

Tyto podmínky obsahují bližší úpravu práv a povinností vyplývajících z uzavřené Smlouvy o elektronickém podpisu a Bankovní identitě KB. Seznamte se prosím důkladně s tímto dokumentem. Vaše případné dotazy rádi zodpovíme.

## Článek 1. Metody pro elektronický podpis

- 1.1 Metody.** V rámci vybraných Bankovních služeb, zejména při využívání služeb přímého bankovníctví, můžete používat následující Metody:
- Certifikát uložený na čipové kartě,
  - KB Klíč,
  - Bezpečnostní heslo.
- U některých Bankovních služeb si vyhrazujeme právo akceptovat pouze některé Metody, a to i v závislosti na tom, jakým způsobem jsme vás identifikovali. Jednotlivé Metody mohou sloužit pro vaši autentizaci, potvrzení vašeho projevu vůle, anebo pro podepisování vašim Elektronickým podpisem. Některé Metody pro účely autentizace, potvrzení vašeho projevu vůle i Elektronického podpisu můžete používat též vůči třetím osobám, pokud vám to v konkrétním případě umožníme.
- 1.2** Metody můžete používat pouze vy osobně.
- 1.3** Za poskytnutí a používání Metod a souvisejících služeb platíte ceny podle Sazebníku.
- 1.4** Smlouva se řídí právním řádem České republiky, a to zejména občanským zákoníkem<sup>1</sup>.
- 1.5** Podpisem Smlouvy stvrzujete, že jste se seznámil s obsahem a významem Certifikační politiky a s Desaterem bezpečnosti a souhlasíte, že se jimi budete řídit a dodržovat zásady v nich uvedené.
- 1.6** Berete na vědomí, že předpokladem plné funkčnosti Metod je splnění technických parametrů uvedených v Technických podmínkách.

## Článek 2. Bankovní identita KB

- 2.1 Bankovní identita KB.** Bankovní identitu KB tvoří sada vašich identifikačních údajů u nás ve spojení s některou z výše uvedených Metod, přičemž každá z Metod zakládá vaši jedinečnou Bankovní identitu KB. Bankovní identita KB je váš elektronický průkaz totožnosti, díky kterému může být Vaše totožnost ověřována na dálku.
- 2.2 Použití Bankovní identity KB vůči nám.** Bankovní identita KB slouží k provedení vaší identifikace při využívání Bankovních služeb a při komunikaci s námi na dálku. Bankovní identitu KB můžete pro ověřování vaší identifikace používat i vůči Členům finanční skupiny Banky, a to bude-li to příslušnými Členy finanční skupiny Banky umožněno a případně po splnění jimi dodatečně stanovených podmínek.
- 2.3 Použití Bankovní identity KB po registraci do Národního bodu a souhlasy s prolomením bankovního tajemství.** V případě, že dojde k registraci vaší Bankovní identity KB do Národního bodu, bude moci Bankovní identita KB sloužit též k provedení vaší identifikace vůči státním orgánům a orgánům územních samosprávných celků, jakož i vůči třetím osobám mimo rámec kvalifikovaného systému elektronické identifikace ve smyslu zákona o elektronické identifikaci<sup>2</sup>, a to při využívání služeb těchto subjektů, bude-li vám to jimi umožněno.
- Provedení identifikačních služeb, kterými se rozumí identifikace, autentizace a služby vytvářející důvěru (například i podepisování dokumentů), prostřednictvím Bankovní identity KB bude možné vůči třetím osobám dle předchozí věty využít pouze s vaším souhlasem prolamujícím bankovní tajemství, včetně vámi schválených identifikačních a jiných údajů, ledaže právní předpisy stanoví jinak.

<sup>1</sup> zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů

<sup>2</sup> zákon č. 250/2017 Sb., o elektronické identifikaci, ve znění pozdějších předpisů

# PODMÍNKY K ELEKTRONICKÉMU PODPISU A BANKOVNÍ IDENTITĚ KB

- 2.4 Registrace do Národního bodu.** Jakmile to bude z právního i technického hlediska možné, zaregistrujeme v souladu s právními předpisy<sup>3</sup> vaši Bankovní identitu KB do Národního bodu. To platí pouze pro Bankovní identity KB, jejichž držitel je starší 15 let a pro Bankovní identity KB, u kterých je registrované unikátní číslo mobilního telefonu. Registraci provedeme vždy nejdříve po uplynutí 14 kalendářních dnů od účinnosti Smlouvy, případně dříve, při vámi iniciovaném využití služby, která registraci vyžaduje. Registrace zahrnuje ověření vaší totožnosti prostřednictvím Národního bodu s využitím vašich údajů, tj. zejména číslo a typ dokladu totožnosti, adresa pobytu, datum narození, jméno, příjmení, místo narození, občanství. Poté bude vaši Bankovní identitě přidělen KB identifikátor, který zapišeme spolu s identifikátorem držitele Bankovní identity KB, úroveň záruky Bankovní identity KB a dalšími parametry do Národního bodu. Po registraci máte povinnost si prostřednictvím portálu MujProfil zkontrolovat správnost identifikačních údajů, které jsou součástí vaší Bankovní identity KB a které o vás evidujeme.
- 2.5 Zákaz a povolení registrace do Národního bodu.** V případě, že nebudete mít zájem o registraci vaší Bankovní identity KB do Národního bodu nebo o následné trvání registrace pro využívání vaší Bankovní identity KB dle článku 2.3, máte právo registraci nebo následné trvání registrace pro využívání Bankovní identity KB zakázat. Zákaz, případně povolení registrace a využívání Bankovní identity KB následující po vašem předchozím zákazu, proveďte na portálu MujProfil po vašem přihlášení Bankovní identitou KB. Samotná registrace do Národního bodu a využívání Bankovní identity KB prostřednictvím Národního bodu je založeno povinností uloženou nám právními předpisy a Smlouvou, nikoliv vaším souhlasem. Registraci však máte právo zakázat a následně povolit způsobem uvedeným výše.
- 2.6 Použitelné Metody.** Berete na vědomí, že k provedení vaší identifikace prostřednictvím Bankovní identity KB vůči subjektům dle článku 2.3 můžete využít pouze ty Metody, u kterých při jejich sjednání či kdykoli později došlo k vaší identifikaci za vaší fyzické přítomnosti, případně byly splněny zákonné předpoklady. Současně berete na vědomí, že pro účely dle předchozí věty lze využít pouze Metody, které je možné do Národního bodu registrovat a které takto zaregistrujeme. Seznam použitelných Metod pro tyto účely naleznete na našich internetových stránkách.
- 2.7 Bezpečnostní pravidla a odpovědnost za jejich porušení.** Pro používání Bankovní identity KB platí bezpečnostní pravidla uvedená v čl. 8 těchto Podmínek a v dokumentu Desatero bezpečnosti. Nedodržení uvedených povinností a doporučení může vést ke zneužití vaší Bankovní identity KB, a to i vůči státním orgánům, nebo důvěrných informací a k případnému vzniku vaší újmy nebo újmy třetí osoby a současně ke vzniku vaší odpovědnosti za takovou újmu. Za takovou ztrátu, odcizení či zneužití vaší Bankovní identity KB či metody pro vytváření Elektronického podpisu, mobilního telefonu/zařízení či přístupových údajů anebo dalších důvěrných informací a zároveň to vylučuje naši odpovědnost. Nahlášení dle předchozí věty máte povinnost učinit bez zbytečného odkladu po zjištění ztráty, odcizení, zneužití, či neautorizovaného použití vaší bankovní identity KB.

