



Tyto podmínky obsahují bližší úpravu práv a povinností vyplývajících z uzavřené smlouvy k elektronickému podpisu. Seznamte se prosím důkladně s tímto dokumentem. Vaše případné dotazy rádi zodpovíme.

Článek 1. Metody pro vytváření elektronického podpisu

- 1.1 V rámci vybraných Bankovních služeb, zejména služeb přímého bankovníctví, můžete používat svůj Elektronický podpis založený na následujících metodách:
 - Certifikát uložený v datovém souboru
 - Certifikát uložený na čipové kartě,
 - KB klíč
 - Bezpečnostní hesloU některých Bankovních služeb si vyhrazujeme právo akceptovat pouze některé metody, přičemž jednotlivé metody mohou sloužit jak pro vaši autentizaci, tak pro Elektronický podpis samotný.
- 1.2 Metody pro vytváření Elektronického podpisu poskytnuté vám na základě Smlouvy 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 zákoníkem¹.
- 1.5 Podpisem Smlouvy stvrzujete, že jste se seznámil s obsahem a významem Certifikační politiky a s Desaterem bezpečnosti a souhlasíte, že se budete řídit jejich ustanoveními a dodržovat zásady v nich uvedené.
- 1.6 Technické informace k jednotlivým metodám naleznete v Technických podmínkách.

Článek 2. Certifikáty

- 2.1 Certifikát můžete sjednat ve formě jeho uložení v datovém souboru nebo na čipové kartě.

Certifikát uložený v datovém souboru

- 2.2 **Aktivace.** Po uzavření Smlouvy vám na sjednané číslo mobilního telefonu zašleme SMS zprávu s jednorázovým heslem pro vytvoření Certifikátu včetně vygenerování Soukromého a Veřejného klíče. Jednorázové heslo je platné po dobu 7 dnů od jeho zaslání. Po uplynutí této lhůty vám Certifikát vydáme pouze na základě nové Smlouvy.
- 2.3 Číslo mobilního telefonu pro zaslání jednorázového hesla a Autorizačních SMS zpráv, které uvedete ve Smlouvě, nemůže být použito pro stejné účely jiným Klientem. Neodpovídáme za škody vzniklé uvedením nesprávného čísla mobilního telefonu nebo e-mailové adresy pro doručení jednorázového hesla nebo Autorizační SMS zprávy.
- 2.4 Certifikát si vytvoříte s pomocí jednorázového hesla v Certifikačním průvodci. Předtím si zkontrolujte správnost zobrazených identifikačních údajů s údaji uvedenými ve Smlouvě.

Certifikát uložený v datovém souboru v internetovém prohlížeči

- 2.5 Certifikát uložený v datovém souboru si můžete přenést do příslušného internetového prohlížeče a využívat jej tak ve formě uložení v datovém souboru i přenesený do internetového prohlížeče. Další informace k tomuto postupu naleznete v Technických podmínkách.

Certifikát uložený na čipové kartě

- 2.6 **Aktivace.** S vaší součinností vám po uzavření Smlouvy zašleme formou SMS zprávy na sjednané číslo mobilního telefonu jednorázové heslo, abyste si mohl Certifikát vytvořit v portálu MůjProfil, nebo vám vytvoříme Certifikát včetně vygenerování Soukromého a Veřejného klíče a uložíme na čipovou kartu. Jednorázové heslo je platné po dobu 7 dnů od jeho zaslání. Současně vám předáme čipovou kartu a

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

PODMÍNKY K ELEKTRONICKÉMU PODPISU

obálku s PIN a PUK.

