Raiffeisen BANK

Banka inspirovaná klienty

Internetový Elektronický klíč

Uživatelská příručka

Internetový Elektronický klíč

Uživatelská příručka

Raiffeisenbank a. s.
Olbrachtova 2006/9, 140 21 Praha 4
IČ 49240901, zapsaná v obchodním rejstříku vedeném
Městským soudem v Praze, oddíl B, vložka 2051

Obsah

1 Úvod

Internetový Elektronický klíč je autentizační a certifikační prostředek určený pro pohodlnou a bezpečnou práci s vaším účtem v Raiffeisenbank prostřednictvím počítače. Lze jej používat výhradně při přístupu přes internet. Výhodou je rychlost a jednoduchost použití celého procesu elektronického podpisu.

1.1 Vymezení pojmů

Autentizace – jednoznačné ověření identity osoby vstupující do Klientského systému Raiffeisenbank.

Certifikace – proces potvrzení a ověření pravosti dispozice předávané Oprávněnou osobou. Certifikace umožňuje Raiffiesenbank ověřit jednak neporušenost a správnost obdržené dispozice a také totožnost osoby, která ji podepsala svým Elektronickým klíčem.

Certifikát – datová zpráva, která je vydána Certifikační autoritou, spojuje Veřejný klíč s podepisující osobou a umožňuje ověřit její identitu.

Certifikační autorita (zkráceně CA) – autorita, která vydává Certifikáty a vede jejich evidenci, případně poskytuje další služby spojené s elektronickými podpisy.

Elektronický podpis – údaje v elektronické podobě, které jsou připojeny k datové zprávě nebo jsou s ní logicky spojené a které umožňují ověření totožnosti podepsané osoby ve vztahu k datové zprávě.

Internetový Elektronický klíč (zkráceně IEk) – je autentizační a certifikační prostředek založený na technologii elektronických podpisů. Obsahuje Soukromý klíč, veřejné klíče a příslušné certifikáty umožňující ověřit podepisující osobu a platnost podpisu. Certifikáty jsou vydávány Certifikační autoritou Raiffeisenbank. Fyzickou podobu IEk představuje soubor s příponou *.key.

Osobní certifikát – certifikát vystavený CA Raiffeisenbank při registraci vašeho Veřejného klíče, který slouží jako důvěryhodná vazba mezi vaší identitou a vaším Veřejným klíčem. Osobní certifikát je platný 12 měsíců od data jeho vystavení, poté je nezbytné certifikát obnovit.

Soukromý klíč (data pro vytváření elektronického podpisu) – jedinečná data, která slouží k prokázání vaší identity při přihlášení k účtu a podepisování vašich požadavků. Soukromý klíč je vždy uložen výhradně v IEk a nelze jej exportovat. Tento klíč máte pouze vy a pro zajištění bezpečnosti vašeho účtu jej musíte chránit před vyzrazením dalším osobám.

Veřejný klíč (data pro ověřování elektronických podpisů) – jedinečná data, která slouží k ověření vámi podepsaných požadavků. Tento klíč je jednoznačně svázán s vaším Soukromým klíčem a je nezbytné jej před prvním použitím IEk pro autentizaci zaregistrovat v bance.

Zaručený elektronický podpis – elektronický podpis splňující následující požadavky:

- je jednoznačně spojen s podepisující osobou,
- umožňuje identifikaci podepisující osoby,
- byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou,
- je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat.

TIP

Neváhejte nás kontaktovat se svými dotazy a připomínkami :
a) pomocí svého bankéře / finančního poradce
b) na bezplatné lince **800 900 900**
c) e-mailem na **adrese info@rb.cz**

2 Obecně o IEk

2.1 Technické požadavky

Pro používání IEk musí být splněny určité technické požadavky zajišťující řádnou funkčnost celého procesu elektronického podpisu. IEk je testován na níže doporučeném programovém vybavení a hardwarové konfiguraci.

