

**PRODUKTOVÉ OBCHODNÍ
PODMÍNKY PRO INTERNETOVÉ
A ELEKTRONICKÉ BANKOVNICTVÍ**
UniCredit Bank
Czech Republic and Slovakia, a.s.

Obsah

PREAMBULE

1 OBECNÁ USTANOVENÍ

2 OSOBY UŽÍVAJÍCÍ INTERNETOVÉ A ELEKTRONICKÉ BANKOVNICTVÍ

3 PRAVIDLA BEZPEČNOSTI INTERNETOVÉHO A ELEKTRONICKÉHO BANKOVNICTVÍ

4 PŘIHLÁŠENÍ DO APLIKACE IEB, AUTENTIZACE, AKTIVACE APLIKACE IEB A AUTORIZACE PLATEBNÍ TRANSAKCE, NEPLATEBNÍHO PŘÍKAZU NEBO POKYNU K NASTAVENÍ

5 ODPOVĚDNOST ZA NEAUTORIZOVANOU NEBO NESPRÁVNĚ PROVEDENOU PLATEBNÍ TRANSAKCI

6 ZVLÁŠTNÍ USTANOVENÍ O ODPOVĚDNOSTI

7 DOSTUPNOST A BLOKACE INTERNETOVÉHO A ELEKTRONICKÉHO BANKOVNICTVÍ

8 ZVLÁŠTNÍ USTANOVENÍ PRO ELEKTRONICKÉ BANKOVNICTVÍ

9 BANKOVNÍ IDENTITA

10 ZÁVĚREČNÁ USTANOVENÍ

PREAMBULE

1. UniCredit Bank Czech Republic and Slovakia, a.s., IČO 64948242, zapsaná v obchodním rejstříku vedeném Městským soudem v Praze v oddíle B, vložce 3608, (dále též jen „Banka“) poskytuje svým klientům, jimž vede účet, (dále jen „Klienti“ nebo „Majitelé účtu“) službu internetové a elektronické bankovnictví (dále také jen „IEB“) na základě příslušné smlouvy umožňující Majitelům účtu při použití příslušného zařízení obsluhu sjednaných bankovních produktů, jako je např. účet, platební karta, úvěr, bankovní záruka, pojištění, investice apod., jejich sjednávání uzavřením příslušné produktové smlouvy (dále jen „Produktová smlouva“) a také zabezpečenou komunikaci mezi Klientem a Bankou prostřednictvím sítě Internet (dále vše souhrnně jen „Produkty internetového a elektronického bankovnictví“ nebo „Produkty IEB“). Produkty IEB jsou k dispozici jak v internetovém bankovnictví (dále jen „IB“), tak v elektronickém bankovnictví (dále jen „EB“).

IB může být poskytováno prostřednictvím webových aplikací Online Banking, BusinessNet Professional, BusinessNet a Trade Finance Gate (dále jen „Webové aplikace IB“) a prostřednictvím mobilních aplikací Smart Banking, Business Smart Banking a BusinessNet Mobile (dále jen „Mobilní aplikace IB“), (dále souhrnně „Aplikace IB“). EB může být poskytováno prostřednictvím aplikací Eltrans 2000 (Gemini 5.0) a MultiCash (dále jen „Aplikace EB“). „Aplikace IB“ a „Aplikace EB“ se dále také souhrnně označují jako „Aplikace IEB“. Pod pojmem „zařízení“ se rozumí zejména mobilní telefon, tablet, počítač nebo jakékoli jiné zařízení, z něhož je možno se přihlásit do internetového a elektronického bankovnictví a poté užívat Produkty IEB.

2. Tyto Produktové obchodní podmínky pro internetové a elektronické bankovnictví UniCredit Bank Czech Republic and Slovakia, a.s., (dále jen „Produktové podmínky IEB“) jsou účinné od 1. 4. 2025 a v plném rozsahu ruší a nahrazují dosud účinné Produktové obchodní podmínky pro poskytování Produktů internetového bankovnictví UniCredit Bank Czech Republic and Slovakia, a.s., dosud účinné Produktové obchodní podmínky pro poskytování Produktů přímého bankovnictví UniCredit Bank Czech Republic and Slovakia, a.s., a dosud účinné Produktové obchodní podmínky pro poskytování Produktů elektronického bankovnictví UniCredit Bank Czech Republic and Slovakia, a.s.

