Pravidlá bezpečného používania elektronického bankovníctva

Účelom tohto dokumentu je poskytnúť vám pred uzatvorením rámcovej zmluvy a predovšetkým zmluvy umožňujúcej využívať služby elektronického bankovníctva informácie podľa zákona č. 492/2009 Z. z. o platobných službách.

Poskytovateľom služieb elektronického bankovníctva je UniCredit Bank Czech Republic and Slovakia, a.s., so sídlom Želetavská 1525/1, 140 92 Praha 4 – Michle, zapísaná v obchodnom registri vedenom Mestským súdom v Prahe, oddiel B, vložka 3608, IČO 64948242 pri vykonávaní bankových činností na území Slovenskej republiky prostredníctvom UniCredit Bank Czech Republic and Slovakia, a.s., pobočka zahraničnej banky, Šancová 1/A, 813 33 Bratislava, IČO: 47 251 336, zapísaná v obchodnom registri Mestského súdu Bratislava III, oddiel: Po, vložka číslo: 2310/B; Banka poskytuje svoje služby v Slovenskej republike na základe jedného bankového povolenia podľa práva Európskej únie, oznámením Českej národnej banky č. 2013/5785/570 zo dňa 20. mája 2013 a oznámením podmienok pôsobenia pobočky zahraničnej banky na území Slovenskej republiky na základe jedného bankového povolenia Národnej banky Slovenska č. OBD-5659/2013 zo dňa 4. júla 2013 (ďalej len „Banka“).

Banka vám ako klientovi/užívateľa poskytuje služby elektronického bankovníctva umožňujúce vám prostredníctvom siete internet obsluhu dohodnutých bankových produktov, ako je napr. účet, platobná karta, úver, banková záruka, poistenie, investícia a pod., ich dohodnutie, uzavretie príslušnej produktovej zmluvy a tiež zabezpečenú komunikáciu medzi vami a Bankou.

1. Osobné bezpečnostné prvky slúžiace na overenie užívateľa (ďalej len „bezpečnostné prvky“)

Prvky slúžiace na vaše overenie sú jedinečné bezpečnostné prvky, ktoré vám umožňujú vstupovať do elektronického bankovníctva a využívať naše služby. Tieto prvky sme vám buď pridelili, alebo ste si ich sami vybrali. Každý prvok je určitého typu:

a) Znalosť – niečo, čo pozná len užívateľ;
b) Vlastníctvo – niečo, čo má len užívateľ;
c) Inherencia/Biometria – niečo, čím je užívateľ (unikátny údaj o užívateľovi).

Ak sú na overenie použité minimálne 2 prvky, pričom každý musí byť z inej kategórie, ide o tzv. silnú autentifikáciu užívateľa.

Osobné bezpečnostné prvky sú:

