# PODMIENKY K ELEKTRONICKÉMU PODPISU

Tieto Podmienky k elektronickému podpisu (ďalej len „**Podmienky**“) predstavujú Produktové podmienky v zmysle VOP. Tieto Podmienky tvoria súčasť Zmluvy a Držiteľ Certifikátu je povinný sa s nimi oboznámiť a dodržiavať ich.

Pojmy s veľkým začiatočným písmenom sú v týchto Podmienkach používané vo význame uvedenom v článku 7 týchto Podmienok.

## Článok 1. Metóda na vytvorenie elektronického podpisu

**1.1** V rámci vybraných Bankových služieb, najmä služieb priameho bankovníctva, môže Držiteľ Certifikátu používať svoj Elektronický podpis založený na metóde Certifikát uložený na čipovej karte. Uvedená metóda môže slúžiť ako na autentizáciu Držiteľa Certifikátu, tak aj pre Elektronický podpis samotný.

**1.2** Metódu na vytvorenie Elektronického podpisu poskytnutú Držiteľovi Certifikátu na základe Zmluvy môže Držiteľ Certifikátu používať výlučne osobne.

**1.3** Za poskytnutie a používanie metódy a súvisiacich služieb je Banka oprávnená požadovať od Klienta uhradenie ceny podľa Sadzobníka.

**1.4** Zmluva sa riadi právnym poriadkom Slovenskej republiky, a to najmä Obchodným zákonníkom [1].

**1.5** Podpisom Zmluvy Držiteľ Certifikátu potvrdzuje, že sa oboznámil s obsahom a významom Certifikačnej politiky a s Desatorom bezpečnosti a súhlasí, že sa bude riadiť ich ustanoveniami a dodržiavať zásady v nich uvedené.

**1.6** Technické informácie k Certifikátu sú uvedené v Technických podmienkach.

## Článok 2. Certifikát

**2.1** Certifikát môže byť Bankou vydaný len na čipovej karte.

**2.2** **Forma certifikátu**. Certifikát (komerčný aj kvalifikovaný) bude uložený na Bankou poskytnutej čipovej karte. Čipovú kartu si Držiteľ Certifikátu môže zariadiť v štandardnom režime alebo v režime QSCD. Po prevzatí čipovej karty obsahujúcej Certifikát je Držiteľ Certifikátu povinný skontrolovať a overiť údaje, ktoré budú v Certifikáte uvedené, najmä svoje identifikačné údaje v rozsahu meno a priezvisko, typ Certifikátu, e-mailová adresa, krajina bydliska alebo pobytu a číslo čipovej karty. Banka nenesie zodpovednosť v prípade nesprávnych alebo neúplných údajov uvedených v Certifikáte po potvrdení Držiteľa Certifikátu.

**2.3** **Druh Certifikátu**. Certifikát sa vydáva v súlade s platnými právnymi predpismi, ktoré sa vzťahujú na Certifikát. Pri uzatváraní Zmluvy si Držiteľ Certifikátu môže vybrať komerčný alebo kvalifikovaný Certifikát. Pokiaľ si Držiteľ Certifikátu zvolí kvalifikovaný Certifikát, bude mu súčasne poskytnutý Komerčný certifikát, ktorý bude uložený na jeho čipovej karte.

**2.4** **Komerčný certifikát**. Na základe komerčného certifikátu si Držiteľ Certifikátu môže vytvoriť elektronický podpis, ktorý je zdokonaleným elektronickým podpisom (AES) v zmysle nariadenia eIDAS.

**2.5** **Kvalifikovaný certifikát**. V závislosti od režimu čipovej karty je kvalifikovaný Certifikát možné použiť na vytvorenie elektronického podpisu v zmysle zákona o dôveryhodných službách [2], a to v podobe kvalifikovaného elektronického podpisu. Iba kvalifikovaný Certifikát na čipovej karte v QSCD režime je možné použiť na vytvorenie kvalifikovaného elektronického podpisu v zmysle nariadenia eIDAS. Kvalifikovaný certifikát nemožno použiť na autentifikáciu.

## Certifikát uložený na čipovej karte

1 zákon č. 513/1991 Zb. – Obchodný zákonník v znení neskorších predpisov

2 zákon č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách)

**2.6** **Aktivácia**. Po uzatvorení Zmluvy na základe súčinnosti poskytnutej Držiteľom Certifikátu zašle Banka Držiteľovi Certifikátu formou SMS správy na dohodnuté číslo mobilného telefónu jednorazové heslo, aby mohol Držiteľ Certifikátu vytvoriť Certifikát v portáli MôjProfil, alebo Banka vytvorí Držiteľovi Certifikátu Certifikát vrátane vygenerovania Súkromného a Verejného kľúča a uloží ho na čipovú kartu. Jednorazové heslo je platné po dobu 3 dní od jeho zaslania. Súčasne Banka odovzdá Držiteľovi Certifikátu čipovú kartu a obálku s PIN a PUK.

Číslo mobilného telefónu pre zaslanie SMS správy, ktoré Držiteľ Certifikátu uvedie v Zmluve, sa musí zhodovať s číslom mobilného telefónu, ktoré na tento účel uviedol Klient pre tohto Držiteľa Certifikátu v Príkaze k administrácii a nemôže byť použité počas doby platnosti príslušného Certifikátu na rovnaké účely iným Držiteľom Certifikátu. Banka nezodpovedá za škody vzniknuté uvedením nesprávneho čísla mobilného telefónu na doručenie SMS správy.

## Článok 3. Platnosť Certifikátu

**3.1** **Platnosť Certifikátu.** Všeobecná platnosť Certifikátu je 2 roky za predpokladu, že v danom období nenastane Rozhodný deň ani nedôjde k zániku Zmluvy. Konkrétna doba platnosti Certifikátu je uvedená v Certifikáte, alebo je ju možné zistiť v portáli MôjProfil. Platný a účinný Certifikát môže Držiteľ Certifikátu používať pri využívaní Služieb. Pred koncom platnosti Certifikátu môže Držiteľ Certifikátu požiadať o jeho predĺženie prostredníctvom portálu MôjProfil.

**3.2** Pokiaľ Držiteľ Certifikátu požiada Banku o predĺženie Certifikátu pred uplynutím doby jeho platnosti, na základe už uzatvorenej Zmluvy vydá Banka Držiteľovi Certifikátu nový Certifikát, a to výlučne za predpokladu, že ku dňu žiadosti Držiteľa Certifikátu o predĺženie Certifikátu nenastal Rozhodný deň ani nedošlo k zániku Zmluvy. Nový Certifikát Banka vydá Držiteľovi Certifikátu v rovnakej forme ako predchádzajúci Certifikát a s rovnakými notifikačnými údajmi. Okamihom vydania nového Certifikátu nie je Držiteľ Certifikátu oprávnený predchádzajúci Certifikát používať. Postup podľa článku 2 Podmienok sa na vydanie nového Certifikátu použije obdobne.