1 OBECNÁ USTANOVENÍ

- 1.1 Banka poskytuje Produkty IEB za podmínek stanovených příslušnou Produktovou smlouvou, Obecnými obchodními podmínkami UniCredit Bank Czech Republic and Slovakia, a.s., ve znění platném k okamžiku vzniku smluvního vztahu, pokud nedojde k jejich změně podle jejich čl. 3, (dále jen „Obecné obchodní podmínky“), těmito Produktovými podmínkami IEB, příslušnými produktovými podmínkami týkajícími se Produktové smlouvy a právními předpisy. Pokud je užívání příslušného Produktu IEB zpoplatněno, je poplatek uveden v Sazebníku odměn za poskytování bankovních služeb UniCredit Bank Czech Republic and Slovakia, a.s., platném pro příslušný segment (dále jen „Sazebník“) a Banka je v takovém případě oprávněna účtovat příslušný poplatek uvedený v Sazebníku a Klient je povinen jej hradit.
- 1.2 Přehled dostupných služeb a funkcionalit Produktů IEB, jakož i výčet technických požadavků kladených na zařízení umožňující přístup k Produktům IEB je uveden v příslušném Přehledu služeb a parametrů internetového bankovnictví a v Přehledu služeb a parametrů elektronického bankovnictví, přičemž aktuálně platné přehledy služeb a parametrů jsou zveřejněny na internetových stránkách Banky www.unicreditbank.cz a jsou přístupné rovněž na obchodních místech Banky.
- 1.3 Banka je oprávněna Produktové podmínky IEB změnit nebo do nich doplnit nové ustanovení, vyvstane-li rozumná potřeba takové změny nebo doplnění, například potřeba změnit či nově výslovně upravit určitá práva a povinnosti stran v návaznosti na změnu právního předpisu, dostupných technologií, situace na finančních trzích nebo obchodní politiky Banky. Znění změn a doplňků nebo úplné znění takto novelizovaných Produktových podmínek IEB Banka zašle Klientovi nejpozději 2 měsíce před datem navrhované účinnosti takové novelizace jakýmkoli způsobem dohodnutým pro komunikaci mezi Bankou a Klientem v rámci příslušného smluvního vztahu. Banka může Klienta informovat o změnách těchto Produktových podmínek IEB i v elektronické podobě. Pokud Klient s navrženou novelizací Produktových podmínek IEB nebude souhlasit, je oprávněn z tohoto důvodu příslušný smluvní vztah písemně vypovědět s účinností k datu bezprostředně předcházejícímu datu účinnosti navržené novelizace nebo, pokud takové právo Klientovi zakládá zákon, s okamžitou účinností. Pokud Klient návrh Banky neodmítne, stává se nové znění Produktových podmínek IEB závazným pro uzavřený smluvní vztah jako změna původně sjednaných podmínek smluvního vztahu, a to s účinností ode dne uvedeného v příslušné novelizaci Produktových podmínek IEB jako den nabytí platnosti nového znění Produktových podmínek IEB.
- 1.4 V případě, že se práva a povinnosti stran upravené Produktovými podmínkami IEB změní přímo v důsledku změny právního předpisu, od něhož se nelze smluvně odchýlit, nepostupuje se podle předchozího odstavce. O takové změně bude Banka Klienta informovat.
- 1.5 Příslušné Aplikace IEB, pokud je to možné technicky, mohou být použity jako prostředek komunikace na dálku mezi Klientem a Bankou, popř. Klientem a třetí stranou, a ke sjednávání smluv o finančních službách uzavíraných na dálku včetně jejich změn. Při sjednávání smluv je autorizace nebo souhlas potvrzený osobním bezpečnostním prvkem (viz čl. 3.1) ekvivalentní podpisu klienta na papírovém nosiči.
- 1.6 Banka je oprávněna do IEB Klientovi poskytovat informace, zasílat návrhy smluv a jejich změn a další relevantní korespondenci. Informace a dokumenty takto zaslané Bankou se považují za doručené dnem, kdy jsou doručeny do schránky příslušné Aplikace IEB, nebo dnem instalace služeb IEB, tj. okamžikem, kdy se dostanou do sféry vlivu Klienta.
- 1.7 Banka informuje Majitele účtu prostřednictvím Aplikací IEB o zůstatcích prostředků na účtech a o provedených transakcích. Majitel účtu je povinen – buď osobně, nebo prostřednictvím Uživatele definovaného v kapitole 2 níže – kontrolovat, zda zadané příkazy byly Bankou provedeny či odmítnuty a zda zprávy o zúčtování odpovídají zadaným příkazům. Zároveň je povinen kontrolovat i veškeré neplatební transakce, včetně příchodících transakcí jemu avizovaných. Zjištěné závady nebo jiné nesrovnalosti je Majitel účtu nebo Uživatel povinen oznámit Bance bez zbytečného odkladu. Pokud Uživatel neuplatnil reklamaci nejpozději do 30 dnů ode dne jejich zobrazení v příslušné aplikaci IEB, aniž by mu v tom bránilo objektivní nepřekonatelné překážky, platí, že reklamaci neuplatnil bez zbytečného odkladu.

- 1.8** Na základě technického a obchodního vývoje může Banka do IEB přidávat nové aplikace/funkce a vyřazovat již neaktuální aplikace/funkce, měnit aplikace, jejich názvy a jejich funkcionality. Banka je rovněž oprávněna s ohledem na zajištění co nejvyšší úrovně bezpečnosti Produktů IEB ukončit používání osobních bezpečnostních prvků nebo upravit jejich nastavení v případě, že v důsledku příčin existujících mimo kontrolu Banky hrozí snížení úrovně jejich bezpečnosti, a to po předchozím upozornění Klienta prostřednictvím Aplikace IEB, které se úprava týká, nebo písemně nejpozději 2 měsíce přede dnem, kdy má ke změně v nastavení Aplikace IEB dojít.
- 1.9** Banka může Klientovi zpřístupnit všechny aktuálně nabízené Produkty IEB a může k těmto Produktům připojit všechny jeho aktuálně i v budoucnu otevřené účty, platební karty a další produkty Banky. Banka umožní Klientovi změnit sadu připojených účtů k jednotlivým Produktům IEB, úroveň oprávnění a výši limitů.