## Článek 3. Certifikát uložený na čipové kartě

- 3.1 Forma certifikátu.** Certifikát (komerční i kvalifikovaný) bude uložen na čipové kartě, kterou vám poskytneme. Můžete si sjednat čipovou kartu ve standardním režimu či QSCD režimu. Při převzetí čipové karty obsahující Certifikát jste povinni zkontrolovat a ověřit údaje, které budou obsahem Certifikátu, zejména vaše identifikační údaje v rozsahu jméno a příjmení, typ Certifikátu, emailová adresa, země bydliště nebo pobytu a číslo čipové karty. Banka nenes odpovědnost v případě chybně uvedených nebo neúplných informací, které budou po vašem potvrzení obsahem Certifikátu.
- 3.2 Druh Certifikátu.** Při uzavírání Smlouvy můžete zvolit komerční nebo kvalifikovaný Certifikát. Pokud zvolíte kvalifikovaný Certifikát, bude vám poskytnut a na čipovou kartu uložen zároveň i komerční Certifikát.
- 3.3 Komerční Certifikát.** Na základě komerčního Certifikátu můžete vytvořit elektronický podpis, který je zaručeným elektronickým podpisem ve smyslu nařízení eIDAS.
- 3.4 Kvalifikovaný Certifikát.** V závislosti na režimu čipové karty je kvalifikovaný Certifikát možné použít pro vytvoření uznávaného elektronického podpisu ve smyslu zákona o službách vytvářejících důvěru<sup>4</sup>, a to v podobě zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu pro elektronický podpis nebo kvalifikovaného elektronického podpisu. Pouze kvalifikovaný Certifikát na čipové kartě v QSCD režimu je možné použít pro vytvoření kvalifikovaného elektronického podpisu ve smyslu nařízení eIDAS. Kvalifikovaný Certifikát nelze použít k autentizaci.

<sup>3</sup> zákon č. 21/1992 Sb., o bankách, ve znění pozdějších předpisů, zákon č. 250/2017 Sb., o elektronické identifikaci, ve znění pozdějších předpisů, Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES.

<sup>4</sup> § 6 odst. 2 zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce.

# PODMÍNKY K ELEKTRONICKÉMU PODPISU A BANKOVNÍ IDENTITĚ KB

- 3.5 KB Podpisový modul.** Máte povinnost si dle našich instrukcí nainstalovat KB Podpisový modul pro komunikaci s naší čipovou kartou. Tento modul obsluhuje všechny operace s čipovou kartou, zejména přihlašování, autorizaci transakcí a podpisů transakcí a dokumentů v příslušných aplikacích. Modul taktéž zajišťuje bezpečné prostředí pro získání sjednaného Certifikátu prostřednictvím portálu MůjProfil a v modulu je také možné změnit PIN či odblokovat PIN čipové karty.
- 3.6 Aktivace.** S vaší součinností vám po uzavření Smlouvy zašleme formou SMS zprávy na sjednané číslo mobilního telefonu jednorázové heslo, abyste si mohl komerční Certifikát vytvořit prostřednictvím portálu MůjProfil, nebo vám vytvoříme Certifikát včetně vygenerování Soukromého a Veřejného klíče a uložíme na čipovou kartu v našem obchodním místě. Jednorázové heslo je platné po dobu 3 dnů od jeho zaslání. Současně vám předáme čipovou kartu a obálku s PIN a PUK. V případě kvalifikovaného Certifikátu musí být nejdříve aktivován komerční Certifikát a jeho prostřednictvím si buď v našem obchodním místě či na portálu MůjProfil aktivujete kvalifikovaný Certifikát.
- 3.7 Certifikační politika.** Podrobná pravidla a postupy při používání Certifikátu (komerčního i kvalifikovaného) jsou stanoveny v Certifikační politice dostupné prostřednictvím internetových stránek Banky.