**3.3** V prípade, že dôjde k zmene identifikačných údajov Držiteľa Certifikátu uvedených v Zmluve (vrátane čísla mobilného telefónu dohodnutého na zasielanie SMS správ), je Držiteľ Certifikátu povinný Banku o tom bez zbytočného odkladu písomne informovať a zároveň s Bankou uzatvoriť dodatok k Zmluve alebo požiadať o vydanie nového Certifikátu. V prípade, že dôjde k zmene e-mailovej adresy Držiteľa Certifikátu uvedenej v Zmluve, je Držiteľ Certifikátu povinný Banku o tom písomne informovať v Klientovom obchodnom mieste. Zmena čísla mobilného telefónu dohodnutého na zasielanie SMS správ nemusí byť Bankou akceptovaná, pokiaľ zmenené číslo mobilného telefónu nie je zhodné s číslom mobilného telefónu, ktoré z dôvodu zmeny identifikačných údajov tohto Držiteľa Certifikátu uviedol Klient pre tohto Držiteľa Certifikátu v Príkaze k administrácii.

## Článok 4. Blokovanie a deaktivácia Certifikátu

**4.1** **Blokovanie a deaktivácia**. Pokiaľ bude Certifikát zablokovaný, jeho platnosť je pozastavená do doby, než Držiteľ Certifikátu Banku požiada o jej opätovnú aktiváciu. Ak je Certifikát deaktivovaný, je úplne ukončený. Pokiaľ ho bude chcieť Držiteľ Certifkátu znova používať, je nevyhnutné ho znova aktivovať. Informácia o zablokovaní metódy bude Držiteľovi Certifikátu oznámená na kontaktný telefón podľa Zmluvy.

**4.2** **Blokovanie zo strany Banky**. Banka je oprávnená zablokovať Certifikát na nevyhnutne potrebný čas, ak je to potrebné zo závažných dôvodov, najmä z bezpečnostných dôvodov (napr. v prípade podozrenia z neoprávneného alebo podvodného použitia alebo v prípade upraveného operačného systému). Keď dôvody na zablokovanie Certifikátu pominú, Banka v súčinnosti s Držiteľom Certifikátu umožní odblokovanie Certifikátu alebo jeho nahradenie iným Certifikátom.

**4.3** **Blokovanie zo strany Držiteľa Certifikátu.** O zablokovanie metódy je Držiteľ Certifikátu oprávnený požiadať kedykoľvek, a to na telefónnom čísle +420 955 551 552, v Klientovom obchodnom mieste alebo na webových stránkach Banky v rámci portálu MôjProfil. O zablokovanie metódy je Držiteľ Certifikátu povinný požiadať vždy, ak má podozrenie na jej možné zneužitie.

**4.4** **Deaktivácia zo strany Banky.** Certifikát Banka zablokuje a prípadne bude Banka požadovať, aby Držiteľ Certifikátu požiadal o jej opätovnú aktiváciu, ak nastane aspoň jedna z nasledujúcich udalostí:

- metóda bola dohodnutá na základe nepravdivých, neúplných alebo zavádzajúcich informácií,
- identifikačné údaje, ktoré sú súčasťou metódy, už nie sú platné,
- Držiteľ Certifikátu porušil akúkoľvek povinnosť vyplývajúcu zo Zmluvy,
- vo viacerých Zmluvách a/alebo pre viac Držiteľov Certifikátu bolo dohodnuté rovnaké číslo mobilného telefónu na zaslanie jednorazového hesla a Autorizačných SMS správ,
- Banka prestane danú metódu poskytovať,
- Banka je k tomu povinná s ohľadom na právne predpisy,
- došlo alebo môže dôjsť k zvýšeniu bezpečnostných rizík alebo opatrení súvisiacich s chybným zadaním bezpečnostných údajov alebo využívaním metódy.

**4.5** **Deaktivácia zo strany Držiteľa Certifikátu**. O deaktiváciu Certifikátu môže Držiteľ Certifikátu požiadať na obchodnom mieste Banky alebo na jej internetových stránkach prostredníctvom portálu MôjProfil.

**4.6** Pri Certifikáte uloženom na čipovej karte sa pri treťom chybnom zadaní PIN čipová karta zablokuje. O odblokovanie čipovej karty môže Držiteľ Certifikátu požiadať v Klientovom obchodnom mieste alebo ho môže Držiteľ Certifikátu vykonať sám prostredníctvom programového vybavenia Cryptoplus KB. V oboch prípadoch spôsobu odblokovania čipovej karty musí Držiteľ Certifikátu uviesť PUK.

**4.7** **Odblokovanie Certifikátu**. V prípade zablokovaného Certifikátu môže Držiteľ Certifikátu požiadať o jeho odblokovanie prostredníctvom obchodného miesta Banky alebo portálu MôjProfil, a to za Bankou stanovených podmienok. Banka si vyhradzuje právo zmeniť spôsoby odblokovania Certifikátu a jeho následného využitia, a to predovšetkým v závislosti na jej technických možnostiach alebo zmene právnych predpisov.

## Článok 5. Bezpečnosť

**5.1** **Bezpečnosť pred aktiváciou metódy – strata, odcudzenie.** Pokiaľ dôjde k strate alebo odcudzeniu mobilného telefónu alebo k zneužitiu či zneprístupneniu e-mailovej adresy, ktoré sú určené na doručenie jednorazového hesla pred vytvorením Certifikátu, alebo pokiaľ dôjde k strate alebo odcudzeniu mobilného telefónu určeného na doručenie jednorazového hesla pred aktiváciou metódy, je Držiteľ Certifikátu povinný Banku o tejto skutočnosti bezodkladne informovať na telefónnom čísle **+420 955 551 552** a dohodnúť s Bankou náhradný spôsob doručenia nového jednorazového hesla. Pôvodné jednorazové heslo následne Banka zablokuje. V prípade Certifikátu môže Banka použiť pre náhradné doručenie jednorazového hesla aj e-mailovú adresu Držiteľa Certifikátu, ak je v Zmluve uvedená.

**5.2** **Certifikát.** Držiteľ Certifikátu zodpovedá za proces vytvorenia Certifikátu vrátane vygenerovania Verejného kľúča a Súkromného kľúča na počítači, ktorý k tomuto účelu Držiteľ Certifikátu použil. Ďalej Držiteľ Certifikátu zodpovedá za používanie Certifikátu vrátane Súkromného kľúča, nakoľko je jeho výlučným užívateľom.

**5.3** Súkromný kľúč uložený v dátovom súbore je chránený heslom. Súkromný kľúč uložený na čipovej karte je chránený PIN.