Prvok	Opis
PIN kód pre mobilnú aplikáciu	Číselný kód pre Mobilnú aplikáciu EB, ktorý sa používa pri aktivácii, prihlásení alebo na potvrdzovanie transakcií.
Heslo pre prihlásenie	Heslo sa skladá z numerických znakov (dĺžka 6 znakov). Používa sa na prihlásenie do Webových aplikácií EB v kombinácii s jednorazovým SMS kódom. Užívateľ je povinný úvodné heslo poskytnuté mu Bankou ihneď zmeniť.
Bezpečnostný kľúč (Smart kľúč, Business kľúč)	Funkcia obsiahnutá v Mobilných aplikáciách EB, určená na prihlásenie do Aplikácií EB alebo na autorizáciu platobných transakcií a iných žiadostí, alebo na generovanie jednorazových kódov na prihlásenie alebo autorizáciu transakcií vo Webových aplikáciách EB aj bez pripojenia zariadenia k internetu, t. j. v režime offline.
Hardvérový bezpečnostný kľúč (token)	Hardvérové zariadenie chránené PIN kódom, ktoré sa používa na generovanie jednorazových číselných kódov pre prihlásenie alebo autorizáciu transakcií vo Webových aplikáciách EB.
SMS kľúč	Kombinácia hesla a jednorazových kódov zaslaných prostredníctvom SMS na mobilný telefón užívateľa pre prihlásenie alebo autorizáciu transakcií vo Webových aplikáciách EB.
Registrované mobilné telefónne číslo	Telefónne číslo, ktoré užívateľ oznámi Banke a ktoré umožňuje prijímať jednorazové bezpečnostné kódy, tzv. SMS OTP (OTP znamená One-Time Password, čiže jednorazové heslo).
Registrovaná e-mailová adresa	E-mailová adresa, ktorú užívateľ Banke oznámi a ktorá umožňuje prijímať jednorazové bezpečnostné kódy (e-mail OTP).
Odtlačok prsta (biometria)	Odtlačok prsta uložený v mobilnom zariadení, v ktorom je aktivovaná mobilná aplikácia EB.
Sken tváre (tzv. Face ID – biometria)	Sken tváre uložený v mobilnom zariadení, v ktorom je aktivovaná mobilná aplikácia EB. Sken tváre sa porovnáva s biometrickými údajmi uloženými v Banke alebo s fotografiou (napr. z identifikačného dokladu).
Heslo	Heslo skladajúce sa z rôznych alfanumerických znakov a slúžiace na overenie užívateľa v rôznych situáciách.
Jednorazové bezpečnostné heslo (OTP = One-Time Password)	Jednorazový bezpečnostný kód, pomocou ktorého možno overiť vlastníctvo bezpečnostného prvku. Je to kód zasielaný na registrované mobilné telefónne číslo, na registrovanú e-mailovú adresu alebo je generovaný mobilnou aplikáciou EB.
Užívateľské meno	Pridelené alebo v určitých prípadoch samostatne nastaviteľné meno (alias), určené na prihlásenie do Aplikácie EB.

UniCredit Bank

Užívateľské číslo	Číslo pridelené užívateľovi Bankou.
Preukaz totožnosti	Doklad užívateľa vydaný orgánom verejnej správy, v ktorom je uvedené meno, priezvisko, dátum narodenia a z ktorého je zrejmá podoba tváre (občiansky preukaz, vodičský preukaz, cestovný pas).
Rodné číslo	Rodné číslo užívateľa.
Kontrolná otázka	Otázka týkajúca sa užívateľa alebo jeho produktov.
Kód CVV2/CVC2	Špeciálne trojmiestne číslo, ktoré je uvedené na platobnej karte. Je to bezpečnostný prvok používaný na identifikáciu držiteľa karty v prostredí bez prítomnosti platobnej karty (napr. internet).
Číslo platobnej karty	Unikátne 16-miestne číslo platobnej karty
Elektronický podpis	Označenie špecifických údajov, ktoré v počítači nahrádzajú vlastnoručný, prípadne aj overený podpis užívateľa

2. Ďalej uvádzame pravidlá pre bezpečné používanie elektronického bankovníctva

a) nepoužívajte heslá a PIN kódy v iných aplikáciách a na internete (napr. v e-shopoch, sociálnych sieťach, e-mailoch a pod.) totožné s heslami a PIN kódmi používanými pre prihlasovanie do EB alebo pre autorizáciu platobných transakcií,

b) nastavte si heslo a PIN kód tak, aby sa nedali jednoducho uhádnuť alebo odvodiť, napr. kombináciou malých a veľkých písmen, číslic, špeciálnych znakov a pod.,

c) neprezraďte iným osobám ani nikam na internete nezadávajte svoj osobný bezpečnostný prvok, ak nejde o aplikácie elektronického bankovníctva na stránke https://sk.unicreditbanking.eu, https://sk.unicreditbanking.net/ alebo https://corporateportal.unicreditgroup.eu/container/sk/login,