Článek 3. KB klíč

- 3.1 Aktivace.** Při uzavření Smlouvy, nebo kdykoliv poté, pokud nás o to námi akceptovaným způsobem požádáte, vám na sjednané číslo mobilního telefonu zašleme SMS zprávu s jednorázovým heslem pro aktivaci aplikace k používání metody KB klíč. Jednorázové heslo je platné po dobu 7 dnů od jeho zaslání. Po uplynutí této lhůty je nutné si nechat aktivační heslo znovu zaslat.
- 3.2** Číslo mobilního telefonu pro zaslání jednorázového hesla a Autorizačních SMS zpráv, které uvedete ve Smlouvě, nemůže být použito pro stejné účely jiným Klientem. Neodpovídáme za škody vzniklé uvedením nesprávného čísla mobilního telefonu pro doručení jednorázové hesla nebo Autorizační SMS zprávy.
- 3.3** Aplikaci k používání metody KB klíč si stáhněte v Google Play pro zařízení se systémem Android nebo v Apple Store pro zařízení se systémem iOS. Věnujte pozornost vydavateli aplikace, kterým musí být Komerční banka a.s.
Aplikaci aktivujete přímo v mobilním telefonu pomocí vašeho identifikačního čísla uvedeného v žádosti o aktivaci metody a pomocí jednorázového hesla zasláného pomocí SMS dle čl. 3.1.
- 3.4** Metodu KB Klíč je možné používat pouze v jednom mobilním zařízení. Další technické informace naleznete v Technických podmínkách.

Článek 4. Bezpečnostní heslo

- 4.1 Aktivace.** Při uzavření Smlouvy, nebo kdykoliv poté, pokud nás o to námi akceptovaným způsobem požádáte, vám na sjednané číslo mobilního telefonu zašleme SMS zprávu s jednorázovým heslem pro aktivaci metody Bezpečnostní heslo. Jednorázové heslo je platné po dobu 7 dnů od jeho zaslání. Po uplynutí této lhůty je nutné si nechat aktivační heslo znovu zaslat.
- 4.2** Číslo mobilního telefonu pro zaslání jednorázového hesla a Autorizačních SMS zpráv, 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 jednorázové hesla nebo Autorizační SMS zprávy.
- 4.3** Při prvním použití metody Bezpečnostní heslo provádíte aktivaci s využitím vašeho identifikačního čísla uvedeného v žádosti o aktivaci a jednorázového hesla zasláného pomocí SMS dle čl. 4.1.
- 4.4** Další technické informace naleznete v Technických podmínkách.

Článek 5. Platnost jednotlivých metod pro vytváření Elektronického podpisu

- 5.1 Platnost Certifikátu.** Obecná platnost Certifikátu je 2 roky. Konkrétní doba platnosti Certifikátu je uvedena v Certifikátu, nebo ji zjistíte v portálu MůjProfil nebo dočasně také v Certifikačním průvodci. Platný a účinný Certifikát můžete používat při využívání Služeb. Před koncem jeho platnosti můžete v Certifikačním průvodci požádat o jeho prodloužení.
- 5.2** 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 2 Podmínek se pro vydání nového Certifikátu použije obdobně.
- 5.3** V případě, že dojde ke změně vašich identifikačních údajů uvedených ve Smlouvě (včetně čísla mobilního telefonu sjednaného pro zasílání Autorizačních SMS zpráv), jste povinen nás o tom bez zbytečného odkladu písemně informovat a zároveň s námi uzavřít dodatek ke Smlouvě nebo požádat o vydání nového Certifikátu. V případě, že dojde ke změně vaší e-mailové adresy uvedené ve Smlouvě, jste povinen nás o tom informovat v Klientově obchodním místě nebo po přihlášení do portálu MůjProfil kde provedete změnu tohoto údaje.
- 5.4 Platnost KB Klíče, Bezpečnostního hesla.** Platnost těchto metod není časově omezena.