Doporučené programové vybavení:

- operační systém MS Windows NT 4.0, 2000 nebo XP,
- internetový prohlížeč Microsoft Internet Explorer 6.0 nebo 7.0, Netscape Browser 8.1, Mozilla Firefox 1.5 nebo 2.0,
- Java plug-in od společnosti SUN Microsystems, Inc. ve verzi J2RE Standard Edition 1.4.2_11 (Multilanguage).

TIP

- nestandardní chování může způsobit diakritika v uživatelském jménu pro přihlášení do systémů Windows
- prohlížeč musí mít povoleno používání Java Virtual Machine a ActiveX
- práci s IEk usnadní povolení cookies
- s OS WIN 98 se při použití MIE5 doporučuje verze J2RE SE 1.3...

Doporučená hardwarová konfigurace:

- PC nebo notebook s procesorem o frekvenci 400 MHz a rychlejší, 128 MB RAM, disketová mechanika 3,5".

Z důvodu velkého množství možných kombinací programového vybavení, na kterém lze IEk používat, obsahuje tento manuál detailní popis práce s IEk pouze v MS Windows XP a MS Internet Explorer 6.0.

2.1.1 Java plug-in

Bankovní aplikace pro práci s IEk je vytvořena v programovacím jazyce Java což vyžaduje na počítači, na kterém bude používána, instalaci tzv. Java plug-inu.
Po vstupu na úvodní stranu pro tvorbu a správu IEk aplikace automaticky detekuje přítomnost Java plug-inu. Pokud není nainstalován, začne se ze stránek Raiffeisenbank automaticky stahovat (pouze při použití Microsoft Internet Exploreru) a poté budete vyzváni k jeho instalaci.

2.1.2 Vytvoření nového IEk

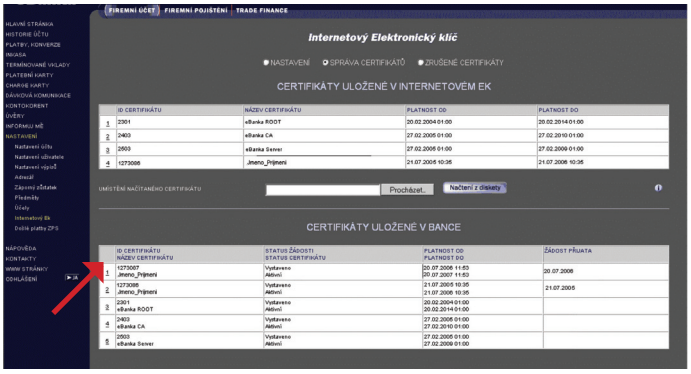
Nový IEk není možné od 20. 7. 2008 vytvořit – nelze zaregistrovat nový certifikát.
Pokud IEk používáte a vyprší platnost Vašeho certifikátu, můžete si na svém účtu v Klientském systému Raiffeisenbank požádat o obnovu certifikátu – viz Kapitola 3.

3 Správa IEk

3.1 Obnova Osobního certifikátu

Registrace vašeho Veřejného klíče je platná 12 měsíců od data jeho vystavení. Měsíc před ukončením platnosti Osobního certifikátu je připraven nový. Obnovu Osobního certifikátu provedete na svém účtu podle následujícího postupu, ke kterému budete před ukončením platnosti dosavadního certifikátu vyzváni e-mailovou zprávou.

- Na vašem účtu v Klientském systému zvolte Nastavení - Internetový Ek.
- Nastavte cestu k vašemu IEk (není-li přednastavena), stiskněte tlačítko OK, zadejte heslo pro přihlášení do IEk a znovu stiskněte tlačítko OK.
- Nový certifikát naleznete v IEk v záložce SPRÁVA CERTIFIKÁTŮ – v části obrazovky CERTIFIKÁTY ULOŽENÉ V BANCE.