2 OSOBY UŽÍVAJÍCÍ INTERNETOVÉ A ELEKTRONICKÉ BANKOVNICTVÍ

- 2.1** Osoba, která má přístup k Produktům IEB, může být Majitelem účtu, Správcem uživatelských oprávnění (dále jen „Správce“) nebo Uživatelem v závislosti na konkrétní roli v dané situaci. Tyto role se navzájem nevylučují, a proto určitá osoba může vystupovat jen v některé z těchto rolí, v několika rolích nebo ve všech rolích najednou.
- 2.2** Majitel účtu odpovídá za to, že Banka bude mít vždy aktuální osobní údaje osoby, která má přístup k Produktům IEB, aby ji mohla řádně identifikovat.
- 2.3** Uživatelem Produktů IEB je:
- a) Majitel účtu nebo spolužadatel o danou bankovní službu, pokud sám využívá Produkty IEB, nebo
 - b) Správce, nebo
 - c) další osoba, která Majitel účtu nebo Správce udělil zmocnění využívat Produkty IEB.
- 2.4** Správce je zvláštní kategorie Uživatele, jehož Majitel účtu zmocnil, aby v Aplikacích IEB jiným Uživatelům přiděloval, měnil nebo odebíral uživatelská oprávnění. Správce může přidělovat, měnit i odebírat uživatelská oprávnění rovněž sám sobě, pokud k tomu byl Majitelem účtu zmocněn.
- 2.5** Podmínkou přístupu Uživatele do Produktů IEB je uzavření příslušné smlouvy Majitelem účtu a souhlas Uživatele s těmito Produktovými podmínkami IEB při prvním vstupu do Produktů IEB, pokud je neodsouhlasil dříve.
- 2.6** Určením Uživatele ve smyslu předchozího odstavce dává Majitel účtu Bance souhlas k tomu, aby Banka této osobě poskytovala veškeré informace, které by jinak podléhaly bankovnímu tajemství, a dále k tomu, aby Uživatel v zastoupení Majitele účtu přijímal písemnosti, které Majiteli účtu Banka v souladu s čl. 1.6 zasílá. Informace a písemnosti zaslané Bankou se považují za doručené rovněž Majiteli účtu dnem, kdy jsou podle čl. 1.6 doručeny Uživateli.
- 2.7** Zmocnění Uživatele pozbývá platnosti:
- a) ke dni zrušení posledního bankovního produktu, k němuž se vztahuje Uživatelské zmocnění,
 - b) odvoláním zmocnění Majitelem účtu nebo Správcem,
 - c) výpovědí zmocnění Uživatelem,
 - d) úmrtím Uživatele.
- 2.8** Přístup Uživatele do IEB bude zrušen nejpozději do konce následujícího pracovního dne po dni doručení sdělení Majitele účtu či výpovědi zmocnění Uživatele, pokud v něm nebude stanoven den pozdější.
- 2.9** Pokud dojde u Majitele účtu právnické osoby ke změně ve funkci člena jejího statutárního orgánu, který vystupoval v roli Uživatele, zůstávají zachována jeho práva Uživatele až do okamžiku, kdy bude nastaven nový Uživatel, a to po předání takového pokynu Bance Majitelem účtu právnickou osobou.

3 PRAVIDLA BEZPEČNOSTI INTERNETOVÉHO A ELEKTRONICKÉHO BANKOVNICTVÍ

- 3.1** Pojmy a charakteristiky osobních bezpečnostních prvků:

PIN pro mobilní aplikaci	Číselný kód pro Mobilní aplikace IB, který se používá při aktivaci, přihlášení nebo pro autorizaci transakcí.
Heslo pro přihlášení	Heslo se skládá z numerických znaků. Používá se ve Webových aplikacích IB v kombinaci s jednorázovým SMS kódem. Uživatel je povinen ihned změnit úvodní heslo poskytnuté Uživateli Bankou.
Bezpečnostní klíč (Smart klíč, Business klíč)	Funkce obsažená v Mobilních aplikacích IB, která je určena pro přihlášení do Aplikací IB nebo pro autorizaci platebních transakcí a jiných požadavků nebo pro generování jednorázových číselných kódů pro přihlášení nebo autorizaci transakcí ve Webových aplikacích IB i bez připojení zařízení k internetu (tzv. režim offline).
Hardwarový bezpečnostní klíč (token)	Hardwarové zařízení chráněné PINem, určené pro generování jednorázových číselných kódů pro přihlášení nebo autorizaci transakcí ve Webových aplikacích IB.
SMS klíč	Kombinace hesla a jednorázových kódů zaslaných prostřednictvím SMS na mobilní telefon Uživatele pro přihlášení nebo autorizaci transakcí ve Webových aplikacích IB.

Registrované mobilní telefonní číslo	Telefonní číslo, které Uživatel Bance oznámí a které umožňuje přijímat jednorázové bezpečnostní kódy, tzv. SMS OTP (OTP znamená One-Time Password neboli jednorázové heslo).
Registrovaná e-mailová adresa	E-mailová adresa, kterou Uživatel Bance oznámí a která umožňuje Uživateli přijímat jednorázové bezpečnostní kódy (e-mail OTP).
Otisk prstu (biometrie)	Otisk prstu uložený v mobilním zařízení, ve kterém je aktivována Mobilní aplikace IB.
Sken tváře (biometrie), tzv. Face ID	Sken tváře uložený v mobilním zařízení, ve kterém je aktivována Mobilní aplikace IB. Sken tváře se porovnává s biometrickými údaji uloženými u Banky nebo vůči fotografií Uživatele (např. z identifikačního dokladu).
Heslo (např. pro komunikaci s bankou, statické heslo, přístupové apod.)	Heslo skládající se z různých alfanumerických znaků, které slouží k ověření Uživatele v různých situacích.
Jednorázové bezpečnostní heslo (OTP = One-Time Password)	Jednorázový bezpečnostní kód, pomocí něhož lze ověřit vlastnictví bezpečnostního prvku. Je to kód zasílaný na registrované mobilní telefonní číslo, na registrovanou e-mailovou adresu nebo generovaný Mobilní aplikací IB.
Uživatelské jméno	Přidělené nebo v určitých případech samostatně nastavitelné uživatelské jméno (alias) určené pro přihlášení do Aplikace IEB.
Uživatelské číslo	Číslo přidělené Uživateli Bankou.
Průkaz totožnosti	Doklad vydaný Uživateli orgánem veřejné správy, v němž je uvedeno jméno a příjmení, datum narození a z něhož je patrná podoba (např. občanský průkaz, řidičský průkaz, cestovní pas).
Rodné číslo	Rodné číslo přidělené Uživateli.
Kontrolní otázka	Otázka týkající se Uživatele nebo jeho produktů.
Kód CVV2/CVC2	Zvláštní trojmístné číslo, které je uvedeno na platební kartě. Je to osobní bezpečnostní prvek používaný k identifikaci držitele karty v prostředí bez přítomnosti platební karty (např. internet).
Číslo platební karty	Unikátní 16místné číslo platební karty.
Klientský certifikát	Certifikát sloužící k autentizaci (ověření totožnosti) Uživatele. Umožňuje stažení a rozšířování důvěrných pasivních informací (výpisy, zůstatky atd.) v aplikaci Eltrans 2000 (Gemini 5.0).
Elektronický/Digitální podpis	Označení specifických dat, která v počítači nahrazují klasický vlastnoruční podpis, respektive ověřený podpis (týká se Aplikací EB).

