

# UŽIVATELSKÁ PŘÍRUČKA PRO INTERNETBANKING PPF banky a.s.

## Část II: Certifikát, OTP kód, SMS kód a práce s Tokeny

## Obsah:

1. Úvod .....	3
2. OTP kód a práce s Hardwarovým OTP Tokenem .....	3
3. SMS kód .....	4
4. Certifikát a práce s Certifikačním Tokenem .....	4
4.1. Certifikační centrum .....	5
4.2. Stažení SW pro správný chod Internetbankingu .....	6
4.3. Stažení knihovny pro práci s elektronickým klíčem (applet pro šifrování dat) .....	9
4.4. Stažení ovladačů pro Certifikační Token .....	12
4.5. Stažení SW pro správu Certifikačního Tokenu .....	15
4.6. Změna PIN k Certifikačnímu Tokenu .....	18
4.7. Vygenerování Certifikátu .....	19
4.8. Obnovení Certifikátu .....	22
4.9. Smazání neplatného Certifikátu .....	24

## 1. Úvod

Uživatelská příručka je pro její větší přehlednost rozdělena do několika částí, které tvoří samostatné dokumenty. Tato část popisuje práci s Tokeny a Certifikátem. Ostatní informace týkající se IB jsou uvedeny v dalších částech Uživatelské příručky.

Jsou-li v textu Uživatelské příručky použity pojmy, zkratky nebo slovní spojení začínající velkým písmenem, mají význam stanovený v článku Výklad pojmů VOP a/ nebo KOP, případně význam specifikovaný v jednotlivých ustanoveních VOP a/nebo KOP a/nebo této Uživatelské příručky.

## 2. OTP kód a práce s Hardwarovým OTP Tokenem

OTP kód je jednorázově použitelný číselný kód (OTP = One Time Password). OTP kód je generován průběžně každých 60 sekund a je založen na synchronizaci mezi autentikačním serverem Banky a OTP Tokenem Uživatele (jedná se o tzv. time-based kód).

OTP kód je platný vždy pouze pro jeden úkon (přihlášení do IB, autorizace Platebního příkazu, žádosti, vytvoření oznámení atd.). Vygenerovaný OTP kód musí být zadán a potvrzen pro provádění úkon do 10-ti minut od jeho vygenerování (**NE zobrazení!**).

**OTP Tokeny zobrazují aktuálně vygenerovaný OTP kód, negenerují jej až v okamžiku jejich zobrazení.**

**Pro generování a zobrazování OTP kódu může být použit pouze Hardwarový OTP Token prodáváný Bankou.**

### Co je to Hardwarový OTP Token?

Hardwarový OTP Token je produkt eToken PASS společnosti SafeNet Inc. Je to malé elektronické zařízení vzhledově připomínající miniaturní MP3 přehrávač. Jedná se o generátor OTP kódů, který přináší silnou dvoufaktorovou autentizaci.



**Na rozdíl od Certifikačního Tokenu se jedná o řešení nezávislé na operačním systému, Uživatel nemusí instalovat žádný podpůrný software nebo ovladače – výhodou je tedy maximální mobilita. Odpadají rovněž problémy při generování Certifikátů.**

Zabudovaná baterie má životnost až 7 let nebo 14 000 zobrazení OTP kódu – např. při deseti zobrazení denně vydrží Hardwarový OTP Token cca 5 let.

Pro zobrazení aktuálního OTP kódu stiskněte tlačítko na pravé straně Hardwarového OTP Tokenu. Hardwarový OTP Token následně zobrazí na LCD displeji aktuálně vygenerovaný OTP kód. Tento OTP kód opište do příslušného pole v IB.



**!!! POZOR !!!**

- **OTP kód je na displeji zobrazen pouze po dobu 30-ti sekund, poté displej zhasne.**
- **I v průběhu těchto 30-ti sekund se může stát, že bude vygenerován a tedy i zobrazen nový OTP kód – OTP kódy jsou generovány vždy průběžně každých 60 sekund bez ohledu na to, zda si je Uživatel právě zobrazuje nebo ne (viz úvodu bodu 2.).**
- **Je proto potřeba věnovat velkou pozornost zobrazenému OTP kódu – pokud nestihnete opsat a potvrdit zobrazený OTP kód, raději počkejte na vygenerování dalšího OTP kódu.**
- **Pokud IB požaduje zadání dvou OTP kódů, jedná se vždy o dva různé, po sobě jdoucí OTP kódy (zejména při registraci Hardwarového OTP Tokenu při prvním přihlášení do IB). V tomto případě je nutné po zadání prvního OTP kódu vyčkat na vygenerování dalšího OTP kódu a teprve poté jej zadat.**

### 3. SMS kód

SMS kód je jednorázově použitelný číselný kód na principu OTP kódu – viz bod 2. Není však generován průběžně, ale až po provedení určité akce (jedná se o tzv. event-based kód nebo také challenge-response).

SMS kód je rovněž platný pouze pro jeden úkon (přihlášení do IB, autorizace Platebního příkazu, žádosti, vytvoření oznámení atd.). Vygenerovaný SMS kód je zasílán Uživateli formou SMS na jeho mobilní telefon a musí být zadán a potvrzen pro prováděný úkon do 10-ti minut od jeho vygenerování (**NE zobrazení!**).

Výhodou oproti OTP kódu je, že Uživatel nepotřebuje žádný speciální token, ale pro získání SMS kódu potřebuje pouze svůj mobilní telefon. Odpadají tak náklady na pořízení nutného zařízení. Navíc pro něj platí stejná výhoda maximální mobility oproti využívání Certifikátu – toto řešení je nezávislé na operačním systému, Uživatel nemusí instalovat žádný podpůrný software nebo ovladače (stejně jako u OTP Tokenů pro OTP kódy).

### 4. Certifikát a práce s Certifikačním Tokenem

**Co je to Certifikační Token?**

Certifikační Token je produkt Borderless Security USB token iKey 4000 společnosti SafeNet Inc. Je to malé USB PKI zařízení podobné flash disku, které přináší silnou dvoufaktorovou autentizaci.



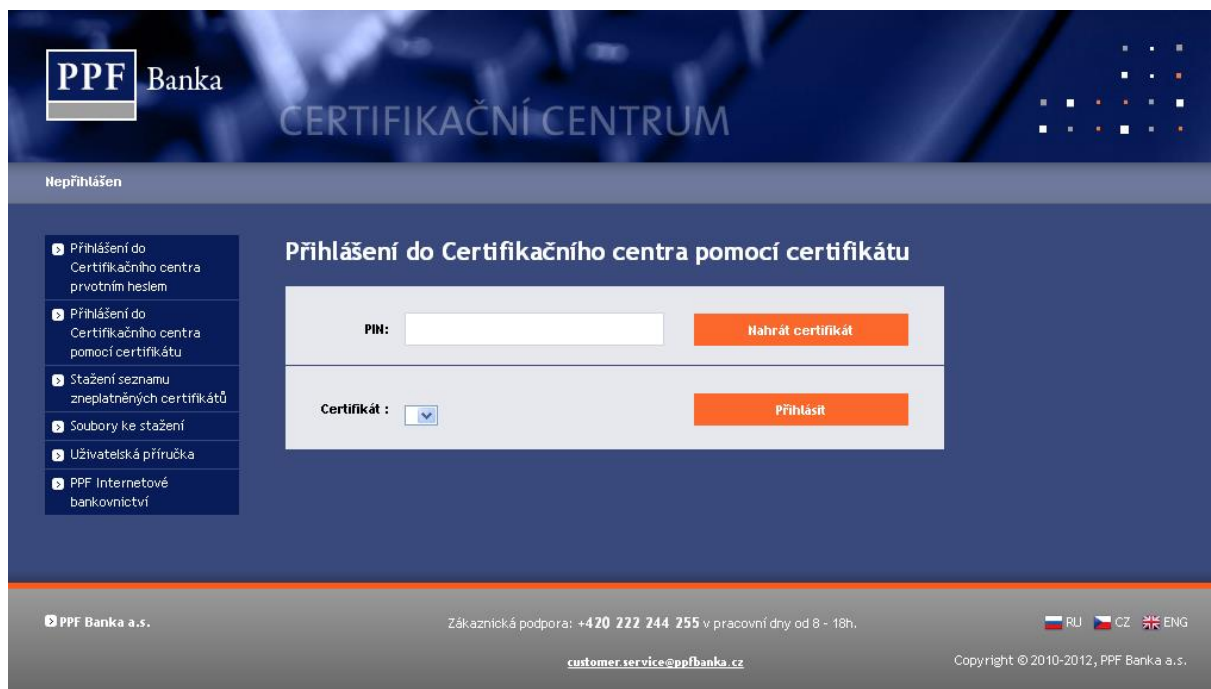
Certifikační Token je kompatibilní s USB1.1 a vyšší a je zabezpečen pomocí PIN kódu. Podpora šifrovacích algoritmů je integrována přímo v hardware Certifikačního Tokenu.