**5.4** Držiteľ Certifikátu je povinný chrániť svoj Súkromný kľúč a heslo, poprípade PIN a PUK, určené k použití Súkromného kľúča po celú dobu platnosti Certifikátu, a to najmä proti strate, vyzradeniu tretej osobe, modifikácii alebo jeho neoprávnenému použitiu. Heslo, poprípade PIN a PUK, určené k použitiu Súkromného kľúča nesmú byť Držiteľom Certifikátu uložené na rovnakom mieste či rovnakom médiu ako Súkromný kľúč a nikdy nesmú byť uložené tak, aby boli prístupné tretím osobám. Držiteľ Certifikátu najmä nesmie ponechať nezabezpečený Súkromný kľúč v počítači v stave, kedy je zadané heslo a kľúč je aktivovaný alebo zasunutú čipovú kartu v čítačke čipových kariet mimo dobu, kedy sa Držiteľ Certifikátu prihlasuje do príslušnej Bankovej služby alebo používa Elektronický podpis. Držiteľ Certifikátu musí sústavne kontrolovať, či nedošlo k strate, odcudzeniu, zneužitiu alebo neautorizovanému použitiu Certifikátu.

**5.5** **Ďalšie povinnosti na zaistenie bezpečnosti zariadenia Držiteľa Certifikátu**. Pri používaní svojho zariadenia má Držiteľ Certifikátu tieto povinnosti: používať a aktualizovať antivírusový softvér, používať aktualizovaný operačný systém a aktualizovaný webový prehliadač, navštevovať len známe stránky, nesťahovať a neinštalovať programy z nedôveryhodných zdrojov, nepoužívať mobilné zariadenie s upravenými nastaveniami (napr. jailbreak alebo root), používať dôveryhodné a riadne zabezpečené zariadenie, sťahovať len aplikácie z oficiálnych zdrojov (napr. Google Play, Apple Store, Windows Phone Store), používať heslo, ktoré nie je jednoduché a nedá sa odvodiť od osobných údajov, mať zariadenie pod neustálou kontrolou, neposkytovať prístupové údaje tretej strane, nezaznamenávať ich v ľahko rozpoznateľnej podobe a neukladať ich ani nenosiť so zariadením, nedovoliť prehliadaču, aby si zapamätal jeho heslo, bezdôvodne nezadávať svoje citlivé údaje prostredníctvom internetu, neotvárať prílohy podozrivých e-mailov alebo súbory s neznámym obsahom, nereagovať najmä na podozrivé e-mailové správy, nereagovať na e-mailové správy, v ktorých sa požadujú heslá, kódy PIN, čísla kreditných kariet atď, neklikať na odkazy v takýchto správach a e-mailoch. Pravosť e-mailu odosielaného z KB si Držiteľ Certifikátu môže overiť podľa Pravidiel pre odosielanie elektronickej komunikácie, ktoré nájde v Desatore bezpečnosti. Držiteľ Certifikátu je tiež povinný chrániť svoje zariadenie, ktoré používa pre priame bankovníctvo alebo na ktorom má aktivovanú metódu na vytvorenie Elektronického podpisu, pred zneužitím treťou osobou, používať na prihlásenie do priameho bankovníctva len svoj počítač alebo mobilný telefón, odmietnuť požiadavku a bezodkladne kontaktovať Banku, ak dostane požiadavku na prihlásenie alebo transakciu, ktorú nezadal, sledovať históriu prihlásení do svojho priameho bankovníctva a pravidelne kontrolovať históriu transakcií.

**5.6** **Strata čipovej karty**. Pokiaľ dôjde k strate čipovej karty s uloženým osobným certifikátom, alebo strate bezpečnostných prvkov k čipovej karte, je Držiteľ Certifikátu povinný Banku o tejto skutočnosti bezodkladne informovať na vyššie uvedenom telefónnom čísle a požiadať o zablokovanie osobného certifikátu.

**5.7** Banka je oprávnená dočasne neposkytovať Službu, ak to bude potrebné zo závažných, najmä bezpečnostných príčin. V prípadoch predvídaných zákonom o konkurze a reštrukturalizácii [3] je Banka oprávnená zablokovať prístup k Službe či pozastaviť poskytovanie Služby.

**5.8** Stratu, odcudzenie alebo zistenie rizika akéhokoľvek zneužitia Certifikátu (hesla, PIN a PUK) je Držiteľ Certifikátu povinný Banke bezodkladne oznámiť a požiadať o zablokovanie príslušnej metódy.

## Všeobecné ustanovenia

**5.8** Informačné povinnosti podľa týchto Podmienok plní Držiteľ Certifikátu voči Banke prostredníctvom Klientovho obchodného miesta, elektronicky na adresu uvedenú v príslušných Produktových podmienkach alebo prostredníctvom vyššie uvedeného telefónneho čísla. Pokiaľ Držiteľ Certifikátu nesplní svoju informačnú povinnosť voči Banke do 3 Obchodných dní odo dňa, kedy Držiteľovi Certifikátu táto povinnosť vznikla, bez toho aby v tom Držiteľovi Certifikátu bránili dôvody hodné zvláštneho zreteľa, platí, že Držiteľ Certifikátu neoznámil výše uvedenú skutočnosť bez zbytočného odkladu.

**5.9** Siete elektronických komunikácii (verejné telefónne linky, linky mobilných sietí, e-mail a fax) slúžiace na vzájomnú komunikáciu medzi Bankou a Držiteľom Certifikátu podľa Podmienok nie sú pod priamou kontrolou Banky a taktiež Banka nezodpovedá za škodu spôsobenú Držiteľovi Certifikátu ich prípadným zneužitím. Držiteľ Certifikátu berie na vedomie, že ochranu týchto sietí a dôvernosť nimi zasielaných správ sú povinní zabezpečovať príslušní poskytovatelia služieb elektronických komunikácii, najmä v zmysle zákona č. 610/2003 Z. z. o elektronických komunikáciách v znení neskorších predpisov.

3 zákon č. 7/2005 Z. z. o konkurze a reštrukturalizácii v znení neskorších predpisov

**5.10** Banka nezodpovedá za neautorizované nebo nesprávne vykonané platobné transakcie, ani za škodu, ktorá Držiteľovi Certifikátu vznikla v dôsledku porušenia jeho povinností stanovených v Podmienkach, ani za škody vzniknuté v dôsledku chybnej autorizácie, nevykonaní Príkazu z dôvodu na strane Držiteľa Certifikátu alebo z dôvodu na strane príjemcu platby. Banka nezodpovedá za zneužitie Certifikátu, ku ktorému došlo v dôsledku zneužitia počítača používaného Držiteľom Certifikátu (napr. programom iného výrobcu, zavírovaním počítača, hardwarovou vadou a pod.).

**5.11** Banka nezodpovedá za prípady, kedy Certifikát nie je možné využiť z dôvodov mimo kontrolu Banky alebo mimo kontrolu partnerov Banky (najmä prerušenie dodávky elektrickej energie, prerušenie spojenia prostredníctvom verejnej telefónnej siete, prerušenie spojenia prostredníctvom verejnej siete Internet, štrajk, atď.). Banka nie je povinná preukázať Držiteľovi Certifikátu, že bol dodržaný postup, ktorý umožňuje overiť, že bol daný platobný príkaz, že platobná transakcia bola autorizovaná, správne zaznamenaná, zaúčtovaná a že nebola ovplyvnená technickou poruchou alebo inou vadou.

**5.12** Držiteľ Certifikátu zodpovedá Banke za škodu, ktorá Banke vznikne porušením povinností Držiteľa Certifikátu uvedených v Podmienkach.