## Článek 4. KB Klíč

- 4.1 Aplikace a zařízení.** Pokud vám to umožníme, můžete si aktivovat Metodu KB Klíč v různých aplikacích (např. v mobilní aplikaci KB+ a nebo v mobilní aplikaci KB Klíč), a to i na více zařízeních. V jednom zařízení můžete mít více aplikací s aktivovaným KB Klíčem. Aktivací aplikace dochází i k aktivaci Metody KB Klíč. Vyhrazuji si právo omezit počet aktivních aplikací, ve kterých můžete mít Metodu KB Klíč. Rozsah funkčnosti Metody KB Klíč může být u jednotlivých aplikací odlišný. Platnost Metody KB Klíč není časově omezena. Metoda KB Klíč je chráněna PINem (osobní číselný kód sloužící k ověření oprávněnosti nakládat s aplikací k používání Metody KB Klíč). V aplikaci je také možné aktivovat biometrickou ochranu PINu. V každé aplikaci s aktivovanou Metodou KB Klíč si můžete nastavit rozdílný PIN. Aktivací aplikace a Metody KB Klíč lze provést níže uvedenými způsoby.
- 4.2 Stažení aplikace.** Máte povinnost do svých zařízení stahovat aplikace k používání Metody pouze z důvěryhodných zdrojů (např. Google Play, Apple Store).
- 4.3 Aktivace.** K aktivaci, a to i v případě, že o aktivaci pro nezletilého žádá zákonný zástupce, dochází na vaši žádost, a to níže uvedeným způsobem.  
Aktivace pomocí QR kódu. Aktivaci provedete s využitím jednorázového kódu nebo QR kódu, který vám předáme na naší pobočce, vygenerujete si v KB bankomatu (pouze pro aplikaci KB Klíč) nebo v aplikaci KB Klíč, případně vám jej zašleme šifrovaně do vašeho e-mailu, a Jednorázového hesla, které vám zašleme prostřednictvím SMS na váš kontaktní telefon. Aktivaci dokončíte nastavením PINu přímo v aplikaci. Každý aktivační kód i Jednorázové heslo má vždy nastavenou maximální dobu platnosti. Po uplynutí této doby nás musíte požádat o jeho opětovné zaslání.
- 4.4 Duplicita.** Číslo mobilního telefonu pro zaslání jednorázového hesla a Autorizačních SMS zpráv, které spoluvytváří vaši Bankovní identitu KB, a které uvedete ve Smlouvě, nemůže být použito pro stejné účely jiným Klientem. Neodpovídáme za škody vzniklé uvedením nesprávného čísla mobilního telefonu pro doručení jednorázového hesla nebo Autorizační SMS zprávy.

## Článek 5. Bezpečnostní heslo

- 5.1 Aktivace.** Požádáte-li nás akceptovaným způsobem o aktivaci Bezpečnostního hesla, aktivaci provedete s využitím jednorázového kódu, který vám předáme na naší pobočce, vygenerujete si v KB bankomatu nebo vám zašleme šifrovaně na váš kontaktní e-mail. Vaše identifikační číslo a jednorázový kód zadáte při prvním přihlášení do internetového bankovníctví nebo do portálu MůjProfil a poté zadáte Jednorázové heslo, které vám zašleme prostřednictvím SMS na váš kontaktní telefon. V portálu MůjProfil je možné aktivovat Metodu Bezpečnostní heslo též pomocí KB Klíče nebo Certifikátu na čipové kartě. Aktivaci dokončíte nastavením hesla. Platnost Bezpečnostního hesla není časově omezena. Každý aktivační kód i Jednorázové heslo má vždy nastavenou maximální dobu platnosti. Po uplynutí této doby nás musíte požádat o jeho opětovné zaslání.
- 5.2** Číslo mobilního telefonu pro zaslání Jednorázového hesla, které uvedete ve Smlouvě, nemusí být námi akceptováno, pokud již bylo použito pro stejné účely jiným Klientem. Neodpovídáme za škody vzniklé uvedením nesprávného čísla mobilního telefonu pro doručení Jednorázového hesla.
- 5.3** Při prvním použití metody Bezpečnostní heslo provádíte aktivaci s využitím vašeho identifikačního čísla uvedeného v žádosti o aktivaci a Jednorázového hesla zaslání pomocí SMS dle čl. 5.1.

# PODMÍNKY K ELEKTRONICKÉMU PODPISU A BANKOVNÍ IDENTITĚ KB

## Článek 6. Platnost jednotlivých Metod

- 6.1 Platnost Certifikátu.** Obecná platnost Certifikátu je 2 roky. Konkrétní doba platnosti Certifikátu je uvedena v Certifikátu, nebo ji zjistíte prostřednictvím portálu MůjProfil. Platný a účinný Certifikát můžete používat při využívání Služeb. Před koncem jeho platnosti můžete prostřednictvím portálu MůjProfil požádat o prodloužení Certifikátu uloženého na čipové kartě.
- 6.2** Pokud nás požádáte o prodloužení Certifikátu před uplynutím doby jeho platnosti, vydáme vám Certifikát nový, a to na základě již uzavřené Smlouvy. Nový Certifikát vám vydáme ve stejné formě jako Certifikát předchozí a se stejnými notifikačními údaji. Okamžikem vydání nového Certifikátu nesmíte předchozí Certifikát používat. Postup dle článku 3 Podmínek se pro vydání nového Certifikátu použije obdobně.
- 6.3** V případě, že dojde ke změně vašich identifikačních údajů uvedených ve Smlouvě (včetně čísla mobilního telefonu sjednaného pro zaslání Jednorázových hesel), máte povinnost nás o tom bez zbytečného odkladu písemně informovat a zároveň s námi uzavřít dodatek ke Smlouvě nebo nás požádat o vydání nového Certifikátu. V případě, že dojde ke změně vaší e-mailové adresy uvedené ve Smlouvě, musíte nás o tom informovat v obchodním místě Banky nebo po přihlášení do portálu MůjProfil, kde provedete změnu tohoto údaje.
- 6.4 Platnost KB Klíče, Bezpečnostního hesla.** Platnost těchto Metod není časově omezena.