Vyžaduje instalaci SW a ovladačů pro správu Certifikačního Tokenu knihovny pro práci s elektronickým klíčem na PC, na kterém bude používán.

**Pro generování a ukládání Certifikátu může být použit pouze Certifikační Token prodáváný Bankou.** Pro jeho správné používání si nainstalujte potřebná zařízení a vygenerujte Certifikát dle následujících bodů.

## 4.1. Certifikační centrum






Certifikační centrum je přístupné z internetových stránek <https://ibcc.ppfbanka.cz>. Po zadání těchto internetových stránek se zobrazí následující obrazovka:



Pro zajištění správného vygenerování Certifikátu je nutné dodržet následující postup:

1. stáhnout SW pro správný chod IB (Java) – bod [4.2.](#) – **tuto verzi Java si nainstalujte i v případě, že již máte Java ve vašem PC nainstalovanou;**
2. stáhnout knihovnu pro práci s elektronickým klíčem (applet pro šifrování dat) – bod [4.3.](#);
3. stáhnout ovladače pro Certifikační Token k příslušnému operačnímu systému – bod [4.4.](#);
4. stáhnout SW pro správu Certifikačního Tokenu – bod [4.5.](#);
5. **restartovat PC;**
6. změnit PIN k Certifikačnímu Tokenu – bod [4.6.](#);
7. vygenerovat Certifikát – bod [4.7.](#)

Ovladače, SW pro Certifikační Token a applet pro šifrování dat stáhnete z volby **Soubory ke stažení**. Zobrazí se všechny soubory, které je nutné si stáhnout do PC pro správnou funkčnost Certifikačního Tokenu.

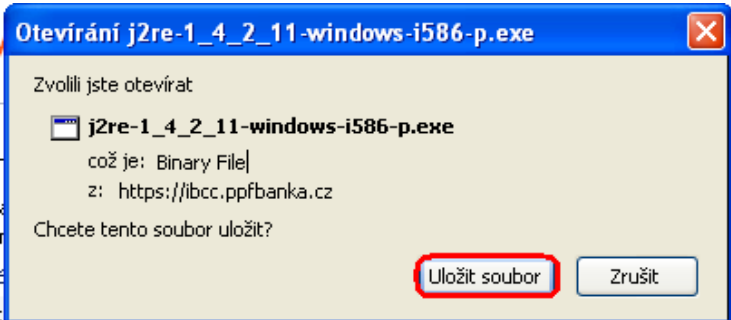
<ul style="list-style-type: none"> <li>1. Přihlášení do Certifikačního centra prvotním heslem</li> <li>2. Přihlášení do Certifikačního centra pomocí certifikátu</li> <li>3. Stažení seznamu zneplatněných certifikátů</li> <li><b>4. Soubory ke stažení</b></li> <li>5. Uživatelská příručka</li> <li>6. PPF Internetové bankovníctví</li> </ul>	<h3 style="color: #e67e22;">Soubory ke stažení</h3> <p><b>Software pro správu tokenu</b> Java(TM) 2 Runtime Environment SE</p> <p>1.  nutno nainstalovat pro správný chod aplikace internetového bankovníctví ve vašem webovém prohlížeči. Pokud již máte poslední verzi Java ve vašem PC nainstalovanou, instalace není třeba. <b>j2re-1_4_2_11-windows-i586-p.exe</b>, 15,4 MB</p> <p>Knihovna PKCS11 pro práci s elektronickým klíčem</p> <p>2.  nutno nainstalovat, aby bylo vaše PC schopno správně komunikovat s elektronickými klíči v systému internetového bankovníctví PPF banky . <b>BSC_Applet_PKCS11.exe</b>, 497 kB</p> <p>Ovladače k tokenu pro 32bit OS Windows</p> <p>3.  nutno nainstalovat, aby bylo vaše PC schopno detekovat USB token iKey 4000 <b>iKeyDrv32_v1.exe</b>, 4,1 MB</p> <p>Ovladače k tokenu pro 64bit OS Windows (U některých verzí OS Win. vyžaduje instalaci v kompatibilním režimu)</p> <p>3.  nutno nainstalovat, aby bylo vaše PC schopno detekovat USB token iKey 4000 <b>iKeyDrv64_v1.exe</b>, 1,5 MB</p> <p>Software pro správu tokenu</p> <p>4.  doporučujeme nainstalovat, jedná se o uživatelské rozhraní pro správu tokenu iKey 4000 (zobrazuje certifikáty včetně jejich platnosti, umožňuje změnu PIN tokenu a další důležité funkce) <b>PPFBswToken_v1.msi</b>, 3,7 MB</p>
---	---

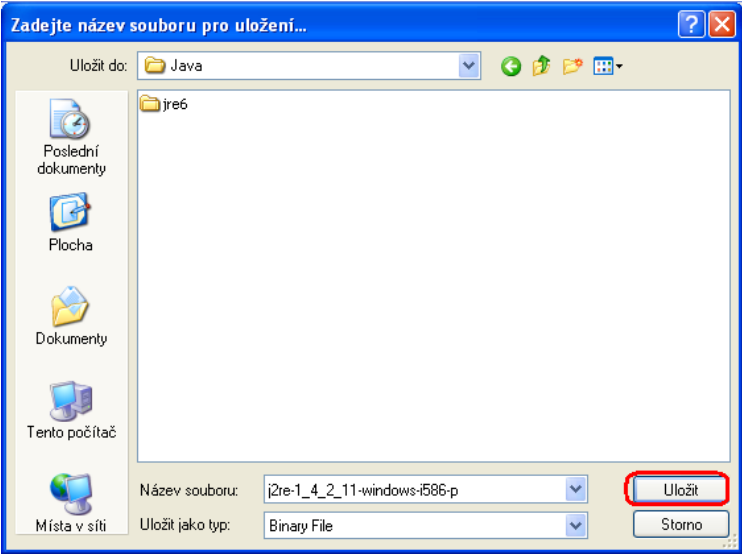
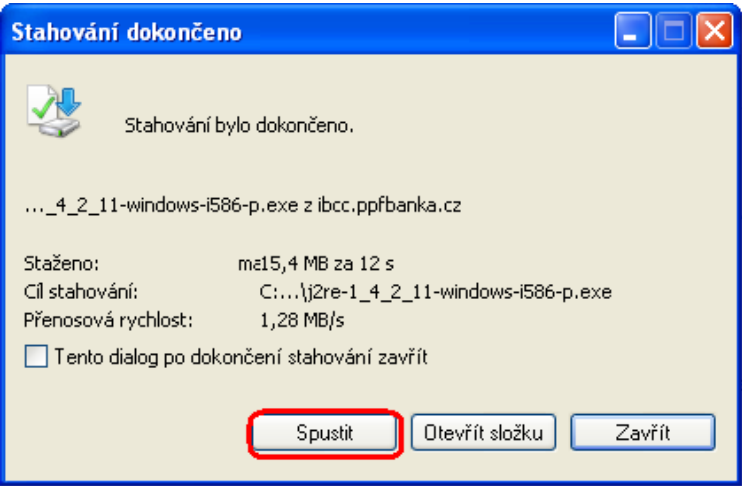
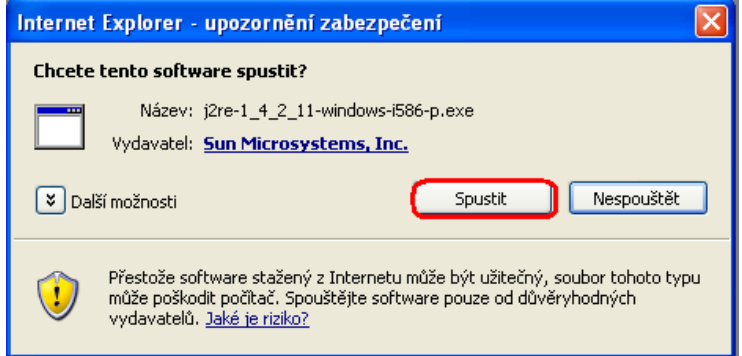
### **DŮLEŽITÉ UPOZORNĚNÍ:**

