

TECHNICKÉ PODMÍNKY

1. Tyto technické podmínky upravují provozní a technické podmínky Banky ve vztahu k jednotlivým Bankovním službám.
2. Pojmy s velkým počátečním písmenem definované v Obchodních podmínkách mají stejný význam i v těchto Technických podmínkách.

Podmínky pro využívání služeb Internetového bankovníctví:

Software a hardware:

Pro využívání služeb Banky prostřednictvím aplikace Internetového bankovníctví je třeba osobní počítač vybavený podporovaným operačním systémem a internetovým prohlížečem¹, jak jsou uvedeny níže.

Podporovaný operační systém	Podporovaný internetový prohlížeč
MS Windows XP a vyšší	Internet Explorer 6 a vyšší Firefox 2.0 a vyšší Google Chrome 1.0 a vyšší
MacOS X 10.4 (Tiger) a vyšší	Firefox 2.0 a vyšší Internet Explorer 5.0 a vyšší

Zabezpečení:

Přístup do aplikace Internetového bankovníctví je podmíněn správným zadáním Personalizovaných bezpečnostních prvků Klientem.

Personalizovanými bezpečnostními prvky v případě aplikace Internetového bankovníctví jsou:

- Uživatelské číslo Klienta (CIF);
- Heslo;
- Datum narození Klienta; a
- v případě platebních transakcí i Jednorázový autorizační kód zasílaný Klientovi ve formě SMS zprávy na číslo mobilního telefonu, které si Klient zvolil ke komunikaci s Bankou.

Uživatelské číslo Klienta (CIF) bude Klientovi sděleno písemně poštou po uzavření Smlouvy.

Při prvním přihlášení do aplikace Internetového bankovníctví bude Klientovi zasláno jednorázové heslo na číslo mobilního telefonu, které si Klient zvolil pro účely komunikace s Bankou. Klient je následně vyzván k zadání svého vlastního Hesla, které bude pro přihlášení do aplikace Internetového bankovníctví nadále používat. Heslo se musí skládat z minimálně osmi a maximálně patnácti alfanumerických a nealfanumerických znaků, v jejichž kombinaci nesmí být obsaženy více, než dva

¹ Banka nevylučuje, že služby Internetového bankovníctví budou funkční i za použití jiného operačního systému nebo internetového prohlížeče. Banka však neručí za plnou funkčnost Internetového bankovníctví v případě použití jiného operačního systému nebo internetového prohlížeče, než je podporovaný Bankou

stejně znaky anebo více než dva znaky po sobě následující. Heslo musí obsahovat alespoň jedno velké písmeno, jedno malé písmeno a jedno číslo.

V zájmu bezpečnosti se doporučuje, aby Klient Heslo nepoužíval mimo aplikaci Internetového bankovníctví a aby Heslo měnil nejméně 1x za 6 měsíců a kdykoliv pokud bude mít pochybnosti o tom, zda nemohlo dojít k prozrazení či zneužití jím zvoleného Hesla. Pokud Klient 5x opakovaně nesprávně zadá Heslo, přístup do Internetového bankovníctví bude blokován.

Aplikace Internetového bankovníctví se automaticky zablokuje rovněž v případě, že se Klient do této aplikace nepřihlásí po dobu delší než 12 měsíců. O provedení této blokace bude Klient informován v souladu s Obchodními nebo Produktovými podmínkami. O odblokování takto zablokovaného přístupu může Klient požádat prostřednictvím Kontaktní linky banky a za předpokladu identifikace Klienta prostřednictvím Personalizovaných bezpečnostních prvků či jiným pro Banku hodnověrným způsobem.

V případě, že Klient zapomene svoje heslo, přihlásí se na Internetových stránkách Banky: www.axa.cz a v sekci „Banka“ klikne na položku "Zapomněli jste heslo?". Následně bude Klientovi zasláno jednorázové heslo na číslo mobilního telefonu, které si Klient zvolil pro účely komunikace s Bankou a bude vyzván k zadání nového Hesla.

Informace o dalších bezpečnostních prvcích a preventivních postupech při používání Internetového bankovníctví jsou uvedeny na Internetových stránkách Banky.

Podmínky pro využívání služeb Telefonického bankovníctví:

Personalizovanými bezpečnostními prvky v případě Telefonického bankovníctví jsou:

- Číslo mobilního telefonu, které si Klient zvolil pro komunikaci s Bankou;
- Jméno a příjmení Klienta;
- Uživatelské číslo Klienta (CIF); a
- Číslo účtu Klienta.

Pokud však Klient bude ke komunikaci prostřednictvím Telefonického bankovníctví využívat jiného telefonního čísla než čísla mobilního telefonu zvoleného pro komunikaci s Bankou (či pokud toto číslo nebude při hovoru zobrazeno) bude mezi Personalizované bezpečnostními prvky Klienta patřit podle volby Banky ještě kterákoliv z následujících informací:

- Rodné číslo Klienta; nebo
- Číslo občanského průkazu Klienta; nebo
- Číslo cestovního pasu Klienta.

V případě změny čísla mobilního telefonu, které si Klient zvolil pro komunikaci s Bankou, předloží Klient Bance:

- i) u čísla mobilního telefonu, které je registrováno na jméno Klienta, kopii smlouvy s mobilním operátorem nebo kopii faktury (vyúčtování) vystavené mobilním operátorem za služby spojené s tímto číslem mobilního telefonu;

- ii) u čísla mobilního telefonu s předplacenou SIM kartou čestné prohlášení Klienta o změně takového čísla mobilního telefonu s úředně ověřeným podpisem Klienta nebo potvrzením Poradce o tom, že Klient žádá o takovou změnu;
- iii) u čísla mobilního telefonu, které je registrováno na zaměstnavatele Klienta (služební telefon) písemné potvrzení zaměstnavatele s podpisem statutárního zástupce zaměstnavatele, o tom, že je Klient oprávněn užívat toto číslo mobilního telefonu.

Veškeré transakce či změny Klientských dat a informací mohou být dále ověřovány formou zpětného volání na číslo mobilního telefonu, které si Klient zvolil ke komunikaci s Bankou.

Zpětné volání bude probíhat v rámci Doby dostupnosti Služby Telefonického bankovníctví, avšak s výjimkou transakcí, jejichž výše přesahuje částku 2.700.000,- Kč (slovy: dva miliony sedm set tisíc korun českých), kdy bude zpětné volání probíhat jen v rámci Provozní doby Banky.

V zájmu vlastní bezpečnosti doporučujeme Klientům uchovávat neveřejné informace sloužící jako Personalizované bezpečnostní prvky mimo dosah třetích osob a nahlásit Bance bezodkladně ztrátu mobilního telefonu, jehož číslo si Klient zvolil ke komunikaci s Bankou.

Tyto Technické podmínky jsou platné a účinné od 15. února 2011