## Článek 7. Blokace a deaktivace Metod

- 7.1 Blokace a deaktivace.** Pokud bude Metoda zablokována, její platnost je pozastavena do doby, než nás požádáte o její odblokování. V případě deaktivace Metody, je Metoda zcela ukončena. Pokud ji budete chtít opět používat, je nutné ji znovu aktivovat. Informaci o zablokování či deaktivaci Metody vám sdělíme na kontaktní telefon dle Smlouvy. V případě Certifikátu uloženého na čipové kartě poskytovaného na základě původní Smlouvy o certifikátu dochází k blokadě či deaktivaci certifikátu k automatickému ukončení této smlouvy. Blokace či deaktivace Metody znefunkční tu Bankovní identitu KB, která je na danou Metodu navázána.
- 7.2 Blokace z naší strany.** Jsme oprávněni zablokovat Metodu na dobu nezbytně nutnou, bude-li to zapotřebí ze závažných, zejména bezpečnostních příčin (např. při podezření na její neoprávněné nebo podvodné použití či v případě upraveného operačního systému). Jakmile pominou důvody zablokování Metody, s vaší součinností umožníme Metodu odblokovat nebo ji nahradit jinou. V některých případech si vyhrajujeme právo Metodu odblokovat i bez vaší součinnosti.
- 7.3 Blokace z vaší strany.** O blokaci Metody můžete požádat kdykoli prostřednictvím Klientské linky, v kterémkoli našem obchodním místě nebo na našich internetových stránkách prostřednictvím portálu MůjProfil. O blokaci Metody musíte požádat vždy, máte-li podezření na její možné zneužití.
- 7.4 Deaktivace z naší strany.** Metodu vám deaktivujeme, a případně budeme požadovat, aby bylo vámi požádáno o její opětovnou aktivaci, nastane-li alespoň jedna z následujících událostí:
- Metoda byla sjednána na základě nepravdivých, neúplných nebo zavádějících informací,
  - identifikační údaje, jež jsou součástí Metody, již nejsou platné,
  - došlo z vaší strany k porušení jakékoliv povinnosti vyplývající ze Smlouvy,
  - ve více Smlouvách a/nebo pro více Klientů bylo sjednáno stejné číslo mobilního telefonu pro zaslání Jednorázového hesla,
  - přestaneme danou Metodu poskytovat,
  - jsme k tomu povinni s ohledem na právní předpisy,
  - došlo nebo může dojít ke zvýšení bezpečnostních rizik nebo opatření souvisejících s chybným zadáním Bezpečnostních údajů nebo využíváním Metody.
- 7.5 Deaktivace z vaší strany.** O deaktivaci Metody můžete požádat ve kterémkoli našem obchodním místě, prostřednictvím Klientské linky, ve své aplikaci KB Klíč nebo na našich internetových stránkách prostřednictvím portálu MůjProfil.
- 7.6** U Certifikátu uloženého na čipové kartě se při třetím chybném zadání PIN čipová karta zablokuje. O odblokování čipové karty můžete požádat ve kterémkoli našem obchodním místě nebo jej může provést prostřednictvím programového vybavení KB Podpisový modul a Cryptoplus KB. V obou případech způsobu odblokování čipové karty musíte uvést PUK.
- 7.7** Dále máme právo při stanoveném počtu po sobě jdoucích chybných přihlašovacích pokusů na libovolné z vašich Metod, dočasně zablokovat všechny vaše Metody. K odblokování dojde automaticky bez vaší součinnosti, po uplynutí námi stanovené doby blokace.

# PODMÍNKY K ELEKTRONICKÉMU PODPISU A BANKOVNÍ IDENTITĚ KB

- 7.8 Jsme oprávněni omezit využívání aplikace s Metodou KB Klíč na zařízení, jehož operační systém byl pozměněn.
- 7.9 **Odblokování Metody.** V případě zablokované Metody můžete požádat o její odblokování prostřednictvím kteréhokoliv našeho obchodního místa, našeho bankomatu, mobilní aplikace KB+, své aplikace KB Klíč nebo portálu MůjProfil, a to za námi stanovených podmínek. Pro plné využití Bankovní identity KB Metodou odblokovanou na dálku bez fyzické přítomnosti, můžeme vyžadovat vaši osobní účast na kterémkoliv našem obchodním místě. Vyhrazujeme si právo změnit způsob odblokování Metody a jejího následného využití, a to zejména v závislosti na našich technických možnostech nebo změně právních předpisů.
- 7.10 **Blokace a deaktivace Metody KB Klíč v jednotlivých aplikacích.** Metodu KB Klíč je možné blokovat nebo deaktivovat v souladu s předchozími články. Dále je možné ji blokovat nebo deaktivovat v jednotlivých aplikacích v konkrétním zařízení. Bude-li deaktivována Metoda KB Klíč v poslední aplikaci na posledním zařízení, dojde k deaktivaci celé Metody KB Klíč.
- 7.11 **Výměna zařízení.** V případě, že chcete nahradit jedno zařízení druhým, např. máte nový mobilní telefon, je nutné na novém zařízení provést aktivaci Metody KB Klíč způsobem uvedeným v těchto podmínkách a Metodu KB Klíč ve starém zařízení deaktivovat způsobem uvedeným v těchto podmínkách, pokud ho již nehodláte používat.
- 7.12 **Blokace a deaktivace Metody Certifikát uložený na čipové kartě.** Pokud čipová karta obsahuje současně komerční Certifikát i kvalifikovaný Certifikát a dojde k blokaci či deaktivaci této Metody, pak dochází k blokaci či deaktivaci obou těchto Certifikátů. To neplatí, dojde-li k blokaci této Metody z důvodu změny identifikačních údajů, které jsou součástí této Metody. V takovém případě dojde ke zneplatnění pouze kvalifikovaného Certifikátu. Pro účely těchto podmínek se blokací i deaktivací Certifikátu rozumí jeho zneplatnění. Zneplatnění nabývá účinku okamžitě, jakmile ho provedeme.
- 7.13 **Informace o platnosti Certifikátu.** Na základě eIDAS jsme povinni poskytnout kterékoli spoléhající se straně informace o platnosti nebo o zneplatnění Certifikátů, které jsme vydali.