d) heslá a PIN kódy si nezaznamenávajte, chráňte ich pred vyzradením a bezodkladne ich zmeňte v prípade, že došlo k ich vyzradeniu alebo ak máte čo i len podozrenie, že takáto situácia mohla nastať,

e) dbajte na zvýšenú opatrnosť pri zadávaní osobných bezpečnostných prvkov na verejnosti (napr. vo vozidlách hromadnej dopravy) alebo v monitorovaných priestoroch (napr. v blízkosti bezpečnostných kamier), aby ich nemohli spozorovať iné osoby,

f) neprihlasujte sa do elektronického bankovníctva, ak si nemáte istotu, že na zariadení nemôže byť nainštalovaný škodlivý program alebo ak nemáte zariadenie úplne pod svojou kontrolou (napr. vo verejných internetových kaviarňach, na počítačoch používaných viacerými ľuďmi),

g) oznamujte heslo pre komunikáciu s Bankou iba pracovníkovi Banky v situácii, kedy je toto heslo vyžadované,

h) chráňte odblokovanie a použitie SIM karty v mobilnom zariadení PIN kódom a pokiaľ dôjde k jeho strate alebo odcudzeniu, nechajte SIM kartu bezodkladne zablokovať u operátora,

i) chráňte svoj profil u mobilného operátora a nepripustite, aby si tretia osoba nechala vystaviť novú SIM/eSIM k vášmu telefónnemu číslu,

j) neumožnite prístup k svojmu e-mailovému účtu ďalším osobám a nastavte si dvojfaktorové overenie,

k) neumožnite inej osobe prístup do svojho mobilného zariadenia (napr. odtlačkom prsta, skenom tváre, heslom, PIN kódom),

l) pokiaľ došlo ku strate alebo odcudzeniu mobilného zariadenia alebo SIM karty, bezodkladne oznámte túto udalosť Banke a elektronické bankovníctvo nechajte preventívne zablokovať,

m) neumožnite registráciu biometrických údajov inej osoby (ani členov rodiny) do mobilného zariadenia,

n) zabezpečte prístup do mobilného zariadenia heslom, PIN kódom alebo biometricky (odtlačok prsta, sken tváre) a nenechávajte svoje mobilné zariadenie bez dozoru, prípadne bez automatického zamykania obrazovky zariadenia po krátkom čase,

o) nepoužívajte programové úpravy mobilného zariadenia, ktoré umožňujú doňho plný administrátorský prístup (napr. jailbreak, root),

p) pravidelne aktualizujte operačný systém svojho mobilného zariadenia i jednotlivých inštalovaných aplikácií,

q) používajte na svojom mobilnom zariadení najnovšiu verziu bezpečnostných programov (napr. antivírus, firewall),

r) nepovoľujte nadbytočné oprávnenia v novo inštalovaných alebo aktualizovaných aplikáciách vo svojom mobilnom zariadení (napr. prístup k SMS, uľahčenie nastavenia a pod.),

s) inštalujte do svojho mobilného zariadenia len aplikácie z oficiálnych obchodov s aplikáciami – Google Play (pre Android), App Store (pre iOS) vrátane prípadných doplnkov, ak ich používaná aplikácia vyzýva doinštalovať, vo svojom mobilnom zariadení si nastavte zákaz inštalácie aplikácií z neznámych zdrojov,

t) neinštalujte aplikácie na základe pokynov alebo žiadosti tretej osoby a tretej osobe nepovoľujte vzdialený prístup do mobilného zariadenia (napr. cez aplikáciu Any Desk),

u) pokiaľ to nie je nutné, neprihlasujte sa na počítač ako administrátor, ale ako bežný užívateľ,

v) aktualizujte pravidelne operačný systém a svoje programy, najmä internetový prehliadač. Inštalujte rozšírenie (plug-iny) prehliadača iba v obmedzenej miere a iba od známych a dôveryhodných vydavateľov,