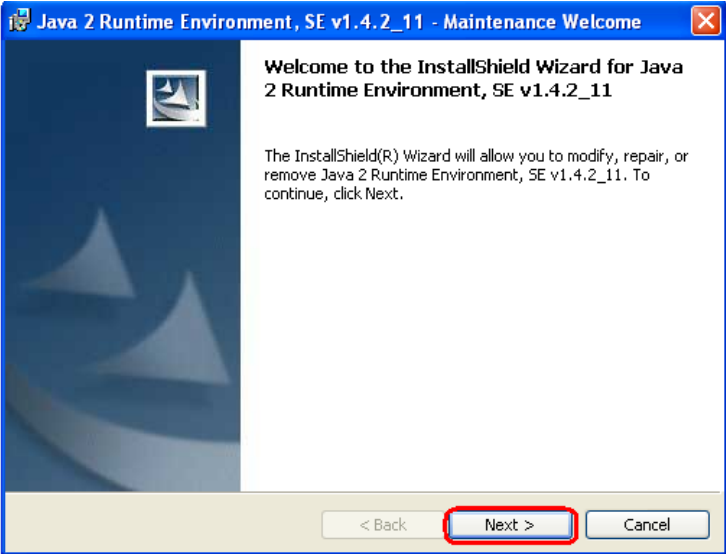
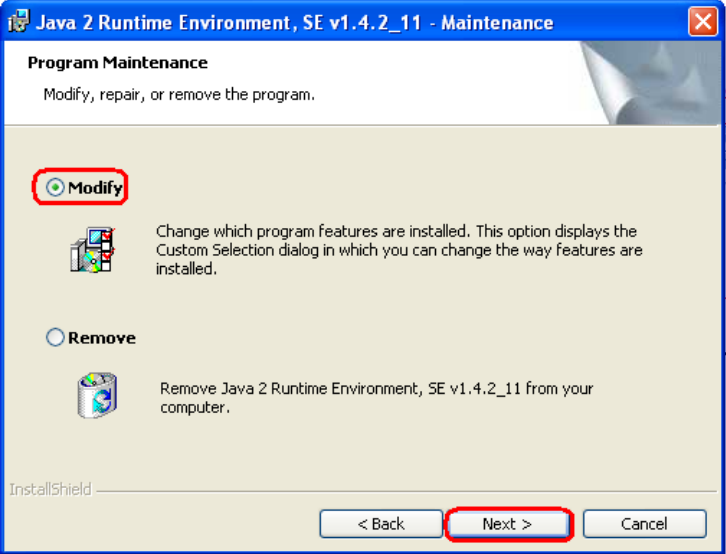
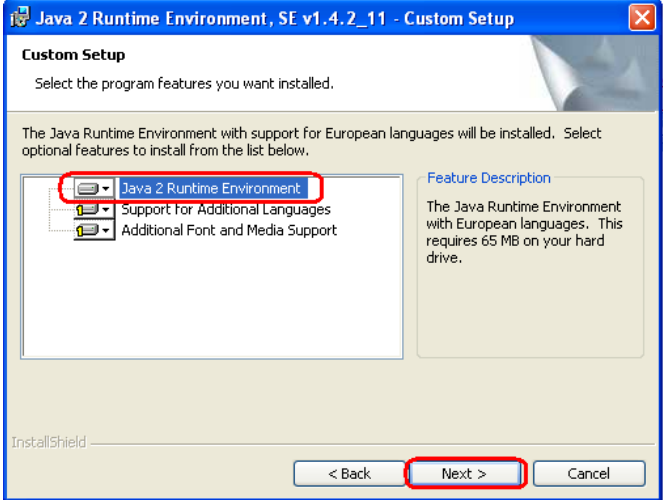
- **V různých prohlížečích (Mozilla Firefox, Internet Explorer, Google Chrome atd.) se mohou zobrazovaná dialogová okna mírně lišit (např. místo tlačítka *Uložit se* zobrazí tlačítko *Uložit soubor*), příp. mohou být některá dialogová okna vložena navíc.**
- **Jazyk dialogových oken závisí na nastavení operačního systému nebo na nastavení v jednotlivých souborech – Banka ani Uživatel jej nemohou ovlivnit.**
- **Pokud již využíváte Certifikační Token nebo čipovou kartu (příp. jim podobné šifrovací zařízení) od jiného dodavatele nebo od jiné banky, doporučujeme odpojit tato zařízení alespoň po dobu generování a ukládání Certifikátu Banky (z důvodů možné kolize SW při generování Certifikátu). V případě, že tak neučiníte, je možné, že se Certifikát pro IB nepodaří uložit na Certifikační Token.**

Instalace se provádí běžným způsobem s využitím technologie Windows Installeru.

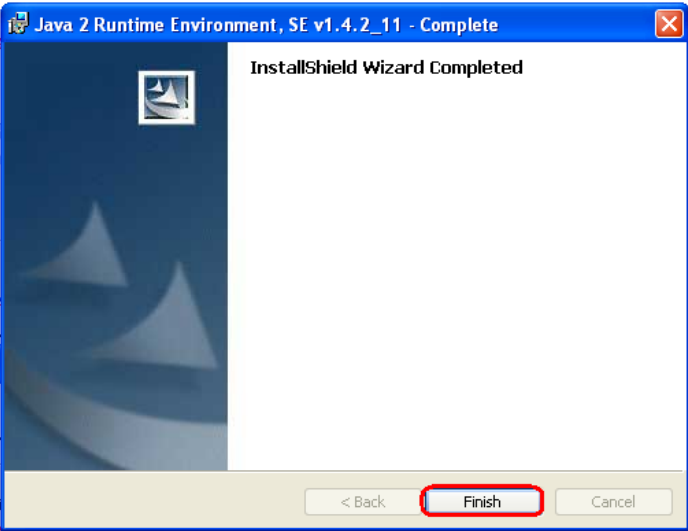
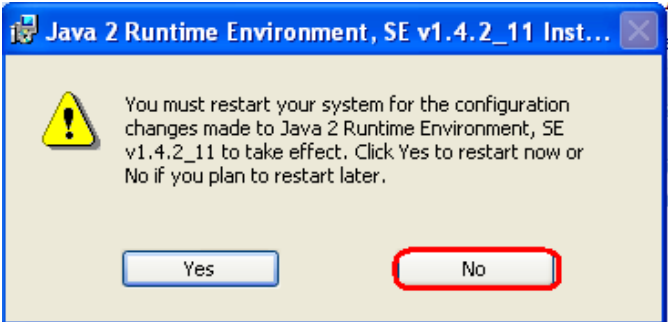
## **4.2. Stažení SW pro správný chod Internetbankingu**

<p>1. Nejdříve vyberte soubor s SW pro správný chod IB. V prvním dialogovém okně klikněte na tlačítko <b>Uložit soubor</b>.</p>	
---	--

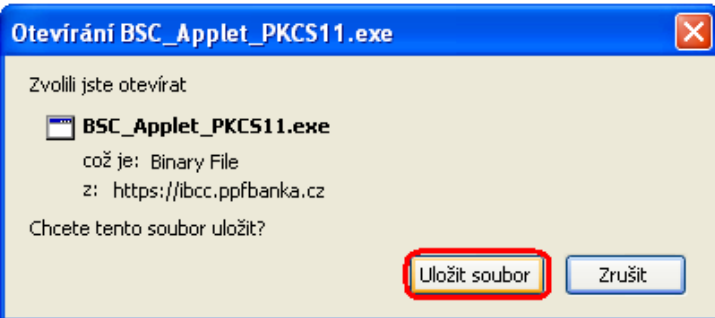
<p>2.</p>	<p>Program Vás vybědne k zadání adresáře pro uložení souboru – zadejte adresář a klikněte na tlačítko <b>Uložit</b>. <b>Název ani typ souboru neměňte!!!</b></p>	
<p>3.</p>	<p>Následně se zobrazí informace o úspěšném ukončení stahování souboru – instalaci spustíte tlačítkem <b>Spustit</b>.</p>	
<p>4.</p>	<p>System zobrazí dotaz, zda chcete SW spustit – potvrďte tlačítkem <b>Spustit</b>.</p>	