3.2 Uživatel je povinen seznámit se zejména:

- a) s možnostmi nastavení osobních bezpečnostních prvků,
- b) s možnostmi nastavení osobních bezpečnostních limitů pro omezení výše platební transakce,
- c) s níže uvedenými povinnostmi ohledně ochrany osobních bezpečnostních prvků a s postupem v případě ztráty, odcizení, zneužití nebo neoprávněného použití osobního bezpečnostního prvku.

3.3 Uživatel je povinen přijmout příslušná opatření na ochranu svých osobních bezpečnostních prvků tak, aby nemohlo dojít k jejich ztrátě, odcizení, zneužití nebo neoprávněnému použití. Zejména je povinen:

- a) Nepoužívat hesla a PINy v jiných aplikacích a na internetu (např. v e-shopech, na sociálních sítích, v e-mailech apod.) shodná s hesly a PINy používanými pro přihlašování do IEB nebo pro autorizaci platebních transakcí.
- b) Nastavit si heslo nebo PIN tak, aby nebyly jednoduše uhodnutelné nebo odvoditelné, např. kombinací malých a velkých písmen, číslic, speciálních znaků apod.
- c) Nesdělovat druhým osobám ani nikam na internetu nezadávat svůj osobní bezpečnostní prvek, vyjma přihlašování do Webových aplikací IB na stránkách <https://cz.unicreditbanking.eu>, <https://cz.unicreditbanking.net> a <https://corporateportal.unicreditgroup.eu/container/cz/login>.
- d) Hesla a PINy si nepoznamenávat, chránit je před vyzrazením a neprodleně je změnit v případě, že došlo k jejich vyzrazení, nebo jestliže má Uživatel pouhé podezření, že tato situace nastala.
- e) Dbát zvýšené opatrnosti při zadávání osobních bezpečnostních prvků na veřejnosti (např. ve vozidlech hromadné dopravy) nebo v monitorovaných místnostech (např. v blízkosti bezpečnostních kamer), aby je nemohly zpozorovat jiné osoby.
- f) Nepřihlašovat se do internetového bankovníctví na zařízení, které nemá Uživatel plně pod svou kontrolou (např. ve veřejných internetových kavárnách, na počítačích sdílených více lidmi) nebo si není jist, že na něm není nainstalován škodlivý program.
- g) Sdělovat heslo pro komunikaci s Bankou pouze pracovníkovi Banky v situaci, kdy je toto heslo vyžadováno.