PODMÍNKY K ELEKTRONICKÉMU PODPISU

Článek 6. Blokování metod pro vytváření Elektronického podpisu

- 6.1 Pokud bude metoda pro vytváření Elektronického podpisu zablokována, její platnost je pozastavena do doby než nás požádáte o její opětovnou aktivaci. Informace o zablokování metody vám bude sdělena na kontaktní telefon dle Smlouvy.
- 6.2 **Blokace z vaší strany.** O blokaci metody jste oprávněn požádat kdykoli, a to na telefonním čísle +420 955 551 552, v kterémkoli našem obchodním místě nebo na našich internetových stránkách v rámci portálu MůjProfil. O blokaci metody jste pak povinen požádat vždy, máte-li podezření na její možné zneužití.
- 6.3 **Blokace z naší strany.** Metodu zablokujeme a případně budeme požadovat, abyste požádal 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,
 - porušil jste jakoukoliv povinnost vyplývající ze Smlouvy,
 - ve více Smlouvách a/nebo pro více Klientů bylo sjednáno stejné číslo mobilního telefonu pro zaslání jednorázového hesla a Autorizačních SMS zpráv,
 - 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.
- 6.4 U Certifikátu uloženého na čipové kartě se při třetím chybném zadání PIN čipová karta zablokuje. O odblokování čipové karty můžete požádat ve vašem obchodním místě nebo jej může provést sám prostřednictvím programového vybavení Cryptoplus KB. V obou případech způsobu odblokování čipové karty musíte uvést PUK.
- 6.5 V případě KB Klíče a Bezpečnostního hesla se při stanoveném počtu chybných pokusů tyto metody zablokují.

Článek 7. Bezpečnost

- 7.1 **Bezpečnost před aktivací metody – ztráta, odcizení.** Pokud dojde ke ztrátě nebo odcizení mobilního telefonu nebo zneužití či znepřístupnění e-mailové adresy určené pro doručení jednorázového hesla před vytvořením Certifikátu, nebo pokud dojde ke ztrátě nebo odcizení mobilního telefonu určené pro doručení jednorázového hesla před aktivací metody, jste povinen nás o této skutečnosti neprodleně informovat na telefonním čísle **+420 955 551 552** 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 vaši e-mailovou adresu, je-li ve Smlouvě uvedena.
- 7.2 **Certifikát.** Odpovídáte za proces vytváření Certifikátu včetně vygenerování Veřejného klíče a Soukromého klíče na počítači, který jste k tomuto účelu použil. Dále odpovídáte za používání Certifikátu včetně Soukromého klíče, neboť jste jeho výlučným uživatelem.
- 7.3 Soukromý klíč uložený v datovém souboru je chráněn heslem. Soukromý klíč uložený na čipové kartě je chráněn PIN.
- 7.4 Jste povinen 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, vyzrazení 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 třetím osobám. 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.
- 7.5 **Ztráta čipové karty.** Pokud dojde ke ztrátě čipové karty s uloženým osobním certifikátem, nebo ztrátě bezpečnostních prvků k čipové kartě, jste povinen nás o této skutečnosti neprodleně informovat na výše uvedeném telefonním čísle a požádat o blokaci osobního certifikátu.
- 7.6 **KB Klíč.** KB klíč je chráněn PIN. V případě KB klíče jste povinen chránit informaci o Vámi zadaném PIN kódu a přístup a užívání zařízení, na kterém jste aplikaci k používání metody KB Klíč aktivovali.
- 7.7 Ztrátu, odcizení nebo zjištění rizika jakéhokoliv zneužití kterékoliv z metod pro vytváření Elektronického podpisu, (hesla, PIN a PUK, jste povinen nám bez odkladu oznámit a požádat o blokaci příslušné metody.

PODMÍNKY K ELEKTRONICKÉMU PODPISU

Ustanovení společná všem metodám

- 7.8** Své informační povinnosti dle těchto Podmínek plníte vůči nám prostřednictvím vašeho 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 jste neoznámil výše uvedenou skutečnost bez zbytečného odkladu.
- 7.9** 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.
- 7.10** 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 pro vytváření Elektronického podpisu, ke kterému došlo v důsledku zneužití vámi používaného počítače (např. programem jiného výrobce, zavirováním počítače, hardwarovou závadou apod.)
- 7.11** 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.
- 7.12** Odpovídáte nám za škodu, která nám vznikne porušením vašich povinností uvedených v Podmínkách.