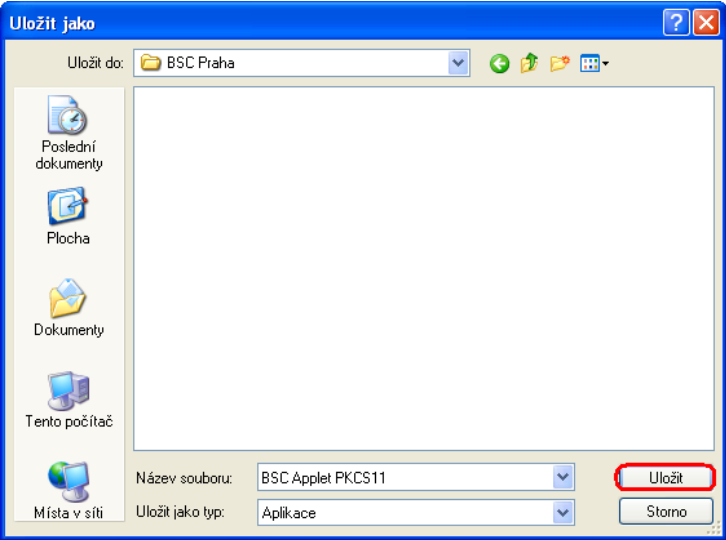
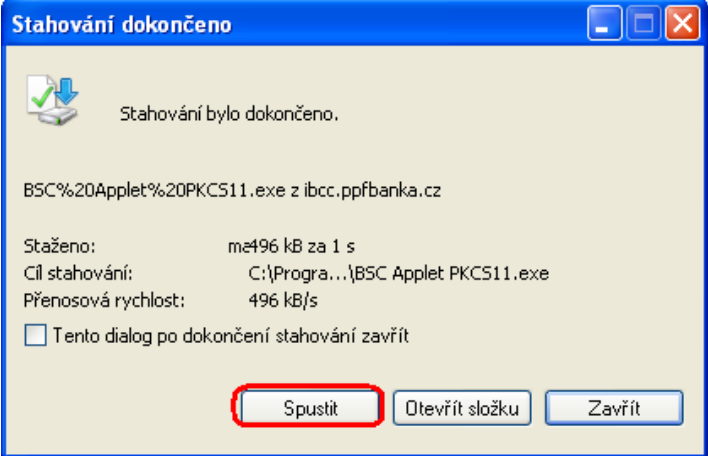
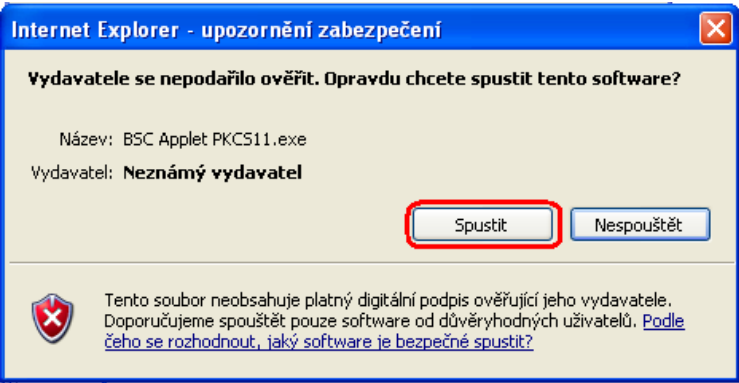
<p>5.</p>	<p>Zobrazí se průvodce instalací. Na první obrazovce průvodce klikněte na tlačítko <b>Next</b>.</p>	
<p>6.</p>	<p>Na další obrazovce ponechejte vybraný typ instalace (<b>Complete</b>, <b>Modify</b> nebo <b>Typical</b>) a klikněte na tlačítko <b>Next</b>.</p>	
<p>7.</p>	<p>Na další obrazovce ponechejte volbu <b>Java 2 runtime Environment</b> a klikněte na tlačítko <b>Next</b>.</p>	

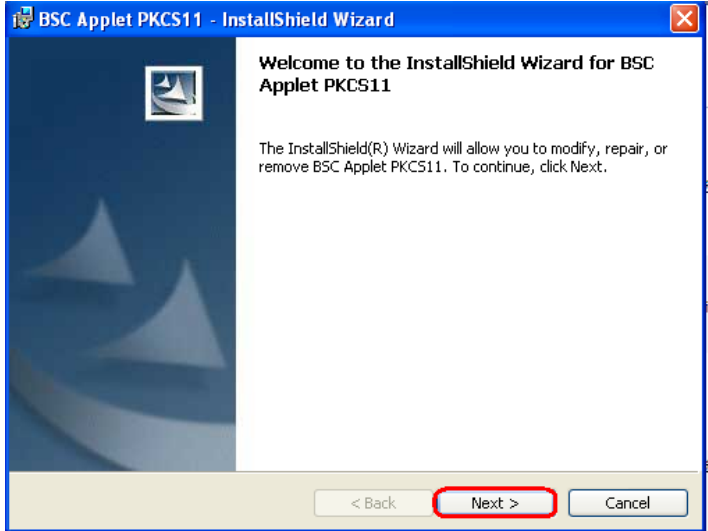
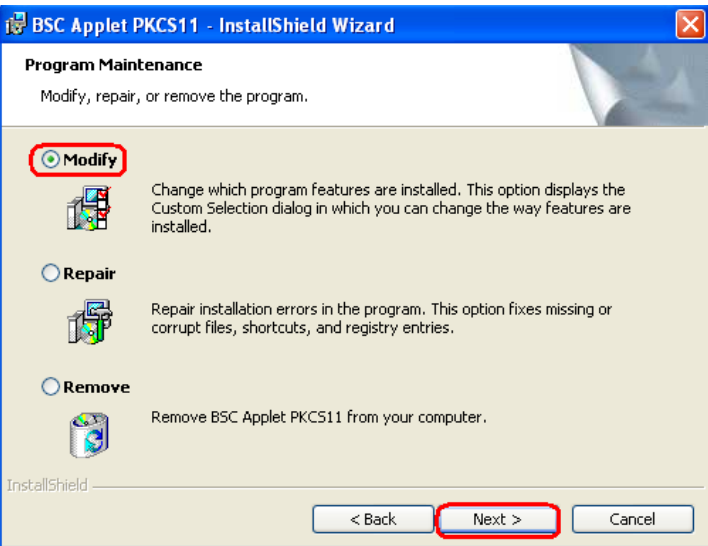
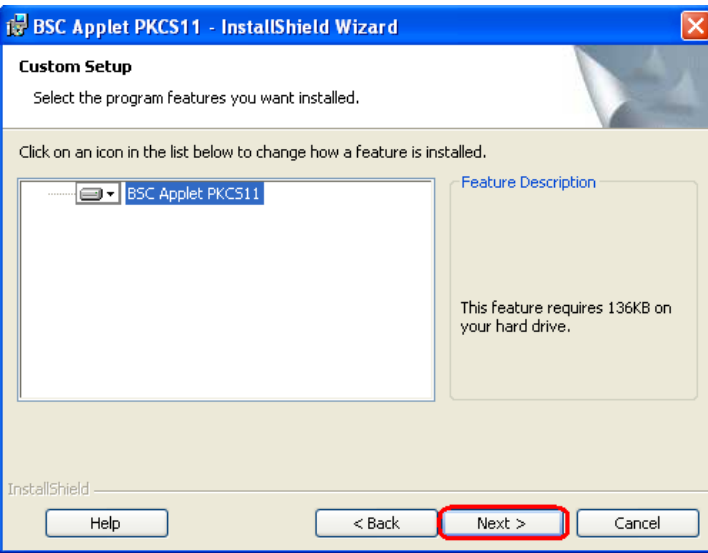


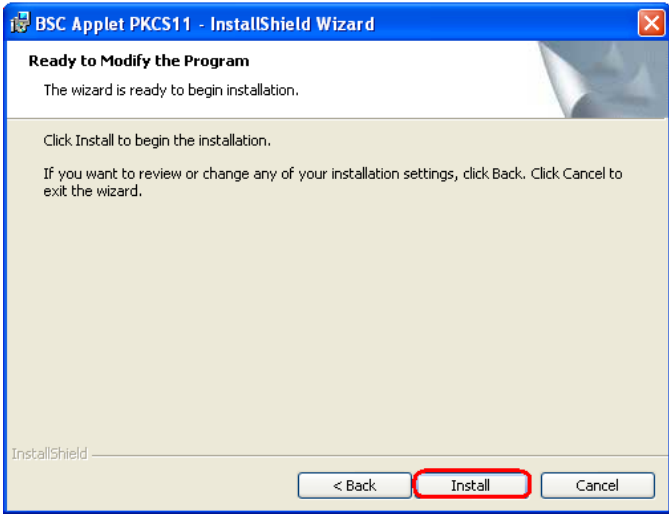
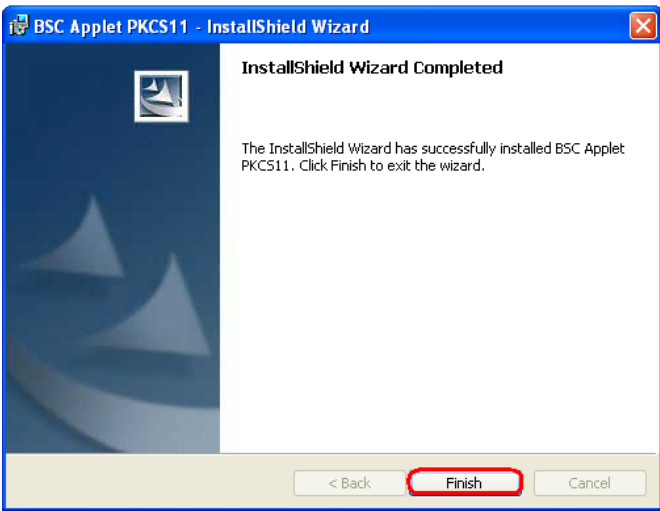
8.	Po ukončení instalace klikněte na tlačítko <b>Finish</b> .	
9.	Následně se zobrazí okno s informací o nutnosti restartování PC – klikněte na tlačítko <b>No</b> (restart PC bude proveden později po nainstalování všech potřebných souborů).	