## Článek 8. Bezpečnost

- 8.1 **Bezpečnost před aktivací Metody – ztráta, odcizení.** Pokud dojde ke ztrátě nebo odcizení mobilního telefonu či zařízení nebo zneužití či znepřístupnění e-mailové adresy určené pro doručení jednorázového hesla před vytvořením Certifikátu, nebo pokud dojde ke ztrátě nebo odcizení mobilního telefonu či zařízení určeného pro doručení jednorázového hesla před aktivací metody, máte povinnost nás o této skutečnosti neprodleně informovat prostřednictvím Klientské linky a dohodnout s námi náhradní způsob doručení nového jednorázového hesla. Původní jednorázové heslo následně zablokujeme. V případě Certifikátu můžeme použít pro náhradní doručení jednorázového hesla vaší e-mailovou adresu dle Smlouvy.
- 8.2 **Certifikát.** Odpovídáte za proces vytváření Certifikátu včetně vygenerování Veřejného klíče a Soukromého klíče na počítači, který jste k tomuto účelu použili. Dále odpovídáte za používání Certifikátu včetně Soukromého klíče, neboť jste jeho výlučným uživatelem.
- 8.3 Soukromý klíč uložený v datovém souboru je chráněn heslem. Soukromý klíč uložený na čipové kartě je chráněn PIN.
- 8.4 Máte povinnost chránit svůj Soukromý klíč a heslo, popřípadě PIN a PUK, určené k použití Soukromého klíče po celou dobu platnosti Certifikátu, a to zejména proti ztrátě, vyrazení třetí osobě, modifikaci nebo jeho neoprávněnému použití. Heslo, popřípadě PIN a PUK, určené k použití Soukromého klíče nesmíte ukládat na stejném místě či stejném médiu jako Soukromý klíč a nikdy jej nesmíte uložit tak, aby bylo přístupné třetí osobě. Zejména nesmíte ponechat nezabezpečený Soukromý klíč v počítači ve stavu, kdy je zadáno heslo a klíč je aktivován, nebo zasunutou čipovou kartu ve čtečce čipových karet mimo dobu, kdy se přihlašujete do příslušné Bankovní služby nebo používáte Elektronický podpis. Soustavně musíte kontrolovat, zda nedošlo ke ztrátě, odcizení, zneužití nebo neautorizované použití Certifikátu.
- 8.5 **Ztráta čipové karty.** Pokud dojde ke ztrátě čipové karty s uloženým osobním certifikátem, nebo ztrátě bezpečnostních prvků k čipové kartě, máte povinnost nás o této skutečnosti neprodleně informovat na výše uvedeném telefonním čísle a požádat o blokaci osobního certifikátu.
- 8.6 **KB Klíč.** Metoda KB Klíč je chráněna PINem. Na různých zařízeních si v jednotlivých aplikacích s aktivovanou Metodou KB Klíč můžete nastavit různé PINy. Tyto PINy musíte chránit a nesmíte je sdělovat třetí osobě. Dále máte povinnost chránit si svá zařízení, na kterých je Metoda aktivována a neumožnit přístup k nim ani jejich používání třetí osobě. Stejným způsobem musíte chránit Jednorázová hesla pro aktivaci této Metody. Máte povinnost zamítnout požadavek a okamžitě nás kontaktovat, pokud vám přijde do KB Klíče požadavek na přihlášení nebo autorizaci transakce, kterou jste nezadali (např. požadavek na provedení platby nebo přidání či výměnu mobilního zařízení). Stejně tak máte povinnost pečlivě číst veškeré požadavky či zprávy, které vám jsou zaslány do KB Klíč a nepotvrzovat je, pokud jste je sami nezadali, nebo jste je nezadali ve spolupráci se zaměstnancem banky.

# PODMÍNKY K ELEKTRONICKÉMU PODPISU A BANKOVNÍ IDENTITĚ KB

- 8.7 Ztrátu, odcizení nebo byť jen podezření na zneužití kterékoliv z Metod, nebo hesla, PINu či PUKu, nám musíte bez odkladu oznámit a požádat nás o blokaci příslušné Metody.
- 8.8 **KB Klíč, Bezpečnostní heslo.** Pro účely dalšího ověření při přihlášení těmito Metodami, můžeme vyžadovat vedle zadání identifikačního čísla, PIN a dalších prvků také číslo kontaktního telefonu dle Smlouvy.

## Ustanovení společná všem Metodám

- 8.9 Své informační povinnosti dle těchto Podmínek plníte vůči nám prostřednictvím kteréhokoliv našeho obchodního místa, elektronicky na adresu uvedenou v příslušných Produktových podmínkách nebo prostřednictvím výše uvedeného telefonního čísla. Pokud nesplníte svou informační povinnost vůči nám do 3 Obchodních dnů ode dne, kdy vám tato povinnost vznikla, aniž by vám v tom bránily důvody hodné zvláštního zřetele, platí, že výše uvedená skutečnost nám nebyla oznámena bez zbytečného odkladu.
- 8.10 Síť elektronických komunikací (veřejné telefonní linky, linky mobilních sítí, e-mail a fax) sloužící pro naši vzájemnou komunikaci dle Podmínek nejsou pod naší přímou kontrolou, a tudíž neodpovídáme za škodu způsobenou vám jejich případným zneužitím. Ochranu těchto sítí a důvěrnost jimi zasílaných zpráv jsou povinni zajišťovat příslušní poskytovatelé služeb elektronických komunikací, zejména ve smyslu z.č. 127/2005 Sb., o elektronických komunikacích, ve znění pozdějších předpisů.
- 8.11 Neodpovídáme za neautorizované nebo nesprávně provedené platební transakce ani za škodu, která vám vznikla v důsledku porušení vašich povinností stanovených v Podmínkách, ani za škody vzniklé v důsledku chybné autorizace, neprovedení Příkazu z důvodů na vaší straně nebo z důvodů na straně příjemce platby. Neodpovídáme za zneužití Metody, ke kterému došlo v důsledku zneužití vámi používaného počítače či jiného zařízení (např. programem jiného výrobce, zavirováním počítače, hardwarovou závadou apod.)
- 8.12 Neodpovídáme za případy, kdy Metodu nelze využít z důvodů mimo naši kontrolu nebo mimo kontrolu našich partnerů (přerušení dodávky elektrické energie, přerušení spojení prostřednictvím veřejné telefonní sítě, veřejné sítě Internet, stávka atd.). Nejste-li Kvalifikovaným klientem dle VOP, nemusíme vám doložit, že byl dodržen postup, který umožňuje ověřit, že byl dán platební příkaz, že platební transakce byla autorizována, správně zaznamenána, zaúčtována a že nebyla ovlivněna technickou poruchou nebo jinou závadou.
- 8.13 **Obecné povinnosti.** Bez odkladu po zjištění ztráty, odcizení nebo zneužití vaší i) Bankovní identity KB, ii) vašich Bezpečnostních údajů a Bezpečnostních prvků a též při podezření na skutečnosti výše uvedené máte povinnost nám takovou skutečnost oznámit a požádat o blokaci příslušné Metody.
- 8.14 Máte povinnost chránit Bezpečnostní údaje a Bezpečnostní prvky, především před jejich ztrátou, vyzrazením, odcizením nebo zneužitím.