w) používajte najnovšiu verziu bezpečnostných programov (napr. antivírus, firewall) a pravidelne ich aktualizujte,

x) chráňte počítač pred neoprávneným prístupom iných osôb nastavením prístupových oprávnení, zabezpečením heslom, prípadne ďalšími prvkami. Nepovoľte tretej osobe vzdialený prístup do počítača (napr. cez aplikácie Any Desk),

y) zadávajte adresu webovej stránky Banky ručne. Pre prístup na stránky webovej aplikácie EB zadajte www.unicreditbank.sk, odtiaľ prejdite na prihlasovaciu stránku internetového bankovníctva, skontrolujte, že pristupuje na webovú adresu https://sk.unicreditbanking.eu, https:// sk.unicreditbanking.net/ alebo https://corporateportal.unicreditgroup.eu/container/sk/login a nepoužívajte zástupcu na prihlasovaciu stránku internetového bankovníctva,

UniCredit Bank

z) nepristupujte do služieb elektronického bankovníctva cez odkaz z vyhľadávača ani odkaz zaslaný e-mailom, SMS alebo iným spôsobom (na sociálnej sieti, cez chatovaciu aplikáciu atď.),

aa) neprihlasujte sa v prípade, že sa vám zdá prihlasovacia obrazovka elektronického bankovníctva podozrivá,

ab) bezodkladne kontaktujte Banku, ak zaregistrujete operáciu, ktorú ste neautorizovali,

ac) nereagujte na telefonáty, ktoré vás vyzývajú k akcii s účtom, pretože Banka nikdy telefonicky nevyzýva svojich klientov k akýmkoľvek transakciám,

ad) neotvárajte e-mail obsahujúci meno Banky, pokiaľ neprišiel z domény: unicreditbank.sk alebo unicreditgroup.sk, neotvárajte prílohy neštandardného typu súboru (napr. prípony: .exe, .php) a neklikajte na odkazy obsiahnuté v nehodnovernej správe,

ae) zoznamujte sa so správami zaslanými Bankou do služieb elektronického bankovníctva, najmä ak ide o varovanie pred podvodmi.

3. Ďalšie pravidlá, ktorých dodržiavanie zvýši pravdepodobnosť, že neprídete o finančné prostriedky

a) Kontrolujte, čo potvrdzujete
   (i) Pred potvrdením prihlásenia alebo pred autorizáciou platobnej transakcie vždy skontrolujte, že zadané údaje (napr. suma, príjemca) zodpovedajú vášmu zámeru.
   (ii) Ak Vám chce niekto poslať peniaze, jeho akciu netreba nijako potvrdzovať. Na zaslané odkazy neklikajte a ani na výzvu inej osoby nikdy nezadávajte vaše bezpečnostné prvky do žiadnej aplikácie.

b) Sledujte aktivitu na vašom účte
   (i) Vedieť, aké platby sa uskutočnili na vašich účtoch, je najlepší nástroj včasného varovania, že niečo nie je v poriadku. Nechajte si preto automaticky posielať SMS, e-maily alebo oznámenia do mobilného telefónu (tzv. push notifikácie) s informáciami o uskutočnených transakciách.
   (ii) V prípade, že sa na účte uskutoční aktivita s vyššou mierou rizika (napr. aktivácia mobilného bankovníctva, zmena kontaktných údajov a pod.), informujeme vás príslušnou správou (napr. push notifikácia, e-mail, SMS).
   (iii) Ak zaregistrujete operáciu, ktorú ste nevykonali, okamžite nás kontaktujte na Infolinku Banky.

c) Nikdy nereagujte na telefonáty, ktoré vás vyzývajú vykonať akciu na účte
   (i) Pravdepodobne ide o falošného bankára, falošného policajta alebo falošného pracovníka štátnej inštitúcie (NBS, NBÚ a pod.). Banka nikdy telefonicky nevyzýva svojich klientov na akékoľvek transakcie, či už ide o výber z účtu, platobnú transakciu alebo dokonca žiadosť o úver.