### 4.3. Stažení knihovny pro práci s elektronickým klíčem (applet pro šifrování dat)

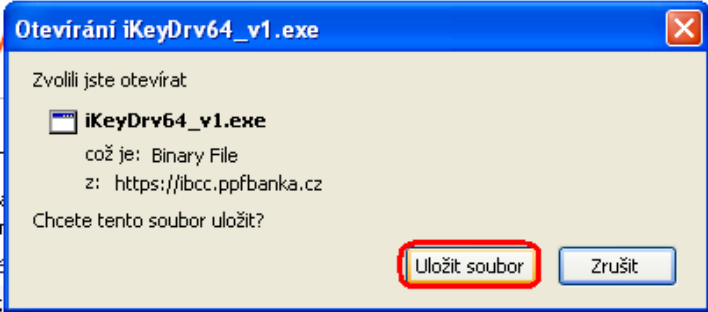
1.	Dále vyberte soubor s appletem pro komunikaci IB s Certifikačním Tokenem. V prvním dialogovém okně klikněte na tlačítko <b>Uložit soubor</b> .	
----	--	--

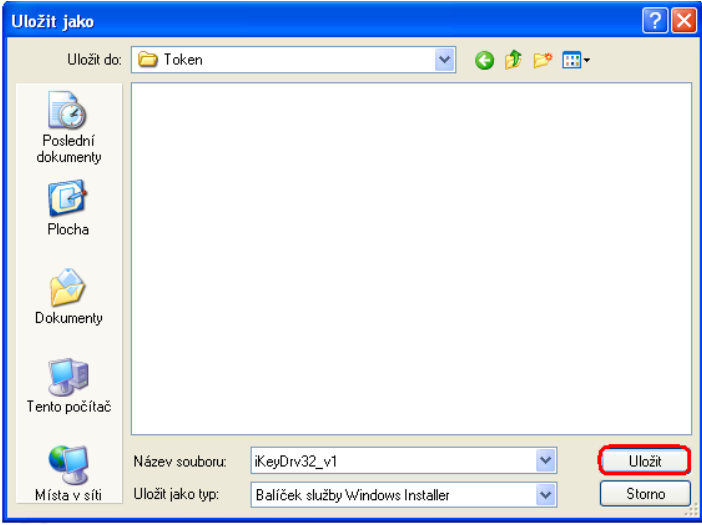
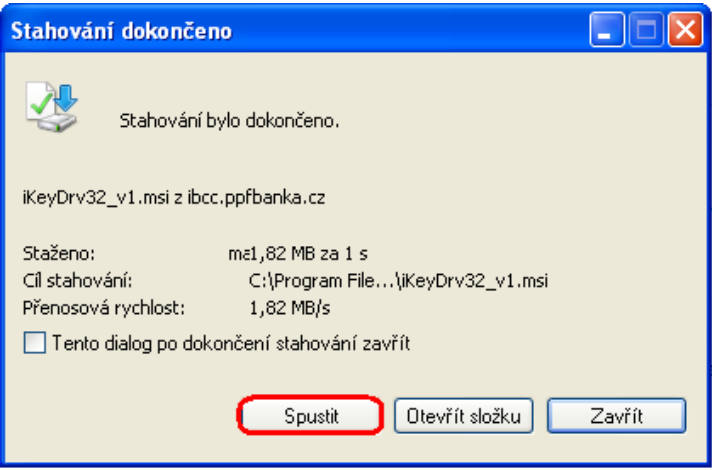
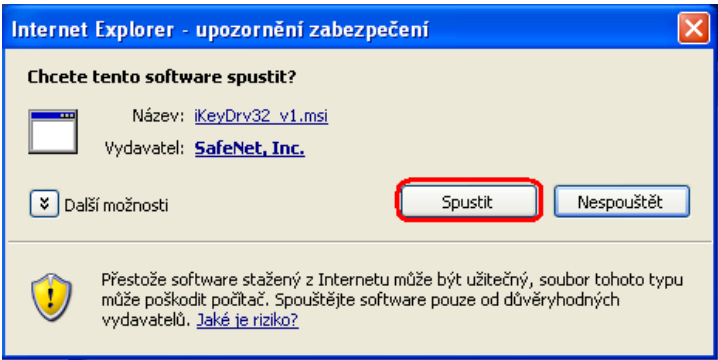
<p>2.</p>	<p>Program Vás vybídne k zadání adresáře pro uložení souboru – zadejte adresář a klikněte na tlačítko <b>Uložit</b>. <b>Název ani typ souboru neměňte!!!</b></p>	
<p>3.</p>	<p>Následně se zobrazí informace o úspěšném ukončení stahování souboru – instalaci spusťte tlačítkem <b>Spustit</b>.</p>	
<p>4.</p>	<p>Systém zobrazí dotaz, zda chcete SW spustit – potvrďte tlačítkem <b>Spustit</b>.</p>	




<p>5.</p>	<p>Spustí se průvodce instalací. Na první obrazovce průvodce klikněte na tlačítko <b>Next</b>.</p>	
<p>6.</p>	<p>Na další obrazovce ponechte vybraný typ instalace (<b>Complete</b>, <b>Modify</b> nebo <b>Typical</b>) a klikněte na tlačítko <b>Next</b>.</p>	
<p>7.</p>	<p>Na další obrazovce klikněte na tlačítko <b>Next</b>.</p>	



<p>8.</p>	<p>Na následující obrazovce spustíte instalaci appletu tlačítkem <b>Install</b>.</p>	
<p>9.</p>	<p>Po ukončení instalace klikněte na tlačítko <b>Finish</b>.</p>	

#### 4.4. Stažení ovladačů pro Certifikační Token

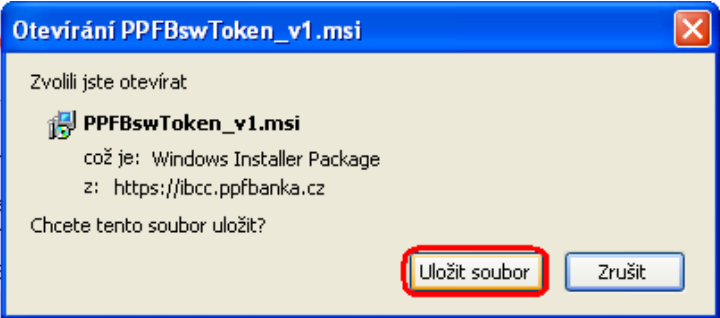
<p>1.</p>	<p>Dále vyberte soubor s ovladači pro Certifikační Token pro příslušný operační systém. V prvním dialogovém okně klikněte na tlačítko <b>Uložit soubor</b>.</p>	
-----------	---	--