## Článok 6. Zánik zmluvného vzťahu

**6.1** Zmluva zaniká:

a) výpoveďou jednej zo zmluvných strán. Banka a Držiteľ Certifikátu sú oprávnení Zmluvu kedykoľvek písomne vypovedať bez uvedenia dôvodu. Výpoveď voči Banke je účinná nasledujúci Obchodný deň po dni, v ktorom bola doručená Banke. Výpoveď voči Držiteľovi Certifikátu je účinná posledným dňom mesiaca nasledujúceho po mesiaci, v ktorom bola doručená Držiteľovi Certifikátu.

b) Rozhodným dňom.

c) Pôvodná Zmluva o vydaní a používaní osobného certifikátu zaniká automaticky s ukončením platnosti Certifikátu.

**6.2** Právo Banky odstúpiť od Zmluvy za podmienok uvedených vo VOP nie je dotknuté.

**6.3** Po zániku Zmluvy Držiteľ Certifikátu nesmie Certifikát ďalej používať.

## Článok 7. Vymedzenie pojmov

**7.1** Pojmy s veľkým začiatočným písmenom majú v Podmienkach nasledujúci význam:

„**Banka**“ je Komerční banka, a.s., so sídlom Praha 1, Na Příkopě 33, čp. 969, PSČ 114 07, Česká republika, IČO: 45317054, zapísaná v Obchodnom registri vedenom Mestským súdom v Prahe, oddiel B, vložka 1360, konajúca prostredníctvom organizačnej zložky Komerční banka, a.s., pobočka zahraničnej banky so sídlom Hodžovo nám. 1A, PSČ 811 06, Bratislava, zapísaná v Obchodnom registri vedenom Mestským súdom Bratislava III, oddiel: Po, vložka č. 1914/B.

„**Bankové služby**“ sú akékoľvek bankové obchody, služby a produkty, ktoré je Banka oprávnená poskytovať v súlade s platnými právnymi predpismi.

„**Certifikačná politika**“ je dokument, v ktorom Banka stanoví pravidlá a postupy používania Certifikátu a jeho špecifikáciu, a ktorý je Banka oprávnená meniť. Certifikačnú politiku Banka zverejňuje na webových stránkach Banky. Certifikačná politika je k dispozícii taktiež v Klientovom obchodnom mieste. Tento dokument nie je Oznámením v zmysle VOP.

„**Certifikát**“ je metóda na vytvorenie Elektronického podpisu vo forme osobného certifikátu umožňujúca overiť autentizáciu podpisujúcej osoby. Obsahuje Verejný kľúč, Súkromný kľúč a identifikačné údaje Držiteľa Certifikátu.

„**Desatoro bezpečnosti**“ je dokument Desatoro bezpečnosti pre používanie priameho bankovníctva, v ktorom sú uvedené základné zásady bezpečného používania priameho bankovníctva a ktorý je Banka oprávnená meniť. Desatoro bezpečnosti Banka zverejňuje na svojich webových stránkach a je tiež k dispozícii v Klientovom obchodnom mieste. Tento dokument nie je Oznámením v zmysle VOP.

„**eIDAS**“ je Nariadenie európskeho parlamentu a rady (EU) č. 910/2014, o elektronickej identifikácii a službách vytvárajúcich dôveru v elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES, ktoré upravuje najmä elektronické podpisy a elektronickú identitu.

„**Elektronický podpis**“ je zaručený elektronický podpis v zmysle Nariadenia európskeho parlamentu a rady (EU) č. 910/2014, o elektronickej identifikácii a službách vytvárajúcich dôveru v elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES, založený na metódach, ktoré Banka poskytuje na základe Zmluvy.

„**Držiteľ Certifikátu**“ je osoba, ktorá uzatvorila s Bankou Zmluvu a ktorá pri uzatváraní a plnení Zmluvy koná v rámci pracovnoprávneho vzťahu existujúceho medzi ňou a ktorýmkoľvek Klientom ku dňu uzatvorenia Zmluvy alebo v rámci výkonu dohodnutej činnosti pre ktoréhokoľvek Klienta na základe zmluvy uzatvorenej medzi ňou a týmto Klientom, a to ako Splnomocnená osoba alebo Štatutárny orgán.

„**Klient**“ je osoba, ktorá uzatvorila s Bankou zmluvu o poskytnutí príslušnej Bankovej služby a v mene ktorej je pri poskytovaní Bankovej služby oprávnený konať Držiteľ Certifikátu ako Splnomocnená osoba alebo Štatutárny orgán v rozsahu v zmysle Príkazu k administrácii.

„**Klientovo obchodné miesto**“ je obchodné miesto Banky nachádzajúce sa v sídle Banky alebo iné obchodné miesto Banky pokiaľ je zriadené.

„**MôjProfil**“ je portál pre podporu a správu metód na vytvorenie Elektronických podpisov. MôjProfil je Držiteľovi Certifikátu prístupný na webových stránkach Banky, kam sa prihlasuje pomocou metódy na vytvorenie elektronického podpisu, prípadne priamo zo Služby PB.

„**Obchodný deň**“ je deň, ktorý nepripadá na sobotu, nedeľu, štátny sviatok ani ostatné dni pracovného pokoja v znení príslušných právnych predpisov a v ktorý je Banka otvorená pre poskytovanie Bankových služieb a zároveň sú pre poskytovanie platobných služieb otvorené iné inštitúcie, ktoré sa zúčastňujú poskytnutia Bankových služieb alebo na ktorých je poskytnutie Bankovej služby závislé. Za Obchodný deň sa nepovažuje deň, ktorý Banka vyhlási za neobchodný z dôvodu osobitne závažných prevádzkových dôvodov.

„**Oznámenia**“ sú oznamy, v ktorých sú v súlade so Všeobecnými podmienkami alebo príslušnými Produktovými podmienkami stanovené ďalšie podmienky a technické aspekty poskytovania Bankových služieb. Oznámením nie je najmä Certifikačná politika a Desatoro bezpečnosti.

„**PIN pro Čipovou kartu**“ je osobné štvormiestne číselné identifikačné číslo slúžiace na overenie oprávnenosti nakladať s čipovou kartou.

„**Platobné služby**“ sú Bankové služby, ktoré sú platobnými službami v zmysle zákona o platobných službách (napr. prevody peňažných prostriedkov alebo vydávanie platobných prostriedkov).

„**Pôvodná Zmluva o vydaní a používaní osobného certifikátu**“ je zmluva, ktorou sa Banka zaväzuje Klientovi vydať Osobný certifikát uzatvorená podľa Podmienok pre vydanie a používanie osobného certifikátu.

„**Produktové podmienky**“ sú podmienky Banky upravujúce poskytovanie jednotlivých Bankových služieb.

„**Príkaz k administrácii**“ je plná moc, ktorou Klient splnomocňuje Držiteľa Certifikátu na využívanie príslušnej Služby PB v rozsahu stanovenom v Príkaze k administrácii.