Obrázek 1

- Zkontrolujte i aktuálnost certifikátů banky (především CA).
- Vyberte postupně všechny (novější oproti horní části obrazovky – poznáte podle platnosti certifikátu) kliknutím na pořadové číslo (Obrázek 1).
- V detailu certifikátu stiskněte tlačítko Uložit do IEk, zadejte heslo a stiskněte tlačítko OK. Následně dojde k vyzvednutí a přenesení aktuálního certifikátu z Raiffeisenbank do vašeho IEk (do souboru *.key).
- Váš nový Osobní certifikát vložte jako poslední. Znovu zkontrolujte v horní části obrazovky pořadí:
  1. eBanka ROOT
  2. eBanka CA
  3. eBanka SERVER
  4. Jméno Příjmení (váš Osobní certifikát)

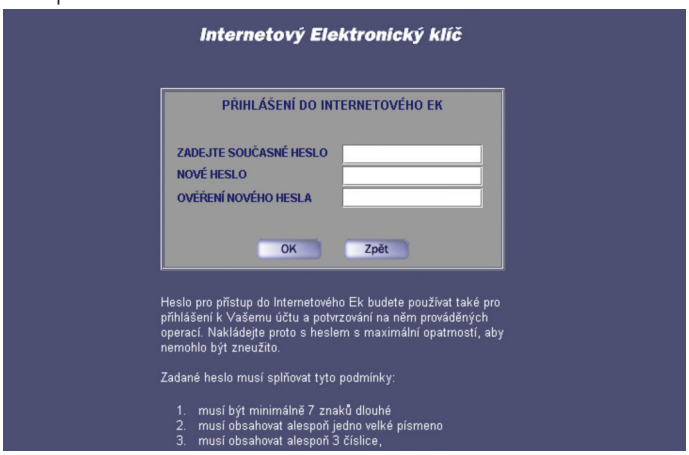
Neprovedení obnovy má za následek ukončení možnosti přihlásit se s IEk k vašemu účtu. Obnova je pak možná pouze tehdy, pokud současně využíváte Osobní či Mobilní Elektronický klíč s jehož pomocí se přihlásíte na účet a ze stránky pro správu IEk (Obrázek 1) si stáhnete váš nový Osobní certifikát.

3.2 Změna hesla IEk

- Změnu hesla provedete po přihlášení na svůj účet v Klientském systému a volbou v menu Nastavení - Internetový Ek.
- Zde nastavte cestu ke svému IEk (není-li přednastavena), stiskněte tlačítko OK.
- Zadejte heslo pro přihlášení do IEk a znovu stiskněte tlačítko OK. Tím se dostanete na záložku SPRÁVA CERTIFIKÁTŮ.
- V záložce NASTAVENÍ vyvolejte obrazovku pro změnu hesla kliknutím na tlačítko Změnit heslo, zadejte současné heslo, nové heslo a pro kontrolu nové heslo ještě jednou (Obrázek 2).

Nové zadané heslo musí splňovat tyto podmínky:

- musí být minimálně 7 znaků dlouhé,
- musí obsahovat alespoň jedno velké písmeno,
- musí obsahovat alespoň 3 číslice,které nesmí být po sobě jdoucí nebo stejné.
- Zadání potvrďte stisknutím tlačítka OK a při další práci s IEk zadávejte již nové heslo.



Obrázek 2

3.3 Blokace a zneplatnění Osobního certifikátu

Osobní certifikát může být v době jeho platnosti dočasně blokován. Blokovaný Osobní certifikát není možné použít k autentizaci ani certifikaci, ale je standardně obnovován. Blokaci Osobního certifikátu je vhodné provést zejména tehdy, pokud nehodláte IEk delší dobu používat.
Blokace může být provedena telefonicky na infolince **800 900 900**.
Opětovná aktivace může být provedena pouze osobně na pobočce.

V případě podezření na vyzrazení hesla do IEk, ztráty samotného IEk (souboru *.key) nebo při napadení vašeho počítače, na kterém IEk používáte, škodlivým softwarem nebo cizí osobou, neprodleně zneplatněte Osobní certifikát.
Zneplatnění může být provedeno telefonicky na infolince **800 900 900.**
O zneplatnění Osobního certifikátu může v odůvodněných případech rozhodnout také Raiffeisenbank.
Certifikát může být bankou zneplatněn pokud jeho držitel zemřel (po předložení úmrtního listu oprávněnými osobami), soudním rozhodnutím, podezřením Raiffeisenbank na zneužití certifikátu nebo zjištěním, že osoba oprávněná porušuje smluvní podmínky, za kterých byl certifikát vydán.
Zneplatněný certifikát již nemůže být znovu obnoven.