Článek 8. Zánik smluvního vztahu

- 8.1** 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. Výpověď vůči vám je účinná posledním dnem měsíce následujícího po měsíci, ve kterém vám bude doručena, ledaže jste Kvalifikovaným klientem. V takovém případě jsme oprávněni Smlouvu vypovědět v souladu s VOP;
 - Rozhodným dnem.
- 8.2** Naše právo odstoupit od Smlouvy za podmínek uvedených ve VOP není dotčeno.
- 8.3** Po zániku Smlouvy nesmíte žádnou z metod pro vytváření Elektronického podpisu nadále používat.

Článek 9. Vymezení pojmů

- 9.1** Pojmy s velkým počátečním písmenem mají v Podmínkách následující význam:
- „**Autorizační SMS zpráva**“ je zpráva zasílaná Bankou Klientovi na sjednané číslo mobilního telefonu operátora v ČR (v případě čipové karty i operátora v zahraničí), prostřednictvím které je Klientovi zaslán autorizační SMS kód sloužící k ověření identity Klienta při využívání příslušných Bankovních služeb, zejména služby přímého bankovníctví MojeBanka nebo MojeBanka Business s ověřením prostřednictvím Certifikátu uloženého v datovém souboru.
- „**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 pro vytváření Elektronického podpisu založená na vzniku bezpečnostního hesla pro webové aplikace, založená na řetězci znaků známém pouze Klientovi a umožňující ověřit autentizaci podepisující osoby.
- „**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.
- „**Certifikační průvodce**“ je aplikace pro podporu a správu Certifikátu. Certifikační průvodce je Klientovi

PODMÍNKY K ELEKTRONICKÉMU PODPISU

přístupný na internetových stránkách Banky.

„**Certifikát**“ je metoda pro vytváření Elektronického podpisu ve formě osobního certifikátu umožňující ověřit autentizaci podepisující osoby. Obsahuje Veřejný klíč, Soukromý klíč a identifikační údaje Klienta.

„**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.

„**Elektronický podpis**“ je zaručený elektronický podpis ve smyslu 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, založený na metodách, které vám poskytujeme na základě Smlouvy.

„**KB klíč**“ je metoda pro vytváření Elektronického podpisu založená na individuálních vlastnostech aktivované aplikace pro podporovaná mobilní zařízení a znalosti bezpečnostního PINU, umožňující ověřit autentizaci podepisující osoby.

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

„**Klientovo obchodní místo**“ je obchodní místo Banky, kde Klient uzavřel Smlouvu. V tomto významu je v Podmínkách tento pojem používán též ve spojení „vaše obchodní místo“.

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

„**MůjProfil**“ je portál pro podporu a správu metod pro vytváření Elektronických podpisů. MůjProfil je Klientovi přístupný na internetových stránkách Banky, kam se přihlašuje pomocí libovolné metody pro vytváření elektronického podpisu, případně přímo ze služby MojeBanka.

„**Obchodní den**“ je den, na který nepřipadá 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, 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.

„**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 pro vytváření Elektronického podpisu.

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

„**Technické podmínky**“ jsou dokument, ve kterém Banka stanoví technické podmínky 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.

- 9.2 Odkazy na naše internetové stránky jsou odkazy na adresu www.mojebanka.cz, případně na jiné internetové adresy, které používáme nebo budeme používat v souvislosti s poskytováním Bankovních služeb.

Článek 10. Závěrečná ustanovení

- 10.1 Podmínky jsme oprávněni průběžně měnit způsobem uvedeným ve VOP. O změně vás informujeme prostřednictvím příslušné služby přímého bankovníctví nebo způsobem uvedeným ve VOP.
- 10.2 Podmínky ruší a nahrazují Podmínky k elektronickému podpisu ze dne 11. 9. 2017.
- 10.3 Podmínky nabývají účinnosti dne 20. 5. 2018.