Zavazujete se dále provést taková opatření, aby nemohlo dojít ke zneužití systému přímého bankovníctví, nebo vašeho zařízení třetí stranou či Bankovní identity KB. Zejména máte povinnost v případě využívání čtečky otisků prstů nebo technologie rozpoznání obličeje v mobilním zařízení mít v takovémto zařízení uloženy pouze své identifikační prvky a neumožnit přidání identifikačních prvků do zařízení třetí osobě. Obdobně toto platí pro případně další technologie identifikace majitele mobilního zařízení na úrovni operačního systému, které budeme akceptovat. Berete na vědomí, že pro zadání vašich přihlašovacích údajů pro přihlášení do vašeho internetového bankovníctví je možné použít pouze internetovou adresu <https://login.kb.cz>. Tuto adresu zadávejte přímo. K jejímu nalezení nepoužívejte žádné vyhledávače. Pokud se přihlašujete do internetového bankovníctví prostřednictvím KB Klíče, máte povinnost si ověřit, že alfanumerický kontrolní kód zobrazený v KB Klíči se shoduje s kódem na přihlašovací obrazovce. Pro přístup přes aplikace PSD2 licencovaných třetích stran je přípustné přesměrování z těchto aplikací, avšak pouze na kteroukoli z výše uvedených stránek pro zadání vašich přihlašovacích údajů. Porušení této povinnosti považujeme za hrubou nedbalost a neodpovídáme za škodu vám způsobenou, pokud dojde k zadání vašich přihlašovacích údajů do vašeho internetového bankovníctví prostřednictvím jiné než výše uvedené internetové adresy nebo na jinou než výše uvedenou internetovou adresu. V důsledku této hrubé nedbalosti jste odpovědní v plné výši za veškeré újmy způsobené vám ze strany třetích osob, a to až do okamžiku prokazatelného nahlášení ztráty, odcizení nebo zneužití vašich Bezpečnostních údajů a Bezpečnostních prvků.

# PODMÍNKY K ELEKTRONICKÉMU PODPISU A BANKOVNÍ IDENTITĚ KB

- 8.15 Další povinnosti zajišťující bezpečnost vašeho zařízení.** Máte povinnost při práci s vaším zařízením: používat a aktualizovat antivirový program, používat aktualizovaný operační systém a aktualizovaný internetový prohlížeč, navštěvovat pouze známé stránky, nestahovat a neinstalovat programy z nedůvěryhodných zdrojů, nepoužívat mobilní zařízení s upraveným nastavením (např. jailbreak či root), používat zařízení důvěryhodné a řádně zabezpečené, do chytrého telefonu stahovat pouze aplikace z oficiálních zdrojů (např. Google Play, Apple Store) používat heslo nikoliv jednoduché, nikoliv odvoditelné z osobních údajů, trvale kontrolovat své zařízení, nesdělovat přístupové údaje třetí osobě, nezaznamenávat je ve snadno rozeznatelné podobě ani neuchovávat či nenosit společně se zařízením, nepovolovat zapamatování hesla v internetovém prohlížeči, nezadávat bezdůvodně své citlivé údaje prostřednictvím internetu, neotevírat přílohy podezřelých e-mailů či soubory s neznámým obsahem, nereagovat na podezřelé e-mailové zprávy zejm. požadující zaslání hesel, kódů PIN, čísel platebních karet atd., neklikat na odkazy v takových zprávách a e-mailech. Pravost emailu odesílaného z KB si můžete ověřit v Pravidlech pro odesílání elektronické komunikace, která najdete v Desateru bezpečnosti. Dále máte povinnost chránit své zařízení, které používáte k internetovému bankovníctví, nebo na kterém máte aktivovanou Metodu, před jeho zneužitím třetí osobou, používat pouze svůj počítač nebo mobilní telefon pro přihlášení do svého internetového bankovníctví, zamítnout požadavek a okamžitě nás kontaktovat, pokud vám přijde do KB Klíče požadavek na přihlášení nebo transakci, který jste nezadali, pravidelně sledovat historii svého přihlašování do internetového bankovníctví a pravidelně kontrolovat svou transakční historii.
- 8.16 Vaše odpovědnost.** Odpovídáte nám za škodu, která nám vznikne porušením vašich povinností uvedených v Podmínkách.
- 8.17** Z bezpečnostních důvodů, zejména s ohledem na prevenci případného zneužití jednotlivých Metod, jsme oprávněni získávat anonymní údaje související s vaším využíváním těchto Metod a zároveň jsme oprávněni omezit zaslání Jednorázových hesel.
- 8.18** V souladu s Nařízením Komise (EU) 2018/389 uplatňujeme mechanismus sledování transakcí pro odhalování neautorizovaných nebo podvodných platebních transakcí. V rámci vašeho přihlášení do následujících služeb přímého bankovníctví: MojeBanka, MojeBanka Business, Profibanka a Mobilní Banka zpracováváme a vyhodnocujeme údaje o vašem zařízení, prohlížeči a probíhajícím spojení za účelem identifikace známek napadení malwarem. Zpracování probíhá pomocí komponenty ThreatMark Anti-Fraud Suite, kterou nám poskytuje společnost ThreatMark s.r.o. (IČO: 04222091), která je pro nás zpracovatelem vašich osobních údajů. Údaje jsou uchovávány pro identifikaci a vyhodnocení možných hrozeb. Další informace o zpracování osobních údajů naleznete v Informaci o zpracování osobních údajů pro naše klienty zveřejněné na našich internetových stránkách.
- 8.19** V případě, že elektronický dokument podepíšete Metodou KB Klíč nebo Bezpečnostní heslo je k elektronickému dokumentu připojen náš serverový certifikát a dojde k tzv. vzdálenému podepisování formou služby „Server Side Signing“. Tím je zajištěno zachycení jednatelky osoby, obsahu právního jednání a objektivní zajištění zachování integrity záznamů uchovávaných v našem elektronickém informačním systému. K připojení našeho serverového certifikátu dochází automaticky.
- 8.20** Zákonní zástupci nezletilých uživatelů v postavení smluvní strany, mají povinnost nepoužívat či nezneužívat systém přímého bankovníctví, zařízení či Bankovní identitu KB vystavenou těmto nezletilým uživatelům. Při porušení této povinnosti nese zákonný zástupce odpovědnost nejen vůči nezletilému uživateli, ale i nám a třetím stranám.