„**PUK**“ je osemmiestny číselný kód slúžiaci k odblokovaniu čipovej karty.

"**QSCD**" (Qualified Signature Creation Device) je typ hardvérového zariadenia, ktoré spĺňa špecifické technické požiadavky, bolo certifikované kvalifikovaným poskytovateľom dôveryhodných služieb a používa sa na vytváranie kvalifikovaných elektronických podpisov v zmysle nariadenia eIDAS.

„**Rozhodný deň**“ je (i) deň, kedy sa Banka hodnoverným spôsobom dozvie o úmrtí Držiteľa Certifikátu, t.j. deň, kedy sa Klientovmu obchodnému miestu doručia preukazné doklady o skutočnosti, že Držiteľ Certifikátu zomrel alebo bol vyhlásený za mŕtveho (najmä úmrtný list, potvrdenie súdu alebo notára vykonávajúceho dedičské konanie, rozhodnutie súdu s doložkou právoplatnosti o vyhlásení Držiteľa Certifikátu za mŕtveho) alebo (ii) najskôr deň, kedy dôjde k zrušeniu všetkých oprávnení a prístupov Držiteľa Certifikátu ako Splnomocnenej osoby alebo Štatutárneho orgánu v zmysle Príkazu k administrácii príslušného Klienta, za predpokladu, že zanikli všetky oprávnenia a prístupy Držiteľa Certifikátu ako Splnomocnenej osoby alebo Štatutárneho orgánu vo vzťahu k akémukoľvek Klientovi.

„**Sadzobník**“ je prehľad všetkých poplatkov, ostatných cien a iných platieb za Bankové služby a za úkony s Bankovými službami súvisiacimi.

„**Služba PB**“ je služba priameho bankovníctva Profibanka, ktorú Klient využíva na základe zmluvy o poskytovaní a využívaní priameho bankovníctva.

„**Služba**“ je akákoľvek Banková služba pre Klienta, pre ktorú sa používa Certifikát.

„**Zmluva**“ je zmluva, ktorou sa Banka zaväzuje Držiteľovi Certifikátu vydať Certifikát ako metódu na vytvorenie Elektronického podpisu.

„**Súkromný kľúč**“ sú dáta na vytváranie Elektronického podpisu Držiteľa Certifikátu vo forme Certifikátu.

„**Splnomocnená osoba**“ je fyzická osoba, okrem Štatutárneho orgánu, ktorá je Držiteľom Certifikátu, oprávnená využívať Službu PB v rozsahu stanovenom v Príkaze k administrácii.

„**Štatutárny orgán**“ je, bez ohľadu na spôsob konania menom Klienta – právnickej osoby navonok, fyzická osoba – štatutárny orgán právnickej osoby, člen štatutárneho orgánu právnickej osoby, alebo iná fyzická osoba, v obdobnom postavení ako štatutárny orgán právnickej osoby, ktorej bolo Klientom udelené v Príkaze k administrácii oprávnenie, aby využívala Službu PB.

„**Technické podmienky**“ je dokument, v ktorom Banka stanoví technické podmienky pre poskytovanie služieb priameho bankovníctva. Technické podmienky Banka zverejňuje na svojich internetových stránkach. Technické podmienky je Banka oprávnená meniť. Technické podmienky nie sú Oznámením v zmysle VOP.

„**Verejný kľúč**“ sú dáta na overenie Elektronického podpisu Držiteľa Certifikátu vo forme Certifikátu.

„**VOP**“ sú Všeobecné obchodné podmienky Banky.

**7.2** Odkazy na webové stránky Banky sú odkazy na adresu www.kb.sk, prípadne na iné webové adresy, ktoré Banka používa alebo bude používať v súvislosti s poskytovaním Bankových služieb.

## Článok 8. Záverečné ustanovenia

**8.1** Tam, kde je v zmluvách a ďalších dokumentoch dohodnutých medzi Bankou a Klientom, či zmluvných dokumentoch, ktoré tvoria neoddeliteľnú súčasť takýchto zmlúv, uvedený odkaz na pojem Podmienky pre vydanie a používanie osobného certifikátu, rozumejú sa tým Podmienky k elektronickému podpisu.

**8.2** Podmienky je Banka oprávnená priebežne meniť spôsobom uvedeným vo VOP.

**8.3** Podmienky nadobúdajú účinnosť dňa 1. 7. 2024. Tieto Podmienky súčasne rušia a nahrádzajú Podmienky pre vydanie a používanie osobného certifikátu vydávané Bankou a viazané na Zmluvu o vydaní a používaní osobného certifikátu účinné od 19. 5. 2019.

# TERMS AND CONDITIONS APPLYING TO THE ELECTRONIC SIGNATURE

The below Terms and Conditions Applying to the Electronic Signature (hereinafter the "**Conditions**") represent Product conditions in terms of the General Terms and Conditions of the Bank (hereinafter the "**General Conditions**"). The Conditions form part of the Contract and the Certificate Holder is obliged to familiarise himself/herself with them and to comply with them.

Capitalised terms used herein shall have the meaning as defined in Article 7 hereof.

## Article 1. Electronic Signature Creation Methods

**1.1** The Certificate Holder may use his/her Electronic Signature based on the method described as "the certificate stored on a chip card (smart card)" when utilizing selected Banking Services, in particular direct banking services. The aforementioned method may be used both for the authentication of the Certificate Holder and for the Electronic Signature as such.

**1.2** Only the Certificate Holder shall be entitled to use the Electronic Signature creation method provided under the Contract.

**1.3** The Bank shall be entitled to charge to the Certificate Holder a fee as per the Tariff of Fees for the provision and use of the method and related services.

**1.4** The Contract shall be governed by the law of the Slovak Republic, in particular by the Commercial Code[4].

**1.5** By signing the Contract, the Certificate Holder confirm that he/she has familiarised himself/herself with the contents and meaning of the Certification Policy and the Decalogue of the Security, and he/she shall abide by their provisions and adhere to the principles contained therein.

**1.6** Technical information concerning the Certificate is available in the Technical Terms and Conditions.

## Article 2. Certificates

**2.1** The Bank may only issue the Certificate in the form of a Certificate stored on a chip card (smart card).

**2.2** **Form of the Certificate.** The certificate (both commercial and qualified) shall be stored on a chip card the Bank shall provide the Certificate Holder with. The Certificate Holder may arrange the chip card in a standard mode or in a QSCD mode. Upon receipt of the chip card containing the Certificate, the Certificate Holder shall be obliged to check and verify the details contained in the Certificate, in particular his/her identification details (i.e., his/her name, type of the Certificate, email address, country of residence or domicile, and the chip card number). The Bank shall not be liable in the event that any incorrect or incomplete information is still contained in the Certificate after Certificate Holder's confirmation.

**2.3** **Type of the Certificate**. The Certificate Holder may choose a commercial or qualified Certificate when entering into the Contract. If he/she chooses a qualified Certificate, a commercial Certificate shall be provided to him/her and stored on his/her chip card as well.