d) Pravidelne sledujte novinky o bezpečnosti na internete
   (i) Čím viac informácií máte, tým bezpečnejšie sa dokážete správať na internete. Pravidelne preto sledujte najnovšie správy z oblasti bezpečnosti na internete a dodržiavajte všetky odporúčané zásady.

e) Čítajte zasielané správy
   (i) E-maily, listy a ďalšie správy nie sú vždy zábavné. Avšak často bývajú dôležité a oplatí sa ich pozorne čítať. Platí to aj pre správy zasielané do mobilného telefónu.

f) Kontaktujte Infolinku Banky
   (i) Reagujte na prípadné bezpečnostné upozornenie, ktoré môžete dostať, ak nastane riziková udalosť. V prípade podozrenia na podvod alebo bezpečnostnú hrozbu UniCredit Bank klienta vhodným spôsobom informuje, a to s využitím primárnych kontaktných údajov, ktoré klient uviedol pri uzatváraní zmluvy.

4. Autorizácia (podpis) aktívnej operácie / platobnej transakcie a odvolanie platobnej transakcie

Banka umožňuje klientom/užívateľom podpísať rôzne druhy aktívnych operácií – napr. platobný príkaz, zmluvu, dokument alebo iný úkon. Spôsob autorizácie v jednotlivých aplikáciách sa líši a je nasledujúci:

V Mobilných aplikáciách EB prebieha autorizácia niektorým z nasledujúcich spôsobov, po tom, ako je Užívateľ k tomu vyzvaný:
a) odtlačkom prsta alebo priložením (skenom) tváre k zariadeniu,
b) zadaním PIN kódu.

Vo Webových aplikáciách EB prebieha prihlásenie a autorizácia niektorým z týchto spôsobov:

a) Bezpečnostný kľúč, a to:
   (i) Smart kľúč – Online metóda – do Mobilnej aplikácie EB dostane Užívateľ oznámenie vo forme push notifikácie a po otvorení aplikácie operáciu podpíše odtlačkom prsta, skenom tváre alebo zadaním PIN kódu.
   (ii) Smart kľúč – Offline metóda – Webová aplikácia EB zobrazí QR kód, ktorý Užívateľ zosníma prostredníctvom Smart kľúča v Mobilnej aplikácii Smart Banking, ktorá vygeneruje 6-miestny jednorazový kód. Užívateľ tento kód napíše do prihlasovacej časti Webovej aplikácie Online Banking a potvrdí.
   (iii) Business kľúč – Offline metóda pre prihlásenie do aplikácií BusinessNet Professional, BusinessNet a Trade Finance Gate – Užívateľ vygeneruje 6-miestny kód pre prihlásenie prostredníctvom Smart kľúča v mobilnej aplikácii Business Smart Banking alebo BusinessNet Mobile.

b) SMS kľúč
Táto metóda sa skladá z kombinácie osobného hesla a jednorazových kódov zaslaných na mobilný telefón Užívateľa. Užívateľ zadá na obrazovke Webovej aplikácie EB svoje heslo a Banka mu na určený mobilný telefón odošle SMS správu obsahujúcu jednorazový kód. Tento časovo obmedzený kód Užívateľ prepíše späť do Webovej aplikácie EB a potvrdí tak operáciu.

c) Hardvérový bezpečnostný kľúč (token)
Heslo na podpis operácie je vygenerované tokenom. Užívateľ zadá PIN kód na klávesnici tokenu. V prípade zadania správneho PIN kódu token vygeneruje 8-miestny jednorazový kód, ktorý Užívateľ prepíše do Webovej aplikácie. Aplikácia následne zobrazí 6-miestny jednorazový kód, ktorý užívateľ prepíše opäť do aplikácie, čím operáciu autorizuje.
V službe Multicash prebieha autorizácia prostredníctvom elektronického podpisu na základe zadania hesla v jej klientskej časti. Použitím elektronického podpisu dôjde k podpísaniu a zašifrovaniu súboru dát, ktorý je následne možné odoslať do Banky na spracovanie.