## Článek 9. Zánik smluvního vztahu

- 9.1** Smlouva zaniká:
- Výpovědí jedné ze smluvních stran. Vy i my jsme oprávněni Smlouvu kdykoli písemně vypovědět bez udání důvodu. Výpověď vůči nám je účinná následující Obchodní den po dni, ve kterém nám bude doručena. Vůči vám činí výpovědní doba 2 měsíce, nestanovíme-li ve výpovědi dobu delší, a počíná běžet okamžikem, kdy vám bude výpověď doručena. Původní Smlouva o certifikátu zaniká automaticky s ukončením platnosti Certifikátu,
  - Rozhodným dnem,
  - V případě, že vypovídáte smlouvu o Účtu v rámci změny platebního účtu dle příslušných právních předpisů<sup>5</sup>, dnem, kdy tento platební účet zanikne, pokud vám již současně jiný platební účet nevedeme,
  - Počínaje dnem 18. 7. 2023, pak uplynutím 2 let od okamžiku uzavření smlouvy, na základě, které vám byla Metoda poskytnuta (bez ohledu na její aktivaci či deaktivaci), či od posledního použití Metody, a to vždy za předpokladu, že z vaší strany nedošlo vůči nám či jinému subjektu v průběhu tohoto období k úspěšnému použití žádné vaší Metody za účelem autentizace, autorizace či elektronického podpisu.
- 9.2** Naše právo odstoupit od Smlouvy za podmínek uvedených ve VOP není dotčeno.

<sup>5</sup> z.č. 370/2017 Sb., o platebním styku, ve znění pozdějších předpisů

# PODMÍNKY K ELEKTRONICKÉMU PODPISU A BANKOVNÍ IDENTITĚ KB

9.3 Po zániku Smlouvy nesmíte žádnou z Metod nadále používat.

## Článek 10. Vymezení pojmů

10.1 Pojmy s velkým počátečním písmenem mají v Podmínkách význam stanovený ve VOP nebo následující:

„**Bezpečnostní prvky**“ jsou zejména výpočetní technika (např. počítač, notebook) a mobilní zařízení (např. mobilní telefon, hodinky, tablet) včetně software, čipová karta, platební karta a další prvky sloužící k využívání bankovních služeb a Metod.

„**Bezpečnostní údaje**“ jsou údaje sloužící k ověření Klienta, zejména Jednorázové heslo, heslo, PIN, PUK, jednorázový kód (QR kód, kontrolní kód apod.) Touch ID, Face ID, vaše přihlašovací identifikační číslo (ID), uživatelské jméno, Soukromý klíč a jiné přístupové údaje, číslo platební karty a bezpečnostní CVV/CVC kód.

„**Banka**“ je Komerční banka, a.s. se sídlem Praha 1, Na Příkopě 33, čp. 969, PSČ 114 07, IČO: 45317054, zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl B, vložka 1360.

„**Bankovní služby**“ jsou jakékoliv bankovní obchody, služby a produkty poskytované Bankou na základě bankovní licence Banky, včetně investičních služeb poskytovaných Bankou jako obchodníkem s cennými papíry.

„**Bezpečnostní heslo**“ je Metoda založená na vzniku bezpečnostního hesla pro webové aplikace, založená na řetězci znaků známém pouze Klientovi a umožňující zejména ověřit identitu podepisující osoby, elektronicky podepisovat dokumenty či autorizovat platební transakce.

„**Certifikační politika**“ je dokument, ve kterém Banka stanoví pravidla a postupy při používání Certifikátu a jeho specifikaci a který je Banka oprávněna měnit. Certifikační politiku Banka zveřejňuje na internetových stránkách Banky. Certifikační politika je k dispozici také v obchodních místech Banky. Tento dokument není Oznámením ve smyslu VOP.

„**Certifikát**“ je Metoda ve formě osobního certifikátu uloženého na čipové kartě umožňující zejména ověřit identitu podepisující osoby, elektronicky podepisovat dokumenty či autorizovat platební transakce. Obsahuje Veřejný klíč, Soukromý klíč a identifikační údaje Klienta. Certifikát může být dle volby Klienta komerční nebo kvalifikovaný.

„**Desatero bezpečnosti**“ je dokument Desatero bezpečnosti pro používání přímého bankovníctví, ve kterém jsou uvedeny základní zásady bezpečného používání přímého bankovníctví a který je Banka oprávněna měnit. Desatero bezpečnosti Banka zveřejňuje na svých internetových stránkách a je též k dispozici v obchodních místech Banky. Tento dokument není Oznámením ve smyslu VOP.

„**eIDAS**“ je Nařízení evropského parlamentu a rady (EU) č. 910/2014, o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES, ve znění pozdějších revizí, které upravuje zejména elektronické podpisy a elektronickou identitu.

„**Elektronický podpis**“ je elektronický podpis ve smyslu eIDAS, založený zejména na Metodách, které vám poskytujeme na základě Smlouvy.

„**Jednorázové heslo**“ je bezpečnostní heslo zasílané prostřednictvím SMS zprávy na sjednané číslo mobilního telefonu, které slouží jako jednorázové heslo pro aktivaci či odblokování Metody, Mobilní banky, pro přidání či výměnu zařízení pro KB Klíč nebo přidání zařízení pro Mobilní banku, dále v některých případech k autorizaci transakcí a pro použití Metody Bezpečnostní heslo.