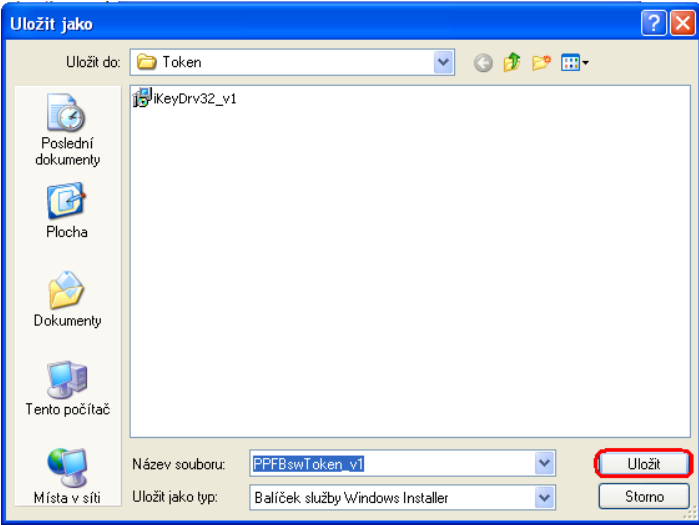
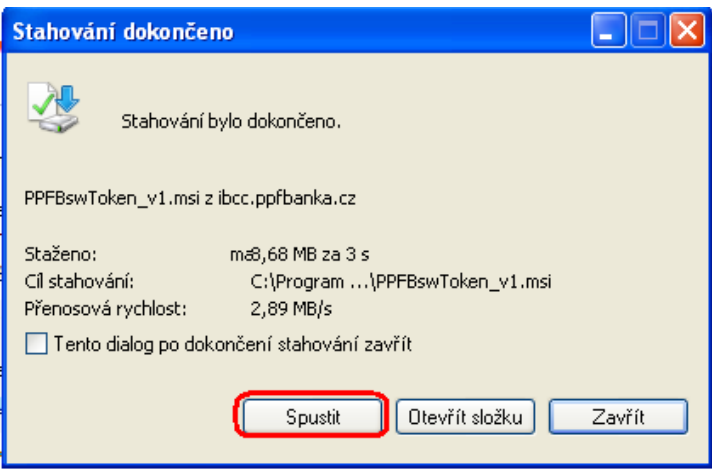
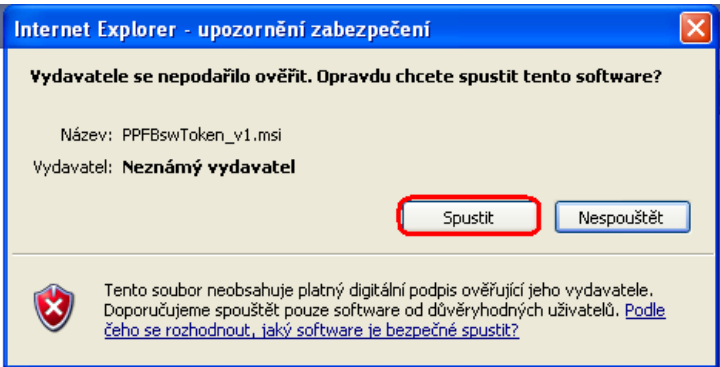
<p>2.</p>	<p>Program Vás vybědne k zadání adresáře pro uložení souboru – zadejte adresář a klikněte na tlačítko <b>Uložit</b>. <b>Název ani typ souboru neměňte!!!</b></p>	
<p>3.</p>	<p>Následně se zobrazí informace o úspěšném ukončení stahování souboru – instalaci spustíte tlačítkem <b>Spustit</b>.</p>	
<p>4.</p>	<p>System zobrazí dotaz, zda chcete SW spustit – potvrďte tlačítkem <b>Spustit</b>.</p>	

<p>5.</p>	<p>Spustí se průvodce instalací. Na první obrazovce průvodce klikněte na tlačítko <b>Next</b>.</p>	
<p>6.</p>	<p>Na další obrazovce je licenční smlouva. Tuto smlouvu si přečtete, a pokud s ní souhlasíte, zaškrtnete volbu <b>I accept the terms in the license agreement</b> a klikněte na tlačítko <b>Next</b>. Pokud nevyjádříte souhlas s licenční smlouvou, nebude možné nainstalovat ovladače pro Certifikační Token a tedy ani vygenerovat Certifikát nezbytný pro přihlášení a Autorizaci v IB.</p>	
<p>7.</p>	<p>Na následující obrazovce spustíte instalaci ovladačů tlačítkem <b>Install</b>.</p>	

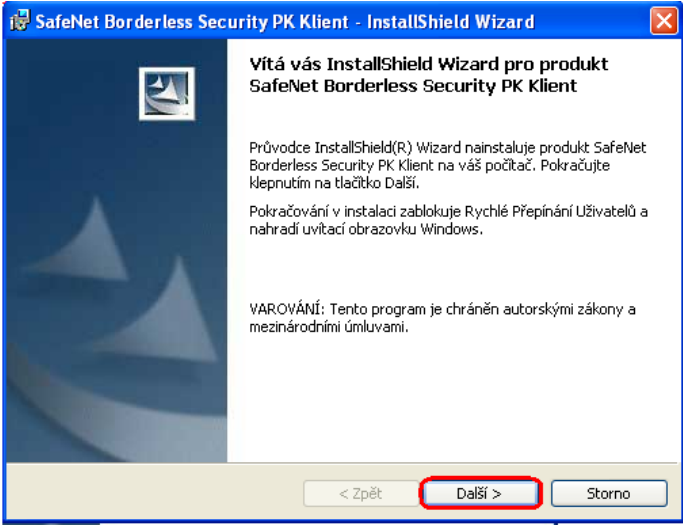
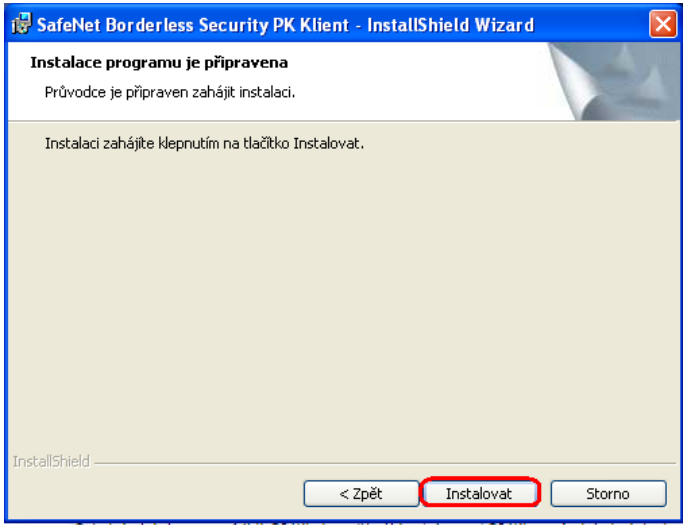
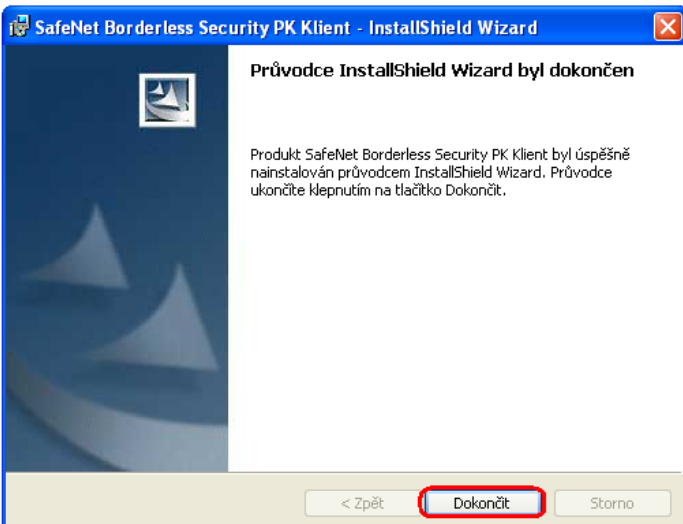
8.	Instalační program Vás vyzve k vložení Certifikačního Tokenu. Vložte Certifikační Token do USB a okno zavřete tlačítkem <b>Close</b> .	
9.	Po ukončení instalace klikněte na tlačítko <b>Finish</b> .	

#### 4.5. Stažení SW pro správu Certifikačního Tokenu

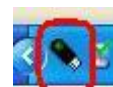
1.	Dále vyberte soubor s SW pro Certifikační Token. V prvním dialogovém okně klikněte na tlačítko <b>Uložit soubor</b> .	
----	---	--

<p>2.</p>	<p>Program Vás vybědne k zadání adresáře pro uložení souboru – zadejte adresář a klikněte na tlačítko <b>Uložit</b>. <b>Název ani typ souboru neměňte!!!</b></p>	
<p>3.</p>	<p>Následně se zobrazí informace o úspěšném ukončení stahování souboru – instalaci spusťte tlačítkem <b>Spustit</b>.</p>	
<p>4.</p>	<p>Systém zobrazí dotaz, zda chcete SW spustit – potvrďte tlačítkem <b>Spustit</b>.</p>	



<p>5.</p>	<p>Spustí se průvodce instalací. Na první obrazovce průvodce klikněte na tlačítko <b>Další</b>.</p>	
<p>6.</p>	<p>Na následující obrazovce spustte instalaci SW tlačítkem <b>Instalovat</b>.</p>	
<p>7.</p>	<p>Po ukončení instalace klikněte na tlačítko <b>Dokončit</b>.</p>	

Po úspěšné instalaci se v pravém dolním rohu PC zobrazí ikona Certifikačního Tokenu.