- h)** Chránit odblokování a použití SIM PINem, a pokud dojde ke ztrátě nebo odcizení mobilního zařízení, nechat SIM kartu bezodkladně zablokovat u operátora.
- i)** Chránit svůj profil u mobilního operátora a nepřipustit, aby si třetí osoba nechala vystavit novou SIM/eSIM k telefonnímu číslu Uživatele.
- j)** Neumožnit přístup ke svému e-mailovému účtu dalším osobám a nastavit si dvoufaktorové/dvoufázové ověření.
- k)** Neumožnit cizí osobě přístup do svého mobilního zařízení (např. otiskem prstu, skenem tváře, heslem, PINem).
- l)** Pokud došlo ke ztrátě nebo odcizení mobilního telefonu (nebo SIM karty), neprodleně tuto událost oznámit Bance a internetové nebo elektronické bankovníctví nechat preventivně zablokovat.
- m)** Neumožnit registraci biometrických údajů cizí osoby (ani členů rodiny) do mobilního zařízení.
- n)** Zabezpečit přístup do mobilního zařízení heslem, PINem nebo biometricky (otisk prstu, sken tváře) a nenechávat své mobilní zařízení bez dozoru, případně bez automatického zamykání zařízení (obrazovky) po krátké době.
- o)** Nepoužívat programové úpravy mobilního zařízení, které umožňují plný administrátorský přístup do něj (např. jailbreak, root).
- p)** Pravidelně aktualizovat operační systém svého mobilního zařízení i jednotlivých instalovaných aplikací.
- q)** Používat na svém mobilním zařízení nejnovější verzi bezpečnostních programů (např. antivír, firewall).
- r)** Nepovolovat nadbytečná oprávnění v nově instalované nebo aktualizované aplikaci ve svém mobilním zařízení (např. přístup k SMS, usnadnění nastavení apod.).
- s)** Instalovat do svého mobilního zařízení pouze aplikace z oficiálních obchodů s aplikacemi – Google Play (Android), App Store (iOS) – včetně případných doplňků, jestliže je používána aplikace vyzývá doinstalovat, nastavit si na svém mobilním zařízení zákaz instalace aplikací z neznámých zdrojů.
- t)** Neinstalovat aplikace na základě pokynů cizí osoby a zejména cizím osobám nepovolovat vzdálený přístup do mobilního telefonu (např. přes aplikaci AnyDesk).
- u)** Nepřihlašovat se na počítač jako administrátor, pokud to není nutné, ale jako běžný uživatel.
- v)** Aktualizovat pravidelně operační systém a své programy, zejména internetový prohlížeč. Instalovat rozšíření (plug-iny) prohlížeče v omezené míře a pouze od známých a důvěryhodných vydavatelů.
- w)** Používat nejnovější verzi bezpečnostních programů (např. antivír, firewall) a pravidelně je aktualizovat.
- x)** Chránit počítač před neoprávněným přístupem dalších osob nastavením přístupových oprávnění, zabezpečením heslem, případně dalšími prvky. Nepovolit cizí osobě vzdálený přístup do počítače (např. přes software AnyDesk).
- y)** Zadávat adresu internetové stránky Banky ručně. Pro přístup do IB využít internetovou stránku Banky www.unicreditbank.cz, odtud přejít na přihlašovací stránku IB, zkontrolovat, že přistupuje na příslušnou internetovou stránku Webové aplikace IB definovanou v bodě 3.3 c), a nepoužívat zástupce na přihlašovací stránku internetového bankovníctví.
- z)** Nepřistupovat do internetového bankovníctví přes odkaz z vyhledávače ani odkaz zasláný e-mailem, SMS nebo jiným způsobem (na sociální síti, přes chatovací aplikaci atd.).
- aa)** Nepřihlašovat se v případě, že se Uživateli zdá přihlašovací obrazovka k Produktům IEB podezřelá.
- bb)** Bez odkladu kontaktovat Banku, pokud Uživatel zaregistruje operaci, kterou neautorizoval.
- cc)** Nereagovat na telefonáty, které Uživatele vybízejí k akci s účtem, protože Banka nikdy telefonicky nevyzývá své Klienty k jakýmkoli transakcím.
- dd)** Neotvírat e-mail obsahující jméno Banky, pokud nepřišel z domény unicreditbank.cz nebo unicreditgroup.cz, neotvírat přílohy nestandardního typu souboru (např. přípony .exe, .php) a neklikat na odkazy obsažené v podezřelé zprávě.
- ee)** Seznamovat se se zprávami zaslány Bankou do internetového bankovníctví nebo do mobilního telefonu, zejména pokud jde o varování před podvodem.

3.4 Je-li Majitel účtu nebo Uživatel:

- a)** nezletilý, odpovídá za ochranu osobních bezpečnostních prvků a bezpečné užívání Produktů IEB zákonný zástupce.
- b)** zastoupen soudem jmenovaným opatrovníkem, odpovídá za ochranu osobních bezpečnostních prvků a bezpečné užívání Produktů IEB opatrovník.

4 PŘIHLÁŠENÍ DO APLIKACE IEB, AUTENTIZACE, AKTIVACE APLIKACE IEB A AUTORIZACE PLATEBNÍ TRANSAKCE, NEPLATEBNÍHO PŘÍKAZU NEBO POKYNU K NASTAVENÍ

- 4.1** Při přihlášení do Aplikace IEB Banka autentizuje Uživatele prostřednictvím příslušné kombinace osobních bezpečnostních prvků uvedených v kapitole 3.
- 4.2** Uživatel autorizuje platební transakci, aktivuje příslušnou Aplikaci IEB, poskytuje souhlas s uzavřením smlouvy, uděluje Bance neplatební příkaz, pokyn k nastavení Produktu IEB apod. řádným použitím svých bezpečnostních prvků a stiskem potvrzovacího tlačítka v příslušné Aplikaci IEB.

- 4.3** Banka provede platební transakci, neplatební příkaz nebo pokyn k nastavení, obsahují-li úplná data odpovídající předepsaným formátům a jsou-li autorizovány v závislosti na příslušné Aplikaci IEB v souladu s těmito Produktovými podmínkami IEB. Banka neodpovídá za škody vzniklé neprovedením platebních příkazů nesplňujících příslušné podmínky.
- 4.4** V Mobilních aplikacích IB probíhá aktivace pomocí aktivčního kódu generovaného Bankou a doručeného Uživateli prostřednictvím SMS a PINu definovaného Uživatelem.
- 4.5** V Mobilních aplikacích IB probíhá autorizace následujícím způsobem:
- otiskem prstu či přiložením (skenem) obličeje k zařízení poté, co je k tomu Uživatel vyzván,
 - zadáním PINu poté, co je k tomu Uživatel vyzván.
- 4.6** Ve Webových aplikacích IB probíhá přihlášení a autorizace některým z těchto způsobů:
- Bezpečnostním klíčem, a to:
 - Smart klíčem – online metodou pro přihlášení do Aplikací IB – kdy Uživatel obdrží do aplikace Smart Banking oznámení, tzv. push notifikaci, a poté potvrdí operaci biometricky (otiskem prstu či skenem obličeje) nebo zadáním PINu.
 - Smart klíčem – offline metodou pro přihlášení do Aplikací IB – kdy Aplikace IB zobrazí na přihlašovací stránce QR kód, který Uživatel ofotí prostřednictvím Smart klíče v mobilní aplikaci Smart Banking, Smart klíč vygeneruje 6místný jednorázový kód, který Uživatel přepíše do aplikace Online Banking a potvrdí.
 - Business klíčem – offline metodou pro přihlášení do aplikací BusinessNet Professional, BusinessNet a Trade Finance Gate – kdy Uživatel vygeneruje 6místný kód pro přihlášení prostřednictvím Smart klíče v mobilní aplikaci Business Smart Banking, resp. BusinessNet Mobile.
 - SMS klíčem
Tato metoda se skládá z kombinace osobního hesla a jednorázových kódů zaslanych na mobilní telefon Uživatele. Uživatel zadá své statické heslo a poté Banka odešle Uživateli SMS obsahující OTP na mobilní telefon určený Uživatelem. Tento časově omezený kód Uživatel přepíše zpět do Webové aplikace IB a potvrdí tím operaci.
 - Hardwarovým bezpečnostním klíčem (tokenem)
Heslo pro podpis operace je vygenerováno tokenem. Uživatel zadá PIN přímo na klávesnici tokenu. V případě zadání správného PINu token vygeneruje 8místný jednorázový kód, který Uživatel přepíše do Webové aplikace IB. Aplikace poté zobrazí 6místný jednorázový kód (OTP), který Uživatel přepíše opět do Webové aplikace IB a tím operaci potvrdí.
- 4.7** Přihlášení do Aplikací EB probíhá jedním z následujících způsobů: zadáním uživatelského jména a hesla, pomocí elektronického/digitálního podpisu nebo prostřednictvím systémového uživatelského jména.
- 4.8** V Aplikacích EB probíhá autorizace pomocí elektronického/digitálního podpisu na základě zadání hesla v klientské části aplikace. Použitím elektronického/digitálního podpisu dojde k podepsání a zašifrování souboru dat, který je následně možné odeslat do Banky ke zpracování.
- 4.9** Odvolání platební transakce se uskuteční stejným způsobem jako její autorizace, pokud příslušná aplikace odvolání připouští.
- 4.10** V IEB může Uživatel využívat platební služby nepřímého dání platebního příkazu a službu informování o platebním účtu.
- 4.11** Banka je oprávněna změnit způsob autentizace Uživatele, autorizace a jiného právního jednání především z důvodu vyšší bezpečnosti Produktů IEB. Banka informuje Uživatele o novém způsobu autentizace nebo autorizace prostřednictvím té Aplikace IEB, které se změna způsobu autentizace či autorizace týká, nebo písemně nejpozději 2 měsíce přede dnem, kdy má změna nabýt účinnosti.