„**KB Klíč**“ je Metoda poskytovaná na základě Smlouvy, založená na individuálních vlastnostech aktivované mobilní aplikace pro podporovaná zařízení a znalosti bezpečnostního PIN nebo biometrie, umožňující zejména ověřit identitu podepisující osoby, elektronicky podepisovat dokumenty či autorizovat platební transakce. Tato Metoda může být aktivována v různých aplikacích (např. v aplikaci KB Klíč).

„**KB Podpisový modul**“ je softwarový doplněk, který je instalován jako součást programového vybavení pro bezpečné používání Certifikátu KB a jeho správu ve službách přímého bankovníctví nebo portálu MůjProfil.

„**Klient**“ je osoba, která uzavřela s Bankou Smlouvu.

„**Klientská linka**“ je nepřetržitá telefonní linka s číslem + 420 955 551 552 pro volání v českém jazyce a s číslem + 420 955 551 556 „Customer Service KB“ pro volání v anglickém jazyce. V případě změny telefonního čísla je aktuální vždy k dispozici na internetových stránkách.

„**Metoda**“ je prostředek pro vaši identifikaci, autentizaci, autorizaci a vytváření Elektronického podpisu a případně Bankovní identity KB, poskytovaný na základě Smlouvy.

„**MojeBanka**“ je internetové bankovníctví, které může Klient využívat na základě smlouvy o poskytování přímého bankovníctví.

# PODMÍNKY K ELEKTRONICKÉMU PODPISU A BANKOVNÍ IDENTITĚ KB

„**MůjProfil**“ je portál pro podporu a správu Metod. MůjProfil je Klientovi přístupný na internetových stránkách Banky, kam se přihlašuje pomocí libovolné Metody, případně, je-li to umožněno, pak přímo z našeho internetového bankovníctví.

„**Národní bod**“ je informační systém veřejné správy podporující proces elektronické identifikace a autentizace prostřednictvím kvalifikovaného systému, jehož správcem je Digitální informační agentura.

„**Obchodní den**“ je den, na který nepřípadá sobota, neděle, státní svátek ani ostatní svátky ve smyslu příslušných právních předpisů a ve který je Banka otevřena pro poskytování Bankovních služeb, a zároveň jsou jiné instituce, které se účastní poskytnutí Bankovní služby nebo na kterých je poskytnutí Bankovní služby závislé, otevřeny pro poskytování příslušných služeb.

„**Oznámení**“ jsou sdělení, ve kterých jsou v souladu s VOP nebo příslušnými Produktovými podmínkami stanoveny další podmínky a technické aspekty poskytování Bankovních služeb. Oznámením není zejména Certifikační politika a Desatero bezpečnosti.

„**PIN pro Čipovou kartu**“ je osobní čtyřmístné číselné identifikační číslo sloužící k ověření oprávněnosti nakládat s čipovou kartou.

„**PIN pro KB Klíč**“ je osobní číselný kód sloužící k ověření oprávněnosti nakládat s aplikací k používání Metody KB Klíč.

„**Platební služby**“ jsou Bankovní služby, které jsou platebními službami ve smyslu zákona o platebním styku (např. převody peněžních prostředků, vydávání platebních prostředků a výběry a vklady hotovosti).

„**Podmínky**“ jsou tyto Podmínky k elektronickému podpisu a Bankovní identitě KB, jež představují Produktové podmínky dle VOP.

„**Produktové podmínky**“ jsou podmínky Banky upravující poskytování jednotlivých Bankovních služeb.

„**PUK**“ je osmimístný číselný kód sloužící k odblokování čipové karty.

„**QSCD**“ (Qualified Signature Creation Device) je typ hardwarového zařízení, které splňuje specifické technické požadavky, bylo certifikováno kvalifikovaným poskytovatelem důvěryhodných služeb a používá se k vytváření kvalifikovaných elektronických podpisů ve smyslu nařízení eIDAS.

„**Sazebník**“ je přehled všech poplatků, ostatních cen a jiných plateb za Bankovní služby a za úkony s Bankovními službami souvisejícími.

„**Smlouva**“ je smlouva, na základě které si Klient sjednává Metodu/y.

„**Soukromý klíč**“ jsou data pro vytváření Elektronického podpisu Klienta ve formě Certifikátu.

„**Technické podmínky**“ jsou dokument, ve kterém Banka stanoví technické parametry pro poskytování služeb přímého bankovníctví. Technické podmínky Banka zveřejňuje na svých internetových stránkách. Technické podmínky je Banka oprávněna měnit. Technické podmínky nejsou Oznámením ve smyslu VOP.

„**Veřejný klíč**“ jsou data pro ověření Elektronického podpisu Klienta ve formě Certifikátu.

„**VOP**“ jsou Všeobecné obchodní podmínky Banky.

**10.2** Odkazy na naše internetové stránky jsou odkazy na adresu [www.mojebanka.cz](http://www.mojebanka.cz), případně na jiné internetové adresy, které používáme nebo budeme používat v souvislosti s poskytováním Bankovních služeb.

## Článek 11. Závěrečná ustanovení

**11.1** Tam, kde jsou ve smlouvách a dalších dokumentech sjednaných mezi námi a vámi či smluvních dokumentech, které jsou nedílnou součástí takových smluv, uvedeny pojmy Podmínky k elektronickému podpisu nebo Smlouva o elektronickém podpisu, rozumí se tím Podmínky k elektronickému podpisu a Bankovní identitě KB nebo Smlouva o elektronickém podpisu a Bankovní identitě KB.

**11.2** Podmínky jsme oprávněni průběžně měnit způsobem uvedeným ve VOP. O změně vás informujeme prostřednictvím příslušné služby přímého bankovníctví nebo způsobem uvedeným ve VOP.

**11.3** Podmínky ruší a nahrazují Podmínky k elektronickému podpisu ze dne 16. 4. 2024.

**11.4** Podmínky nabývají účinnosti dne 1. 5. 2026.