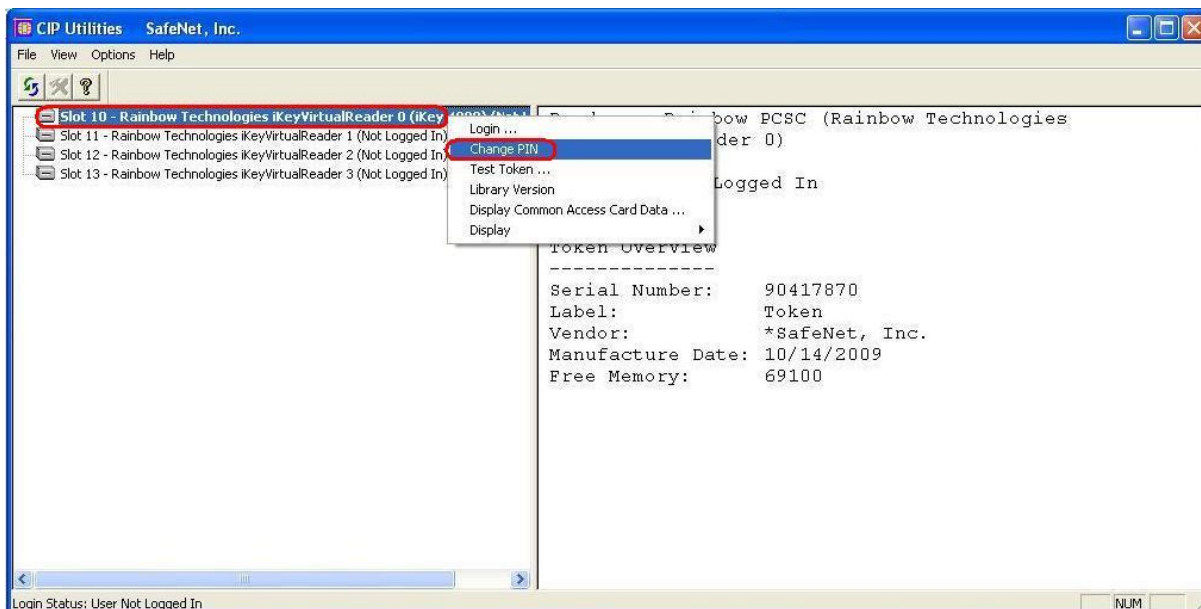
**Nyní restartujte PC.**

#### 4.6. Změna PIN k Certifikačnímu Tokenu

Po restartování PC si změňte defaultně přednastavený PIN pro přístup k Certifikačnímu Tokenu. Pokud si PIN nezměníte, nebudete si moci vygenerovat Certifikát – Certifikační centrum při pokusu o generování Certifikátu zobrazí tuto informaci.

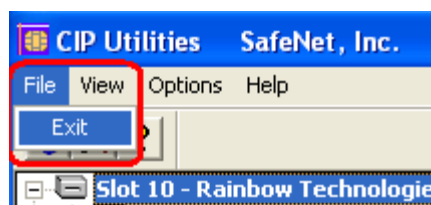


Pro změnu PIN vložte Certifikační Token do PC a spusťte SW pro Certifikační Token (Start, Všechny programy, SafeNet, Borderless Security PK, SafeNet CIP Utilities). Po otevření SW klikněte pravým tlačítkem myši na první řádek ze seznamu. Ze zobrazené nabídky klikněte na volbu **Change PIN**.



Do pole **Staré heslo** zadejte defaultně přednastavený PIN, do polí **Nové heslo** a **Opakovat nové heslo** zadejte nový PIN. PIN musí mít šest až dvacet míst, může obsahovat pouze alfanumerické znaky bez diakritických znamének, z toho minimálně jedno velké písmeno, minimálně jedno malé písmeno a minimálně jednu číslici. Změnu potvrďte tlačítkem **OK**.

PIN si můžete tímto způsobem kdykoli opět změnit – nový PIN se nesmí opakovat. Program poté ukončete volbami **File** a **Exit**.



Pokud byste chtěli Certifikační Token používat na jiném PC, je nutné si na tento PC opět nainstalovat ovladače a SW pro Certifikační Token.

#### 4.7. Vygenerování Certifikátu

Pro vygenerování Certifikátu se opět přihlaste na internetové stránky Certifikačního centra (<https://ibcc.ppfbanka.cz>) a klikněte na volbu **Přihlášení do Certifikačního centra prvotním heslem**.

Na přihlašovací obrazovce do pole **Uživatelské jméno** zadejte přístupové jméno do Certifikačního centra (obálka **přístupové jméno do Certifikačního centra**) a do pole **Heslo** zadejte přístupové heslo do Certifikačního centra (obálka **přístupové heslo do Certifikačního centra**). Obě tyto obálky jste obdrželi po podpisu smluvní dokumentace. Zadání potvrďte tlačítkem **Přihlásit**.

Automaticky se vybere volba **Vytvoření nového certifikátu**. Certifikační centrum zobrazí jméno a adresu Uživatele, jméno Uživatele je zároveň zobrazeno v levém horním rohu aplikace. V poli **Jméno certifikátu** je přednastaven název, pod kterým bude Certifikát uložen na Certifikační Token. **Toto jméno doporučujeme změnit** – v názvu Certifikátu nesmí být použita diakritika ani speciální znaky (např. + \* ? atd.). Do pole PIN zadejte PIN k Certifikačnímu Tokenu a klikněte na tlačítko **Generovat**.

**Vytvoření nového certifikátu**

Jméno a příjmení: SERVÁČ STŘEDEČNÍ  
Adresa: 110 00 PRAHA 1  
V CELNÍCI 1031/4

Typ uložení certifikátů: Electronic key

Název certifikátu: Servac 17 04 2012

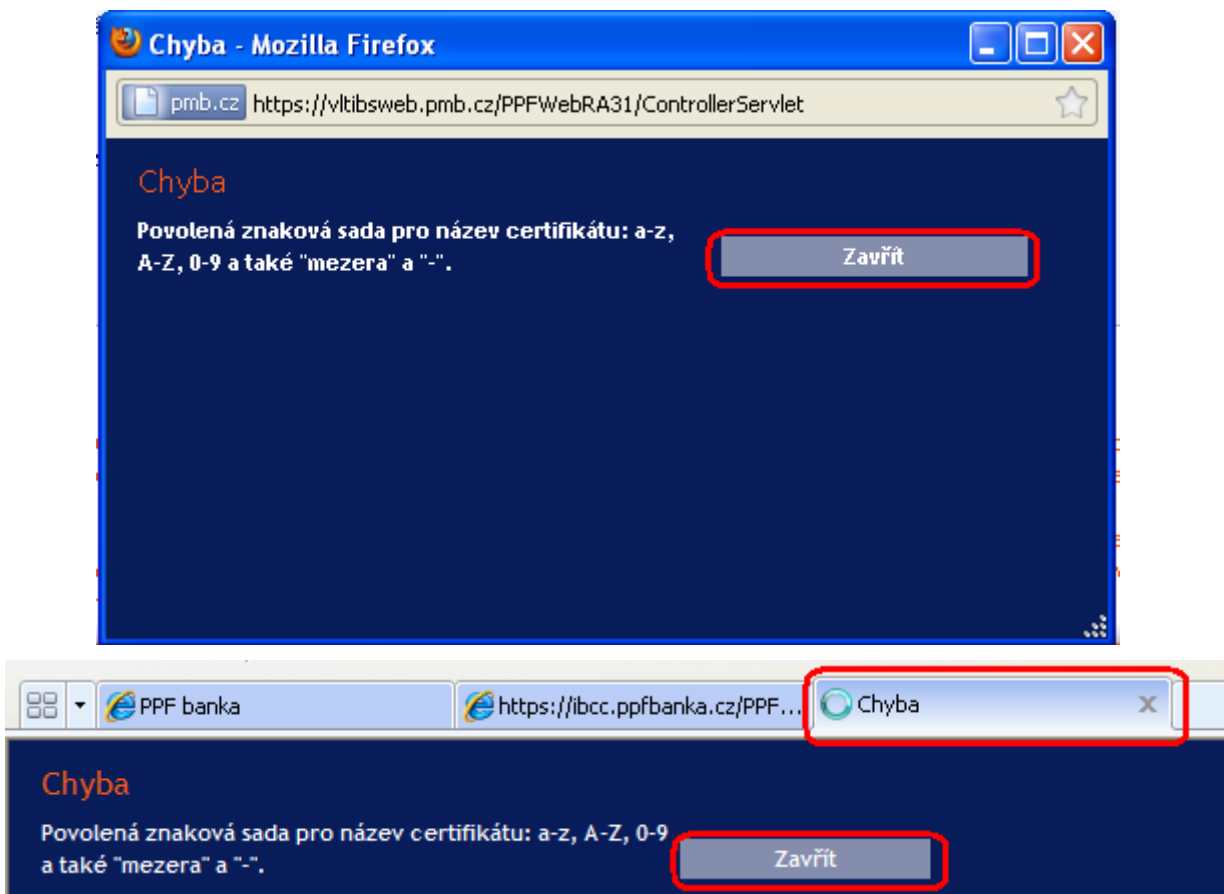
PIN: \*\*\*\*\*

**Generovat**

Pokud již využíváte podobné šifrovací zařízení od jiného dodavatele nebo banky, doporučujeme nejdříve odpojit tato zařízení alespoň po dobu generování a ukládání certifikátu. V případě že tak neučiníte, je možné, že se certifikát nepodaří nainstalovat.