**2.4** **Commercial Certificate**. The Certificate Holder may create an electronic signature based on the Commercial Certificate, which is a guaranteed electronic signature within the meaning of the eIDAS Regulation.

**2.5** **Qualified Certificate**. Depending on the mode of the chip card, the Qualified Certificate can be used to create an electronic signature within the meaning of the Trust Services Act[5], in the form of a qualified electronic signature. Only a Qualified Certificate on a chip card in QSCD mode can be used to create a Qualified Electronic Signature within the meaning of the eIDAS Regulation. A qualified certificate cannot be used for authentication.

## Certificate Stored on a Chip Card (Smart Card)

4 Act No. 5131991 Coll. – the Commercial Code, as amended.

5 Act No. 272/2016 Coll. on trust services for electronic transactions in the internal market and on amendment and supplementation of certain acts (Act on trust services)

**2.6** **Activation**. Upon entering into the Contract and in cooperation with the Certificate Holder, the Bank shall send the Certificate Holder a one-time password to the agreed GSM mobile telephone number so that he/she can create the Certificate at MůjProfil portal, or the Bank shall create the Certificate, including the generation a Private and Public Keys, and store it on a chip card (smart card). The one-time password shall remain effective for a period of 3 days from being sent. At the same time, the Bank shall deliver to the Certificate Holder the chip card and an envelope containing the PIN and PUK Codes.

The mobile telephone number indicated by the Certificate Holder in the Contract as that to which the SMS messages should be delivered must be identical to that specified by the Client in the Authorisation Order with respect to the specific Certificate Holder and must not be used for the same purpose by another Certificate Holder as long as the given Certificate is valid. The Bank shall not be held liable for any damage caused by the fact that the Certificate Holder might have stated a wrong mobile telephone number to which the Bank should deliver the SMS messages.

## Article 3. Validity of the Certificate

**3.1** **Validity of the Certificate.** The Certificate shall be valid for 2 years, unless the Conclusive Date occurs or the Contract is terminated in the meantime. The term of validity of a specific Certificate is specified in the Certificate itself or can be determined at MůjProfil portal. The Certificate Holder may use a valid and effective Certificate while utilising the Services. The Certificate Holder also may ask for the renewal of the Certificate via MůjProfil portal before its expiry

**3.2** If the Certificate Holder asks for the renewal of the Certificate before its expiry, the Bank shall issue him/her with a new Certificate under the existing Contract, unless the Conclusive Date occurs or the Contract is terminated before the date of the submission by the Certificate Holder of the request for the renewal of the Certificate. The Bank shall issue the new Certificate in the same form and with the same identification data as the previous one. As of the moment of issue of the new Certificate, the Certificate Holder shall not be allowed to use the previous one any longer. The procedure described in Article 2 hereof shall accordingly apply to the issue of a new Certificate.

**3.3** If the identification data of the Certificate Holder stated in the Contract (including the mobile telephone number to which the SMS Messages are to be sent) should change, the Certificate Holder shall be obliged to notify the bank of this fact without any unnecessary delay in writing and to execute an amendment to the Contract with the Bank, or to apply for the issue of a new Certificate. If the electronic address of the Certificate Holder stated in the Contract should change, the Certificate Holder shall be obliged to notify the Bank in writing at the Client's Point of Sale. The Bank shall not be obliged to accept any change to the mobile telephone number to which the SMS Messages are to be sent or to the agreed-upon electronic address, if the new number/address are not identical to those specified by the Client in the Authorisation Order with respect to the specific Certificate Holder whose identification data should be changed.

## Article 4. Blocking and Deactivating the Certificate

**4.1** **Blocking and Deactivating**. If the Certificate is blocked, its validity shall be suspended until the Certificate Holder asks the Bank to reactivate it. If the Certificate is deactivated, it is completely terminated. If the Certificate Holder wishes to use it again, it must be reactivated. The Certificate Holder shall be informed about the method of blocking on the contact telephone number specified in the Contract.

**4.2** **Blocking by the Bank**. The Bank is entitled to block the Certificate for the time strictly necessary if it is necessary for serious reasons, in particular for security reasons (e.g. in the case of suspected unauthorised or fraudulent use or in the case of a tampered operating system). Once the reasons for blocking the Certificate have passed, the Bank, in cooperation with the Certificate Holder, shall allow the Certificate to be unblocked or replaced with another Certificate.

**4.3** **Blocking by the Certificate Holder**. The Certificate Holder may request the method blocking at any time on the telephone number +420 955 551 552, at any of the Bank's points of sale or at MůjProfil portal on the Bank's website. The Certificate Holder shall be obliged to request the method blocking any time he/she suspects that the method might have been misused.

**4.4** **Deactivating by the Bank.** The Bank shall block the Certificate and possibly also demand that the Certificate Holder apply for the reactivation of the Certificate if at least one of the following events occurs:

- The method has been arranged on the basis of false, incomplete or misleading information,
- The identification data that form part of the method is no longer valid,
- The Certificate Holder is in breach of any of his/her duties under the Contract,
- The mobile telephone number to which the Bank should send the one-time password and SMS Messages has been used in several Contracts and/or for several Clients,
- The Bank ceases to provide the given method,
- The Bank is required to do so by law,
- Security risks have increased or might increase, or measures relating to the erroneous inputting of security data or the use of the method have become stricter.

**4.5** **Deactivating by the Certificate Holder.** The Certificate Holder may request the deactivation of the Certificate at the Bank's point of sale or on the Bank's website via the MôjProfil portal.

**4.6** For Certificates stored on a chip card (smart card), the chip card shall be blocked after the third incorrect PIN entry. The Certificate Holder may ask for the chip card to be unblocked at the Client's Point of Sale or can do it by himself/herself using the KB Cryptoplus application. In both cases, the Certificate Holder must enter the PUK Code to unblock the chip card.

**4.7** **Unblocking the Certificate**. In the case of a blocked Certificate, the Certificate Holder may request its unblocking through the Bank's point of sale or the MôjProfil portal, under the terms and conditions set by the Bank. The Bank reserves the right to change the methods of unblocking the Certificate and its subsequent use, especially depending on its technical capabilities or changes in legislation.

## Article 5. Security

**5.1** **Security Prior to Activating the Method – loss or theft**. If the mobile telephone to which the one-time password should be sent is lost or stolen or the e-mail address to which the one-time password should be sent is misused or blocked before you create the Certificate, or the mobile telephone to which the one-time password should be sent is lost or stolen prior to activating the method, the Certificate Holder shall be obliged to notify the Bank without any unnecessary delay to the telephone number **+420 955 551 552** and agree upon an alternative method of the delivery of a new one-time password. The Bank shall subsequently invalidate the old password. The Bank can deliver the one-time password at the electronic address of the Certificate Holder, if such an address is stated in the Contract, in the case of the Certificate.

**5.2** **Certificate.** The Certificate Holder shall be fully responsible for the process of the creation of the Certificate, including the generation of a Public and Private Key on the PC that the Certificate Holder has used for this purpose. Being the sole user of the Certificate including the Private Key, the Certificate Holder shall be liable for their use.