5 ODPOVĚDNOST ZA NEAUTORIZOVANOU NEBO NESPRÁVNĚ PROVEDENOU PLATEBNÍ TRANSAKCI

- 5.1** Uživatel je povinen oznámit Bance bez zbytečného odkladu, nejpozději do 13 měsíců od dne, kdy byla částka platební transakce odepsána z účtu, neautorizovanou nebo nesprávně provedenou transakci, ztrátu, odcizení, zneužití nebo neoprávněné použití platebního prostředku nebo osobního bezpečnostního prvku, osobních dokladů, mobilního telefonu s uloženou platební kartou, s aktivovaným mobilním bankovníctvím nebo cokoli podezřelého v souvislosti s internetovým nebo elektronickým bankovníctvím. Místem pro nahlášení je Infolinka Banky, která je uvedena na stránkách Banky v sekci Kontakty s dostupností 24/7 (nonstop), nebo kterákoli pobočka v rámci provozní doby. Banka uvádí rovněž na svých internetových stránkách a na svých obchodních místech informace o způsobu, jímž má Uživatel oznámit ztrátu, odcizení, zneužití nebo neoprávněné použití osobních bezpečnostních prvků, platebního prostředku nebo Produktu IEB, a to i mimo provozní dobu Infolinky a poboček.
- 5.2** Majitel účtu nese ztrátu finančních prostředků vzniklou z neautorizované platební transakce do částky odpovídající 50 eurům, byla-li tato ztráta způsobena použitím ztraceného nebo odcizeného platebního prostředku nebo osobního bezpečnostního prvku nebo zneužitím platebního prostředku nebo osobního bezpečnostního prvku, pokud jsou současně splněny následující podmínky:
- k provedení neautorizované platební transakce došlo dříve, než Uživatel Bance nahlásil ztrátu, odcizení, zneužití nebo neoprávněné použití platebního prostředku, a
 - Uživatel úmyslně nebo z hrubé nedbalosti neporušil povinnost chránit osobní bezpečnostní prvky.
- 5.3** Majitel účtu nese ztrátu finančních prostředků z neautorizované platební transakce v plném rozsahu, jestliže Uživatel způsobil tuto ztrátu svým podvodným jednáním nebo tím, že úmyslně nebo z hrubé nedbalosti porušil povinnost chránit své osobní bezpečnostní prvky.
- 5.4** Uživatel odpovídá Bance za škody vzniklé v přímé souvislosti s porušením jeho povinností uvedených v kapitole 3.