V případě, že byl váš Osobní certifikátu zneplatněn před vypršením jeho řádné platnosti, je zařazen na Seznam zrušených certifikátů. Vytváření seznamu probíhá každý den, platnost svých certifikátů si můžete kdykoliv oproti tomuto seznamu ověřit.

3.4 Ověření platnosti certifikátů

Ověření platnosti certifikátů probíhá automaticky vždy při použití IEk k autentizaci, bez platných certifikátů se nelze přihlásit do Klientského systému. Pro případy vypršení platnosti certifikátu doporučujeme mít pro přihlášení do Klientského systému aktivovaný i jiný Ek.

Ověření lze provést i manuálně po přihlášení na účet v Klientském systému:

- Zvolte menu Nastavení - Internetový Ek.
- Zde nastavte cestu ke svému IEk (není-li přednastavena), stiskněte tlačítko OK.
- Zadejte heslo pro přihlášení do IEk a znovu stiskněte tlačítko OK. Tím se dostanete na stránku SPRÁVA CERTIFIKÁTŮ.
- Na záložce ZRUŠENÉ CERTIFIKÁTY stiskněte tlačítko Ověřit (Obrázek 3) a tím provedete ověření platnosti certifikátů v IEk jejich porovnáním se Seznamem zrušených certifikátů.

Obrázek 3

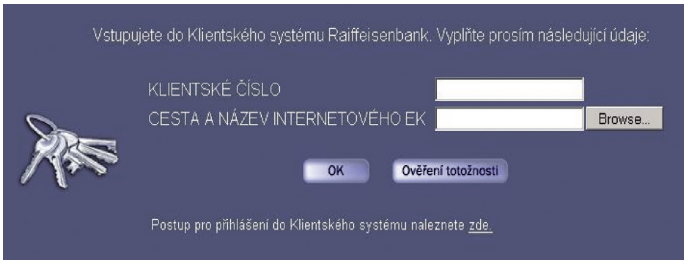
3.5 Export certifikátů

Při načítání certifikátů z internetu máte možnost si je uložit v datové podobě jako soubory např. pro účely záložní obnovy IEk. Uložení provedete v DETAILU CERTIFIKÁTU tlačítkem Export certifikátu.

4 Používání IEk při práci s účtem

4.1 Přihlášení na účet

Přihlášení na účet spočívá v zadání Klientského čísla a cesty k IEk na přihlašovací stránce k účtu, která je přístupná na www adrese http://www.rb.cz – Vstup na účet – eKonto Internetový klíč. Po prvním úspěšném přihlášení k účtu bude tato cesta při opětovném přihlášení automaticky načtena (máte-li povoleno používání cookies – Obrázek 4).
Po stisknutí OK budete vyzváni k zadáni hesla k IEk. Potvrďte OK.



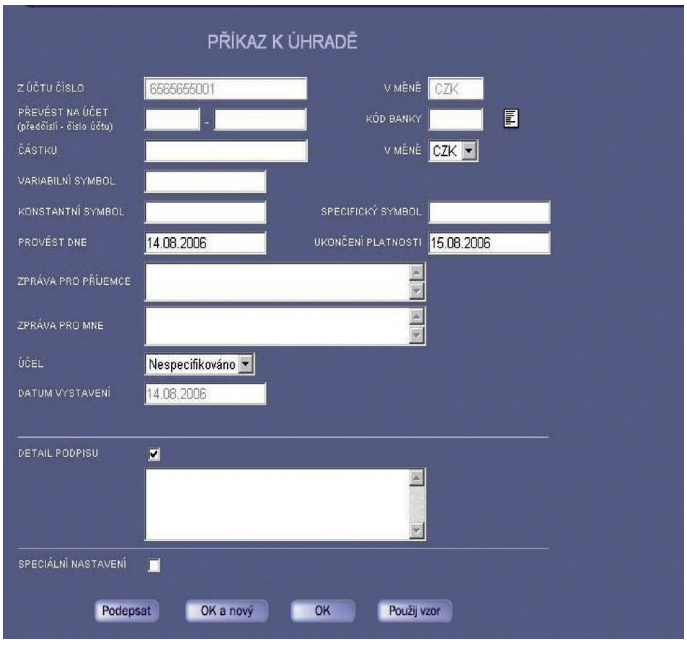
Obrázek 4

TIP

Při přihlášení v internetovém prohlížeči Firefox se na přihlašovací obrazovce zobrazí i pole Heslo (u jiných prohlížečů se toto pole zobrazí až po stisknutí tlačítka OK).