**5.3** A Private Key stored in a data file is protected by a password. A Private Key stored on a chip card is protected by a PIN Code.

**5.4** The Certificate Holder shall be obliged to protect his/her Private Key, the password and, as the case may be, the PIN and PUK Codes, to be used with the Private Key throughout the entire term of the validity of the Certificate, in particular from a possible loss, disclosure to a third party, alteration, or unauthorised use. The password or the PIN and PUK Codes to be used with the Private Key must not be stored in the same place or on the same media as the Private Key and may never be stored in any manner that would make them accessible to third parties. In particular, the Certificate Holder must not leave an unsecured Private Key in the PC with a password entered and the key activated, or leave the chip card inserted in the chip card reader outside the time when he/she is logging into a given Banking Service or is using the Electronic Signature. The Certificate Holder must continuously make sure that the Certificate has not been lost, stolen, misused or used without authorisation.

**5.5** **Other obligations to ensure the security of the Certificate Holder's equipment**. When using his/her device, the Certificate Holder has the following obligations: use and update anti-virus software, use an updated operating system and an updated web browser, visit only known sites, not to download or install programmes from untrusted sources, not to use a mobile device with modified settings (e.g. jailbreak or root), use a trusted and properly secured device, download only applications from official sources (e.g. Google Play, Apple Store, Windows Phone Store), use a password that is not simple and cannot be derived from personal data, keep the device under control at all times, not to provide access data to a third party, not to record it in an easily recognizable form and not to store or carry it with the device, not allowing the browser to remember his/her password, not entering sensitive data over the Internet without any reason, not opening attachments of suspicious emails or files with unknown content, not responding to suspicious email messages in particular, not to respond to e-mail messages requesting passwords, PIN codes, credit card numbers, etc., and not to click on links in such messages and e-mails. The Certificate Holder can verify the authenticity of the e-mail sent from the KB according to the Rules for sending electronic communications, which can be found in the Decalogue of the Safe Internet Banking. The Certificate Holder is also obliged to protect his/her device used for Direct Banking or on which he/she has activated the method for creating an Electronic Signature from misuse by a third party, to use only his/her computer or mobile phone to log in to Direct Banking, to refuse a request and to contact the Bank immediately if he/she receives a request to log in or a transaction he/she did not enter, to keep track of his/her Direct Banking login history and to regularly check the transaction history.

**5.6** **Loss of the chip card (smart card).** If the chip card (smart card) on which the personal certificate is stored is lost, or if the chip card security features are lost, the Certificate Holder shall be obliged to notify the Bank without any unnecessary delay to the above telephone number and apply for blocking the personal certificate.

**5.7** The Bank shall be entitled to suspend the Service temporarily for serious reasons, particularly those of a security nature. In cases as stipulated in the Act on Bankruptcy and Restructuring,[6] the Bank shall be entitled to block access to the Service or suspend the provision of the Service.

**5.8** The Certificate Holder shall be obliged to notify the Bank without any unnecessary delay of the loss, theft or any ascertained risk of threatened misuse of the Certificate (the password, PIN and PUK Codes) and request the blocking of the specific method.

## General Provisions

**5.8** The Certificate Holder shall discharge his/her duty to inform the Bank pursuant to these Conditions at the Client's Point of Sale, by e-mail delivered at the address indicated in the relevant Product Terms and Conditions, or over the telephone to the above telephone number. If the Certificate Holder fails to fulfil the duty to inform the Bank within 3 Business Days from the day on which such duty has arisen without being prevented from doing so by particularly serious reasons, the Certificate Holder shall be deemed to have failed to notify without any unnecessary delay.

**5.9** Electronic communications networks (public telephone lines, mobile network lines, e-mail and fax) used for mutual communication between the Bank and the Certificate Holder pursuant to these Conditions are beyond the direct control of the Bank; therefore the Bank is not liable for any damage caused to the Certificate Holder by their potential misuse. The Certificate Holder acknowledges that the relevant providers of electronic communications services are obliged to secure the protection of these networks and the confidentiality of messages sent via the networks, as envisaged particularly in Act No. 610/2003 Coll., on Electronic Communications, as amended.

6 Act No. 7/2005 Coll. on Bankruptcy and Restructuring, as amended.

**5.10** The Bank shall not be held liable for any unauthorised or erroneously performed payment transactions, for any damage incurred by the Certificate Holder as a result of a breach of his/her duties set forth herein, or for any loss or damage resulting from an incorrect authorisation or non-execution of an Order due to reasons caused by the Certificate Holder or a payee. The bank shall neither be held liable for any misuse of the Certificate resulting from misuse of a PC used by the Certificate Holder (e.g. caused by software supplied by another supplier, a virus infected PC, hardware fault etc.).

**5.11** The Bank shall not be held liable for cases where the Certificate cannot be used due to circumstances that are beyond the Bank's control and/or beyond the control of the Bank's partners (in particular a power failure, interruption to the connection with the Bank via a public telephone/Internet network, strike, etc.). The Bank shall not be obliged to demonstrate to the Certificate Holder that it has followed the procedure that makes it possible to verify that an Order has been submitted, a particular payment transaction has been authorised, correctly documented and entered in the books, and it has not been affected by technical problems or other flaws.

**5.12** The Bank shall hold the Certificate Holder liable for any damage it may suffer in case the Certificate Holder breaches his/her duties set forth herein.

## Article 6. Termination of the Contractual Relationship

**6.1** The Contract shall expire/be terminated:

d) By a notice of termination served by either of the contracting parties. Both the Bank and the Certificate Holder shall be entitled to terminate the Contract in writing at any time without giving a reason. The notice of termination served to the Bank shall become effective on the next succeeding Business Day following the day of receipt of the notice. The notice of termination served to the Certificate Holder shall become effective on the last day of the month following the month in which he/she receives the notice.

e) As at the Conclusive Date.

f) The Initial Contract for the Issue and Use of a Personal Certificate shall expire automatically upon the expiry of the Certificate.

**6.2** The Bank's right to cancel the Contract in accordance with the General Conditions shall not be prejudiced by this provision.

**6.3** The Certificate Holder shall not be allowed to use the Certificate after the expiry/termination of the Contract.

## Article 7. Definition of Terms

**7.1** Capitalised terms used herein shall have the following meaning:

"**Administration Order**" shall mean a power of attorney by which the Client authorises the Certificate Holder to use a particular DB Service to the extent set forth in the Administration Order.

"**Bank**" shall be Komerční banka, a.s., registered office at Praha 1, Na Příkopě 33/969, Postal Code: 114 07, Czech Republic, IČO (Company ID): 45317054, entered into the Commercial Register kept by the Municipal Court in Prague, Section B, Insert 1360, acting through its organisational unit Komerční banka, a.s., pobočka zahraničnej banky (a foreign bank branch), registered office at Hodžovo námestie 1A, Postal Code: 811 06, Bratislava, IČO (Company ID): 47 231 564, Slovak Republic, entered into the Commercial Register kept by the Municipal Court Bratislava III, Section: Po, Insert No. 1914/B.