6 ZVLÁŠTNÍ USTANOVENÍ O ODPOVĚDNOSTI

- 6.1** Uživatel není oprávněn pořizovat kopie obsahu programových médií a je povinen používat pouze zařízení, která nemohou v důsledku svých vad, včetně zavirování, ohrozit nebo znemožnit provoz systémů.
- 6.2** Majitel účtu odpovídá za všechny škody, které Bance nebo třetím osobám vzniknou např. v důsledku přenesení počítačového viru ze zařízení Majitele účtu nebo Uživatele či jimi použitého zařízení třetí osoby.
- 6.3** Banka nenese odpovědnost za kompatibilitu bankovní aplikace s jiným aplikačním vybavením zařízení. Banka neodpovídá za poškození a poruchy či ztrátu funkčnosti mobilního telefonu a aplikačního vybavení mobilního telefonu vzniklé v důsledku toho, že mobilní telefon byl poškozen nebo měl jiné vady, nespĺňoval vlastnosti uváděné výrobcem nebo obsahoval aplikační vybavení neslučitelné s bankovní aplikací. Tím není dotčena úprava vyloučení či omezení odpovědnosti Banky dle Obecných obchodních podmínek.
- 6.4** Pokud je Uživateli prostřednictvím IEB zprostředkováno nahlížení na informace o produktech poskytovaných třetími stranami, neodpovídá Banka za správnost nebo dostupnost takových informací.
- 6.5** Banka neodpovídá za případnou škodu vzniklou z důvodu:
- a)** technického výpadku na zařízení klienta, poruch telefonní sítě nebo veřejné datové sítě, porušení tajemství dopravovaných zpráv, které Banka nemohla ovlivnit, aplikování mezinárodních sankcí ve smyslu právních předpisů o provádění mezinárodních sankcí, případně jiných okolností, které vylučují odpovědnost Banky,
 - b)** neoprávněného užití certifikačních a autorizačních nástrojů a dalších osobních bezpečnostních prvků v období mezi zrušením jejich platnosti Uživatелеm/Majitelem účtu a automatickým předáním této informace z registrační (resp. certifikační) autority do systému Banky.
- 6.6** V případě porušení smluvní povinnosti Bankou tato odpovídá pouze vůči Majiteli účtu, a nikoli vůči osobě, jejímuž zájmu mělo splnění ujednané povinnosti sloužit.

7 DOSTUPNOST A BLOKACE INTERNETOVÉHO A ELEKTRONICKÉHO BANKOVNICTVÍ

- 7.1** Uživatel může používat Aplikace IEB 365 dní v roce 24 hodin denně, pokud se nejedná o situaci, kdy Banka neumožní přístup do IEB z následujících důvodů:
- a)** je-li to nutné pro údržbu bankovních systémů, aplikací anebo pro zpracování dat;
 - b)** jestliže se Uživatel přihlašuje do IEB z IP adresy, která se nachází v zeměpisné oblasti, na niž se vztahují mezinárodní sankce nebo jiná bezpečnostní pravidla Banky. Tyto zeměpisné oblasti Banka uvádí na svých internetových stránkách;
 - c)** je-li to způsobeno přímo či nepřímo okolnostmi mimo kontrolu Banky nebo jejích partnerů v důsledku působení vyšší moci, přírodních katastrof, hardwarových závad, počítačových virů nebo v důsledku jiných událostí způsobených např. třetí stranou;
 - d)** jestliže se Uživatel přihlašuje do IEB z IP adresy, která vykazuje podezřelou aktivitu (např. hromadné posílání nevyžádaných obchodních sdělení, řetězových zpráv, účast na hackerských útocích apod.).
- 7.2** Banka je oprávněna zablokovat všechny Aplikace IEB, případně přístup Uživatele (dále jen „blokace“):
- a)** poruší-li Uživatel nebo Majitel účtu závažným způsobem nebo opakovaně smluvní povinnosti,
 - b)** má-li Banka důvodné podezření, že došlo k neautorizovanému nebo podvodnému použití Aplikace IEB, popř. existuje-li důvodné podezření, že k takovému použití může dojít,
 - c)** je-li ohrožen její oprávněný zájem,
 - d)** v případě zvýšeného rizika, že Majitel účtu nebude schopen splácet úvěr poskytnutý Bankou.
- 7.3** Banka vhodným způsobem informuje konkrétního Uživatele/Majitele účtu o provedení blokace učiněné z podnětu Banky před jejím provedením, případně neprodleně po jejím provedení, ledaže by informování příslušné osoby mohlo zmařit účel blokace nebo by bylo v rozporu s právními předpisy.
- 7.4** V případě blokace Aplikace IEB nelze využít službu nepřímého dání platebního příkazu.
- 7.5** Náklady spojené s blokací z podnětu Uživatele nese Majitel účtu, nejde-li o situaci, kdy je Banka povinna provést tuto blokaci poté, co jí Uživatel oznámil zneužití nebo odcizení platebního prostředku nebo osobního bezpečnostního prvku.

8 ZVLÁŠTNÍ USTANOVENÍ PRO ELEKTRONICKÉ BANKOVNICTVÍ

- 8.1** Banka před zpřístupněním Aplikace EB zabezpečí na základě žádosti Majitele účtu odborné proškolení Uživatele k využívání příslušného Produktu EB, pokud nebyl Produkt EB poskytnut třetí osobou, tj. nikoli Bankou nebo jí pověřenou osobou. V případě, že byl poskytnut příslušný Produkt EB jiným vlastníkem licenčních práv, potvrzuje Majitel účtu podpisem smlouvy, že byl v plném rozsahu seznámen s Produktem EB a nepožaduje proškolení Bankou nebo jí pověřenou osobou k využívání Produktu EB.
- 8.2** Jednotlivé Produkty EB Banka poskytuje na základě objednávky Produktů EB.
- 8.3** Uživatel je povinen při zahájení využívání příslušného Produktu EB provést otestování systému Produktu EB a navázat inicializační spojení s Bankou.

8.4 Počátečním dnem užívání Produktu EB se rozumí den, kdy:

- a) Uživatel převzal od Banky instalační média pro příslušný Produkt EB a/nebo certifikační a autentizační nástroje v případě, kdy Banka poskytuje Majiteli účtu Produkt EB,
 - b) Uživatel převzal od Banky certifikační a autentizační nástroje v případě, kdy byl Uživateli zpřístupněn Produkt EB jiným vlastníkem licenčních práv,
 - c) byla odeslána instalační média systému pro poskytování Produktů EB a/nebo certifikačních a autentizačních nástrojů dle objednávky Produktů EB,
 - d) Banka provedla příslušná nastavení.
- 8.5 Uživatel je povinen před přenosem jednotlivých datových souborů uložit přenášená data v plném znění tak, aby Banka nebo Bankou pověřená osoba mohla kdykoli provést jejich případnou kontrolu. Tyto záznamy je Uživatel povinen uchovávat po dobu nejméně 30 pracovních dnů ode dne jejich odeslání do Banky. Během této doby je Banka oprávněna provést kdykoli kontrolu těchto záznamů a Uživatel je povinen tuto kontrolu Bance nebo osobě Bankou pověřené umožnit.
- 8.6 Majitel účtu a Uživatel se zavazují zachovávat důvěrný charakter všech zpráv přijatých od Banky, a to i po skončení využívání Produktů IEB.