4.2 Podpis IEk

Podpis pomocí IEk provádíte kliknutím na tlačítko Podepsat po vyplnění formuláře požadované operace.
Po výzvě zadáte heslo do IEk, stisknete OK a tím se připojí elektronický podpis k požadované operaci.
Přehled podepisovaných údajů spolu s detailem elektronického podpisu můžete před odesláním podepsaného požadavku do Klientského systému Raiffeisenbank nalézt v okně DETAIL PODPISU.
Takto podepsaný formulář odešlete do Klientského systému kliknutím na tlačítko OK popřípadě OK a nový (Obrázek 5).



Obrázek 5

4.3 Ověření identity při komunikaci s Telefonním bankéřem

IEk mimo jiné umožňuje ověření vaší osoby při telefonické komunikaci s Telefonním bankéřem Infolinky.

Při ověření totožnosti pomocí IEk vám sdělí Telefonní bankéř tzv. autentizační výzvu (jedná se o osmimístné číslo).
Na přihlašovací stránce k účtu, která je přístupná na www adrese http://www.rb.cz – Vstup na účet – eKonto Internetový klíč (Obrázek 4) stiskněte tlačítko Ověření totožnosti.
Na další stránce (Obrázek 6) zadáte vaše klientské číslo, cestu k IEk (pokud není automaticky načtena) a autentizační výzvu (osmimístné číslo).
Tlačítkem Podepsat, zadáním hesla do IEk a stiskem OK tento formulář k ověření totožnosti podepište a tlačítkem Odeslat odešlete do Klientského systému.
Na základě tohoto ověření Telefonní bankéř může s vámi provést veškeré neaktivní operace, tzn. sdělit informace o účtu, převzít reklamaci apod.
Při ověření totožnosti tímto způsobem nelze zadat platby, měnit nastavení účtu a jiné aktivní operace.
Při autentizaci má výzva i elektronický podpis dobu platnosti omezenou na 30 minut. Pokud tedy odešlete formulář k ověření totožnosti po uplynutí 30 minut od podepsání nebo obdržení autentizační výzvy, ověření totožnosti nebude provedeno.

Obrázek 6

5 Bezpečnost při používání IEk

Nejdůležitější bezpečnostní hrozbu představuje možnost získání souboru Internetového Elektronického klíče (případně jeho kopie) neoprávněnou osobou a vyzrazení přístupového hesla k IEk. IEk a znalost přístupového hesla umožňuje útočníkovi předstírat v komunikaci s Raiffeisenbank klientovu identitu a tak získat přístup a možnost manipulace s jeho účtem.

Pro ochranu IEk doporučujeme dodržovat následující zásady:

- Chraňte svůj IEk. Soubor *.key obsahující Soukromý klíč uložte na vyjímatelné paměťové médium, které máte pod svou výhradní kontrolou a toto médium bezpečně uložte. Neukládejte IEk na pevný disk počítače, pracujte pouze s jedinou kopií na vyjímatelném paměťovém médiu, další kopie nepořizujte, resp. smažte. Nevkládejte médium s IEk do nedůvěryhodných počítačů.
- Chraňte přístupové heslo. Heslo volte tak, aby nebylo snadno uhádnutelné nebo odvoditelné z informací o vaší osobě. Heslo v žádném případě nikomu nesdělujte. K ochraně přístupového hesla Raiffeisenbank prohlašuje, že přístupové heslo k Internetovému Elektronickému klíči používá applet banky výhradně lokálně a v žádném okamžiku toto heslo neodesílá z klientské stanice a neukládá jej ani v otevřené podobě na lokální disk klientské stanice.
- Při podezření nebo zjištění vyzrazení, krádeže či ztráty vašeho IEk nebo hesla, neprodleně zneplatněte Osobní certifikát, viz kapitola 3.3.
- IEk používejte pouze na vlastním řádně zabezpečeném počítači, nepoužívejte počítače, o kterých nemáte žádné informace, nebo jsou v nedůvěryhodném prostředí. Počítač zabezpečte řádně nakonfigurovaným firewallem, antivirovým a antispyware softwarem. Pravidelně a v případě vydání bezpečnostních oprav neprodleně aktualizujte operační systém vašeho počítače, prohlížeč, bezpečnostní software, ale i další používaný software.
- Na počítači, kde používáte IEk, nepoužívejte a neinstalujte nedůvěryhodný software, nenavštěvujte nedůvěryhodné webové stránky a neotvírejte podezřelé poštovní zprávy, zejména neotevírejte přílohy takových zpráv. Raiffeisenbank nikdy neposílá nevyžádané zprávy obsahující odkazy na své webové stránky, pokud obdržíte elektronickou poštou zprávu obsahující odkaz na webové stránky Raiffeisenbank, nereagujte na ni a informujte nás prosím.
- Spolu se souborem s příponou *.key je vytvořen i soubor s příponou *.zal, který obsahuje kopii Soukromého klíče určenou pro obnovu IEk v případě jeho poškození nebo smazání souboru *.key. Tento soubor přesuňte na vyjímatelné paměťové médium, které máte pod svou výhradní kontrolou a toto médium bezpečně uložte odděleně od IEk. Obnovu provedete tak, že soubor *.zal nakopírujete do požadovaného místa uložení IEk a přejmenujete na *.key. Takto vytvořený IEk je chráněn heslem zadaným při vytváření původního IEk, které je nutné si pro tento účel pamatovat. Po té do něj provedete vložení certifikátů.

6 Doplněk – detailní popis IEk

Internetový Elektronický klíč je softwarové úložiště soukromých klíčů a certifikátů v jednom souboru na paměťovém mediu pod výhradní kontrolou klienta Raiffeisenbank. Data jsou vkládána zašifrovaná algoritmem TripleDES CBC a přístup k nim je chráněn soukromým heslem klienta. Veškerá práce s Internetovým Elektronickým klíčem je prováděna lokálně na klientově stanici appletem banky, vyvinutým na bázi standardní kryptografické knihovny J/CRYPTO od Baltimore Technologies, Plc. a knihovny Java Key Store společnosti SUN Microsystems, Inc.

Certifikáty vydávané a akceptované Raiffeisenbank mají následující vlastnosti:

- typ certifikátu: X.509
- verze certifikátu: 3
- typy klíčů: RSA asymetrické klíče
- algoritmus generování klíčů: RSA kryptografický algoritmus
- délka klíčů: 1024 bitů
- struktura vlastníka certifikátu: X.500
- struktura vydavatele certifikátu: X.500
- algoritmus podpisu certifikátu: SHA1+ RSA zakódování
- certifikační požadavek: podle PKCS#10
- podpis certifikačního požadavku: SHA1+RSA zakódování
- platnost certifikátu: 1 rok

Obsah certifikátu a žádosti o certifikát tvoří tyto údaje:
název identifikace položky v certifikátu

- jméno NAME
- příjmení SURNAME
- jméno příjmení COMMON NAME
- rodné číslo DESCRIPTION
- město bydliště LOCATION
- stát COUNTRY
- e-mail EMAIL

Tyto údaje jsou v certifikátu dostupné.

Exportní a importní formát je DER+PEM podle X.509 („Distinguished Encoding Rules“ pro ASN.1 + „Personal Enhanced Mail“).
S přístupovým heslem se nakládá podle standardu PKCS#8. Applet banky kontroluje při vytváření Internetového Elektronického klíče minimální požadovanou složitost hesla.

Infolinka: 800 900 900
Web: www.rb.cz
E-mail: info@rb.cz

Raiffeisen BANK

Banka inspirovaná klienty

PE-C075-01-08