"**Banking Services**" shall mean any banking deals, services and products the Bank is entitled to deliver pursuant to applicable law.

"**Business Day**" shall mean a day that does not fall on a Saturday, a Sunday, a public holiday or other holidays within the meaning of the applicable law, on which the Bank is open for the provision of Banking Services and on which other institutions that take part in the provision of Banking Services, or on which the provision of the Banking Services depends, are open and provide the relevant services. A day declared as a non-business day by the Bank due to particularly serious operational reasons shall not be considered a Business Day.

"**Certificate**" shall mean an Electronic Signature creation method consisting in creating a personal certificate that makes it possible to authenticate a signatory. It contains the Public Key, Private Key and Certificate Holder's identification data.

# TERMS AND CONDITIONS APPLYING TO THE ELECTRONIC SIGNATURE

"**Certificate Holder**" shall mean a person who has entered into the Contract with the Bank and who, while entering and discharging the Contract, acts under an employment relationship existing between him/her and the Client as at the date of execution of the Contract, or while performing mutually agreed activities for any of the Clients pursuant to a mutual agreement, either as a Plenipotentiary or as a Statutory Body.

"**Certification Policy**" shall mean a document in which the Bank sets forth the rules and procedures for using the Certificate and its specification, which the Bank is entitled to modify. The Bank publishes the Certification Policy on its website. The Certification Policy is also available at the Client's Point of Sale. This document is not a Notice as envisaged by the General Conditions.

"**Chip Card PIN**" shall mean a four-digit personal identification number used to verify the holder's authorisation to handle the chip card.

"**Client**" shall mean a person who has entered into the contract for the provision of a given Banking Service with the Bank and on whose behalf the Certificate Holder is entitled to act as a Plenipotentiary or a Statutory Body, within the scope and to the extent of the Administration Order, when the Banking Service is provided.

"**Client's Point of Sale**" shall mean the Bank's point of sale located at the Bank's registered address or another branch/point of sale, if it exists.

"**Conclusive Day**" shall be (i) a day on which the Bank learns, in a trustworthy manner, about the death of a Certificate Holder, i.e., a day on which conclusive documents attesting the fact that the Certificate Holder died or was declared dead are delivered to the Client's Point of Sale (these documents can be, e.g., a death certificate, a court or notary memorandum of performing the inheritance proceedings, decision of the court with a legal power clause concerning the declaration of the Certificate Holder's death, or (ii) a day not earlier than the date as of which all authorisations and access rights of the Certificate Holder as a Plenipotentiary or Statutory Body within the meaning of the Administration Order issued by a given Client shall have been cancelled, provided that all authorisations and access rights of the Certificate Holder as a Plenipotentiary or Statutory Body with respect to any Client shall have ceased to exist.

"**Contract**" shall mean a contract in which the Bank undertakes to issue the Certificate Holder with the Certificate as an Electronic Signature creation method.

"**DB Service**" is the *Profibanka* direct Banking Service the Client uses under the Contract for the Provision and Use of Direct Banking.

"**Decalogue of the Safe Internet Banking**" is a document in which basic principles of safe use of the Internet banking are defined, which the Bank is entitled to amend. The Bank has made The Decalogue of the Safe Internet Banking public on its website. It is also available at the Bank's points of sale. This document is not a Notice as envisaged in the General Conditions.

"**eIDAS**" shall mean the Regulation (EU) No. 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, regulating in particular electronic signatures and electronic identity.

"**Electronic Signature**" shall mean an advanced electronic signature within the meaning of the Regulation (EU) No. 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, based on the methods the Bank makes available under the Contract.

"**General Conditions**" shall mean the General Business Terms and Conditions issued by the Bank.

"**Initial Contract for the Issue and Use of a Personal Certificate**" shall mean the contract under which the Bank undertakes to issue the Client with the Personal Certificate entered into pursuant to the Terms and Conditions of the Issue and Use of a Personal Certificate.

"**MůjProfil**" shall mean a portal for the support and management of the Electronic Signature creation methods. Můj Profil is accessible to the Certificate Holder on the Bank's website, to which the Client may log in using any Electronic Signature creation method or directly from the DB Service.

"**Notices**" shall mean communications in which further conditions and technical features of providing the Banking Services are specified in accordance with the General Terms and Conditions or relevant Product conditions. The following documents, without limitation to them, are not Notices: The following documents, without limitation to them, are not Notices: the Certification Policy and the Decalogue of the Security.

"**Payment Services**" shall mean Banking Services falling within the scope of payment services as envisaged by the Payments Act (e.g., money transfers, issuing of payment instruments and cash deposits/withdrawals).

"**Plenipotentiary**" shall be a natural person other than a Statutory Body, who is the Certificate holder entitled to use the DB Service to the extent set forth in the Administration Order.

"**Private Key**" shall mean the data used for creating the Certificate Holder's electronic signature in the form of a Certificate.

"**Product Terms and Conditions**" shall mean the Bank's terms and conditions regulating the provision of separate Banking Services.

"**Public Key**" shall mean the data used for verifying the Certificate Holder's electronic signature in the form of a Certificate.

"**PUK Code**" shall mean an eight-digit code used to unblock the chip card.

"**QSCD**" (Qualified Signature Creation Device) is a type of hardware device that meets specific technical requirements, has been certified by a qualified trust service provider and is used to create qualified electronic signatures within the meaning of the eIDAS Regulation.

"**Service**" shall mean any Banking Service provided to the Client and utilizing the Certificate.

"**Statutory Body**" shall mean, notwithstanding the manner in which they act externally on behalf of the Client – legal person; a natural person – statutory body of the legal person; a member of a statutory body of the legal person; or another natural person in a position similar to that of a statutory body of a legal person authorised by the Client by an Administration Order to use the DB Service.

"**Tariff of Fees**" shall mean a list of all charges, other fees and payments for the Banking Services and operations associated with the Banking Services.

"**Technical Terms and Conditions**" shall mean a document in which the Bank sets technical terms of the provision of the direct banking services, which the Bank is entitled to amend. The Bank has made the Technical Terms and Conditions public on its Internet pages. The Technical Terms and Conditions are not a Notice as envisaged in the General Conditions.

**7.2** Any reference to the Bank's website shall mean a reference to www.kb.sk or other web addresses the Bank currently uses or shall use while providing the Banking Services.

# TERMS AND CONDITIONS APPLYING TO THE ELECTRONIC SIGNATURE

## Article 8. Final Provisions

**8.1** Wherever the contracts and other documents entered into by and between the Bank and the Client, or the contractual documents that are part of such contracts, refer to the Terms and Conditions of the Issue and Use of a Personal Certificate, this shall mean the Terms and Conditions Applying to the Electronic Signature.

**8.2** The Bank is entitled to amend these Conditions from time to time in the manner set forth in the General Conditions.

**8.3** These Conditions come into effect as of 1 July 2024. At the same time, these Conditions repeal and replace the Terms and Conditions of the Issue and Use of a Personal Certificate issued by the Bank and connected to the Contract for the Issue and Use of a Personal Certificate effective as from 19 May 2019.