovníctví;
- b) v aplikaci Mobilního bankovníctví si v průběhu aktivace uživatel zvolí S-PIN (čtyř až osmimístné číslo);
- c) 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;
- d) z bezpečnostních důvodů Banka provede automaticky blokadu S-PINu po pěti (5) neplatných pokusech zadat S-PIN. Banka umožní vytvoření nového S-PINu na základě žádosti Uživatele v Internetovém bankovníctví, která bude podepsána Certifikačním kódem získaným pomocí Elektronického klíče, jenž slouží Uživateli pro přístup do Internetového bankovníctví a pro jeho obsluhu;
- e) v případě zničení, ztráty, blokace nebo jiného důvodu ukončení používání mobilního zařízení, na němž byl vytvořen Smartphone Elektronický klíč, je Uživatel povinen provést blokadu takového Elektronického klíče v Internetovém bankovníctví.
- 4.4. Bezpečnost Telefonního bankovníctví  
Využití služeb Telefonního bankovníctví je chráněno Elektronickými klíči.
- 4.4.1. 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 zasláný 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 blokadu T-PIN, Banka vydá nový T-PIN na základě písemné žádosti Uživatele;
- c) z bezpečnostních důvodů Banka provede automaticky blokadu 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 zaslání Autentizačních kódů je Uživatel povinen tuto skutečnost Bance neprodleně oznámit. V takovém případě je Banka oprávněna provést blokadu příslušného Elektronického klíče.
- 4.4.2. 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 blokadu OEK a na základě písemné žádosti Uživatele vydat nový OEK.
- 4.5. 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 bankovníctví, 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 bankovníctví, poruchami telefonní sítě, sítě datové nebo poruchami na straně mobilního operátora nebo poskytovatele internetového připojení. V případě, že prostřednictvím Služeb přímého bankovníctví 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 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](http://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.
- 7.3. Tyto Produktové podmínky nabývají účinnosti dne 13. 1. 2018 a nahrazují Produktové podmínky služeb přímého bankovníctví, které nabývaly účinnosti dne 1. 4. 2017.

## 8. Vymezení pojmů

Pojmy označené velkými písmeny nevyomezené 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 bankovníctví. 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.

**Elektronické klíče** znamenají prostředky umožňující Uživateli provedení 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. 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 zasílanou na určené telefonní číslo nebo textovou zprávu zasílanou na e-mailovou adresu Uživatele, jejímž prostřednictvím může být Uživatel informován o zůstatku a pohybech na Účtu nebo o jiných skutečnostech.

**Informuj mě** znamená službu zasílání Informačních zpráv.

**Internetové bankovníctví** 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 bankovníctví v kombinaci s Mobilním Elektronickým klíčem SMS.

**Klientské číslo** znamená jednoznačné číselné označení identity Uživatele pro Služby přímého bankovníctví, 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 na Mobilním zařízení. Kódy takto doručené lze použít v kombinaci s T-PINem prostřednictvím Telefonního bankovníctví a v kombinaci s I-PINem prostřednictvím Internetového bankovníctví.

**Mobilní bankovníctví** 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 bankovníctví. Jeho použití je chráněno čtyřmístným číselným kódem (PIN).

**Služby přímého bankovníctví** znamenají služby Internetového, Mobilního a Telefonního bankovníctví.

**Smartphone Elektronický klíč nebo též SPEK** znamená funkčnost v rámci aplikace Mobilního bankovníctví, 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 bankovníctví.

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

**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 bankovníctví** 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 bankovníctví v kombinaci s Mobilním Elektronickým klíčem SMS.

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