Odvolanie platobnej transakcie sa uskutoční rovnakým spôsobom, ako jej autorizácia, ak príslušná aplikácia pripúšťa odvolanie.

5. Zodpovednosť za stratu finančných prostriedkov v prípade straty, odcudzenia, zneužitia alebo neoprávneného použitia platobného prostriedku alebo osobného bezpečnostného prvku

a) Neautorizovanú alebo nesprávne vykonanú platobnú transakciu, stratu, odcudzenie, zneužitie alebo neoprávnené použitie vášho platobného prostriedku alebo osobného bezpečnostného prvku, osobných dokladov, mobilného telefónu s uloženou platobnou kartou, s aktivovaným mobilným bankovníctvom alebo čokoľvek podozrivé v súvislosti s internetovým alebo mobilným bankovníctvom nám bezodkladne nahláste na linku: +421 2 6828 5777 (24/7, nonstop) alebo v ktorejkoľvek našej pobočke v rámci otváracích hodín.
b) Stratu finančných prostriedkov vzniknutú z neautorizovanej platobnej transakcie nesiete do sumy zodpovedajúcej 50 EUR, ak bola táto strata spôsobená použitím strateného alebo odcudzeného platobného prostriedku alebo osobného bezpečnostného prvku alebo zneužitím platobného prostriedku alebo osobného bezpečnostného prvku, v dôsledku vašej nedbanlivosti, okrem prípadov uvedených nižšie.
c) Finančnú stratu neznášate, ak:
   (i) vyplýva z použitia strateného, odcudzeného alebo zneužitého platobného prostriedku od okamihu nahlásenia tejto skutočnosti Banke; to však neplatí, ak by ste konali podvodným spôsobom, alebo
   (ii) stratu, odcudzenie alebo zneužitie platobného prostriedku ste nemohli zistiť pred platobnou operáciou; to neplatí, ak by ste konali podvodným spôsobom.
d) Všetky straty súvisiace s neautorizovanými platobnými operáciami znášate, ak boli zapríčinené vašim podvodným konaním, úmyselným nesplnením jednej alebo viacerých povinností pri zabezpečovaní osobných bezpečnostných prvkov alebo nesplnením jednej alebo viacerých týchto povinností v dôsledku vašej hrubej nedbanlivosti.

6. Zodpovednosť za chybne vykonanú platobnú transakciu

O chybne vykonanú platobnú transakciu ide, ak Banka nezúčtovala sumu platobnej transakcie v správnej mene alebo nepoužila číslo účtu alebo iný jedinečný identifikátor v súlade s vaším príkazom.

Ak má Banka povinnosť napraviť nesprávne vykonanú platobnú transakciu a vy jej oznámite, že netrváte na vykonaní platobnej transakcie, Banka bezodkladne:

a) uvedie váš účet do stavu, v ktorom by bol, ak by toto odpísanie nenastalo, alebo
b) vráti na váš účet sumu, ako aj poplatok za prevod sumy a ušlé úroky, ak postup podľa písmena a) nepripadá do úvahy.

Ak neoznámite Banke, že netrváte na vykonaní platobnej transakcie, Banka bezodkladne:
a) zabezpečí pripísanie sumy nesprávne vykonanej platobnej transakcie na účet poskytovateľa príjemcu,
b) a zároveň uvedie váš účet do stavu, v ktorom by bol, ak by Banka vykonala platobnú transakciu správne, alebo
c) vráti vám nesprávne zaplatený poplatok a ušlé úroky, ak postup podľa písmena a) nepripadá do úvahy.