9 BANKOVNÍ IDENTITA

- 9.1 Bankovní identita je prostředkem pro elektronickou identifikaci splňující podmínky zákona č. 21/1992 Sb., o bankách, v platném znění (dále jen „zákon o bankách“) a slouží k identifikaci klienta na dálku vůči Bance, státním orgánům a orgánům územních samosprávných celků, jakož i vůči třetím osobám mimo rámec kvalifikovaného systému elektronické identifikace ve smyslu zákona č. 250/2017 Sb., o elektronické identifikaci, v platném znění (dále jen „zákon o elektronické identifikaci“), a to při využívání služeb těchto subjektů, pokud to tyto subjekty a jejich technické možnosti umožní. Banka je oprávněna umožnit využití Bankovní identity k poskytnutí služeb vytvářejících důvěru (vč. podepisování dokumentů) ve smyslu nařízení Evropského parlamentu a Rady (EU) č. 910/2014, o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu, v platném znění. Bankovní identita je tvořena identifikačními údaji o Klientovi fyzické osobě ve spojení s osobními bezpečnostními prvky.
- 9.2 Bankovní identita vzniká ke dni své registrace do národního bodu ve smyslu zákona o elektronické identifikaci (dále jen „Národní bod“). Banka tuto registraci provede bezodkladně poté, co to bude z právního i technického hlediska možné.
- 9.3 Klient je oprávněn předem zakázat registraci Bankovní identity do Národního bodu, případně zakázat využívání své již registrované Bankovní identity. Klient je oprávněn takový zákaz kdykoli odvolat.
- 9.4 Banka bude Klienta o provedení registrace jeho Bankovní identity do Národního bodu informovat. Klient je povinen zkontrolovat správnost svých identifikačních údajů, které jsou součástí Bankovní identity, neprodleně poté, co se o její registraci dozví.
- 9.5 Bankovní identita může být vydána Klientovi:
- a) jehož svéprávnost nebyla omezena,
 - b) který je starší 15 let,
 - c) který má uzavřenou příslušnou Produktovou smlouvu,
 - d) který má zřízené osobní bezpečnostní prvky pro přístup do IEB,
 - e) u kterého byla provedena identifikace způsobem stanoveným v ustanovení §38ac odst. 1 písm. b) zákona č. 21/1992 Sb., o bankách, v platném znění, a
 - f) u kterého lze ověřit totožnost prostřednictvím Národního bodu pomocí průkazu totožnosti.
- 9.6 Banka je oprávněna Bankovní identitu Klienta zrušit, pokud zjistí, že byla vydána na základě nepravdivých informací, nebo stanou-li se údaje o Klientovi neplatnými a Banka je nebude schopna aktualizovat.
- 9.7 Banka je oprávněna aktualizovat identifikační údaje Klienta na základě informací obdržených od Národního bodu.
- 9.8 Bankovní identita zanikne v případě, že Klient přestane splňovat některou z podmínek uvedených v čl. 9.5.

10 ZÁVĚREČNÁ USTANOVENÍ

- 10.1 Klient podnikatel a Banka se odchylují od ustanovení § 1799 a 1800 občanského zákoníku o smlouvách uzavíraných adhezním způsobem. Tímto je vyloučena případná neplatnost ustanovení těchto Produktových podmínek IEB nebo příslušné smlouvy pro rozpor s uvedenými ustanoveními o smlouvách uzavíraných adhezním způsobem, zejména neplatnost:
- a) doložek, které odkazují na podmínky mimo vlastní text příslušné smlouvy, s jejichž významem nebyl Klient seznámen a ani nebude prokázáno, že Klient znal jejich význam,
 - b) doložek, které lze přečíst jen se zvláštními obtížemi, nebo doložek, které jsou pro osobu průměrného rozumu nesrozumitelné, a to i když působí Klientovi újmu a Klientovi nebyl jejich význam dostatečně vysvětlen,
 - c) doložek, které jsou pro Klienta zvláště nevýhodné, aniž je pro to rozumný důvod, zejména odchyluje-li se příslušná smlouva závažně a bez zvláštního důvodu od obvyklých podmínek ujednávaných v obdobných případech.

- 10.2** Klient je oprávněn kdykoli smlouvu vypovědět s výpovědní lhůtou 1 měsíc běžící ode dne následujícího po dni doručení výpovědi Bance či k pozdějšímu dni uvedenému ve výpovědi.
- 10.3** Banka může smlouvu písemně vypovědět bez udání důvodu s účinností ke konci druhého kalendářního měsíce následujícího po měsíci, v němž byla výpověď doručena Klientovi, nestanoví-li Banka výpovědní dobu delší.
- 10.4** Banka je oprávněna odstoupit od příslušné smlouvy v případě, kdy se trvání závazků ze smlouvy nebo využívání Produktu IEB stane pro Banku nepřijatelným nebo nezákonným v důsledku existence příslušných právních předpisů nebo interní politiky Banky.
- 10.5** Na práva a povinnosti neupravené těmito Produktovými podmínkami IEB se vztahují Obecné obchodní podmínky UniCredit Bank Czech Republic and Slovakia, a.s., příslušné produktové obchodní podmínky pro sjednané bankovní produkty a příslušné právní předpisy.