PIN tokenu bude požadován při každém přihlášení, autorizaci příkazů a ostatních aktivních pokynů pro banku. Prosím zapamatujte si tento PIN nebo uschovejte pečlivě na nepřístupném místě mimo dosah tokenu. PIN je možné měnit pomocí programového vybavení (sw CIP utilities), které je nainstalováno ve Vašem PC.

Pokud název Certifikátu obsahuje nepovolené znaky, Certifikační centrum zobrazí okno nebo záložku s informací o povolené znakové sadě. Toto okno zavřete tlačítkem **Zavřít**, název Certifikátu opravte a znovu klikněte na tlačítko **Generovat**.



Certifikační centrum vygeneruje a zobrazí Certifikát. **!!! POZOR !!! Generování trvá cca 1 minutu a po celou dobu generování Certifikátu je činnost systému identifikována grafickým symbolem ve tvaru blikajících barevných čtverečků. Během generování neodcházejte od PC ani v daném okně prohlížeče neprovádějte žádné jiné činnosti!!!**

Pro uložení vygenerovaného Certifikátu na Certifikační Token zadejte PIN do pole **PIN** a klikněte na tlačítko **Uložit**.

### Vytvoření nového certifikátu

Sériové číslo:	2C5C (11356)
Vydán:	EMAIL=info@ppfbanka.cz,CN=PPFBWEBRA,OU=InternetBanking,O=PPF banka a.s.,L=Prague,ST=Czech Republic,C=CZ
Vydán pro:	O=TESTOVACÍ KLIENT S.R.O. (IBS),L=110 00 PRAHA 1,L=V CELNICI 1031/4,CN=uid: 48363,CN=SERVÁČ STŘEDEČNÍ
Platnost od:	17.04.2012 16:32
Platnost do:	17.04.2013 16:32
Otisk:	4E:A7:37:7F:B8:20:36:AC:E6:A4:FC:B2:28:4B:6B:A2
PIN:	<input style="width: 100%; border: 1px solid #ccc;" type="password" value="••••••"/>

Následně se zobrazí informace o úspěšném uložení Certifikátu.

### Certifikát byl úspěšně uložen

Certifikát č. 11356 byl úspěšně uložen.  
Informace o certifikátu je možné zobrazit v menu "Seznam platných certifikátů".

Pokud kliknete na volbu **Seznam platných certifikátů**, jsou zobrazeny detaily Certifikátu.

SERVÁČ STŘEDEČNÍ
Odhlásit

- Vytvoření nového certifikátu
- Seznam platných certifikátů
- Seznam zneplatněných certifikátů
- Uživatelská příručka

#### Seznam platných certifikátů

Sériové číslo:	2C5C (11356)
Vydán:	EMAIL=info@ppfbanka.cz,CN=PPFBWEBRA,OU=InternetBanking,O=PPF banka a.s.,L=Prague,ST=Czech Republic,C=CZ
Vydán pro:	O=TESTOVACÍ KLIENT S.R.O. (IBS),L=110 00 PRAHA 1,L=V CELNICI 1031/4,CN=uid: 48363,CN=SERVÁČ STŘEDEČNÍ
Platnost od:	17.04.2012 16:32:31
Platnost do:	17.04.2013 16:32:31
Otisk:	4E:A7:37:7F:B8:20:36:AC:E6:A4:FC:B2:28:4B:6B:A2

Platný Certifikát zde můžete prohlížet (např. zjistit, do kdy je Certifikát platný, abyste si včas vygenerovali nový Certifikát), zneplatnit (kliknutím na tlačítko **Zneplatnit**) nebo obnovit (kliknutím na tlačítko **Obnovit**). Tlačítkem **Odhlásit** v pravém horním rohu se z Certifikačního centra odhlásíte.

Pokud v Certifikačním centru delší dobu nepracujete, budete automaticky odhlášeni. Pokud chcete v Certifikačním centru dále pracovat, klikněte na tlačítko **Nové přihlášení**. Nové přihlášení provedte podle bodu [4.8](#). Pokud již v práci v Certifikačním centru pokračovat nechcete, klikněte na tlačítko **Konec**.

Z důvodu nečinnosti Vás systém automaticky odhlásil.

Pro pokračování v práci s Certifikačním centrem proveďte prosím opětovné přihlášení.

Nové přihlášení Konec

Nyní se můžete přihlásit do IB a po zaregistrování Certifikátu (viz část I. Uživatelské příručky) jej začít využívat.

Před vypršením platnosti Certifikátu je nutné si jej obnovit dle bodu [4.8.](#) **Pokud si Certifikát neobnovíte včas, budete si muset vyžádat z Banky nové přístupové údaje do Certifikačního centra jako při prvním generování Certifikátu.**

## 4.8. Obnovení Certifikátu

Před uplynutí platnosti Certifikátu si musíte vygenerovat Certifikát nový. V tomto případě se přihlaste do Certifikačního centra (<https://ibcc.ppfbanka.cz>) a zvolte **Přihlášení do Certifikačního centra pomocí certifikátu**. Následně do pole **Vložte PIN** zadejte PIN k Certifikačnímu Tokenu a klikněte na tlačítko **Nahrát certifikát**. Poté vyberte Certifikát v poli **Certifikát** a klikněte tlačítko **Přihlásit**.

Automaticky se zobrazí volba **Vytvoření nového certifikátu** stejně jako při generování nového Certifikátu (viz bod [4.7.](#)). Pro obnovení stávajícího Certifikátu můžete rovnou zadat název nového Certifikátu, PIN a začít Certifikát generovat stejně jako v bodě [4.7.](#) – původní Certifikát se automaticky zneplatní a bude nahrazen nově vygenerovaným Certifikátem.

**Jméno nového Certifikátu doporučujeme změnit, aby se jeho název neshodoval s názvem již neplatného Certifikátu** – v takovém případě byste mohli mít problém s přihlášením do IB nebo s autorizací Platebních příkazů a žádostí pro Banku.

Dále postupujte stejně jako při vygenerování prvního Certifikátu (viz bod [4.7.](#)).

Druhou možností pro obnovu Certifikátu je kliknout na volbu **Seznam platných certifikátů**. Po kliknutí na volbu **Seznam platných certifikátů** se zobrazí seznam platných Certifikátů s tlačítky **Zneplatnit** a **Obnovit**.

- 3 Vytvoření nového certifikátu
- 4 Seznam platných certifikátů
- 5 Seznam zneplatněných certifikátů
- 6 Uživatelská příručka

### Seznam platných certifikátů

Sériové číslo: 2C5C (11356)

Vydán: EMAIL=info@ppfbanka.cz,CN=PPFBWEBRA,OU=InternetBanking,O=PPF banka a.s.,L=Prague,ST=Czech Republic,C=CZ

Vydán pro: O=TESTOVACÍ KLIENT S.R.O. (IBS),L=110 00 PRAHA 1,L=V CELNICI 1031/4,CN=uid: 48363,CN=SERVÁC STŘEDEČNÍ

Platnost od: 17.04.2012 16:32:31

Platnost do: 17.04.2013 16:32:31

Otisk: 4E:A7:37:7F:B8:20:36:AC:E6:A4:FC:B2:28:4B:6B:A2

Zneplatnit
Obnovit

#### **Tlačítko *Zneplatnit* nepoužívejte!**

Pro obnovení Certifikátu klikněte na tlačítko **Obnovit** – zobrazí se obrazovka pro generování nového Certifikátu. Do pole **Název certifikátu** zadejte název nového Certifikátu, do pole **PIN** zadejte PIN k Certifikačnímu Tokenu a klikněte na tlačítko **Generovat**.

### Obnova platnosti certifikátu

Jméno a příjmení: SERVÁC STŘEDEČNÍ

Adresa: 110 00 PRAHA 1  
V CELNICI 1031/4

Název certifikátu:

PIN:

Generovat

Pokud již využíváte podobné šifrovací zařízení od jiného dodavatele nebo banky, doporučujeme nejdříve odpojit tato zařízení alespoň po dobu generování a ukládání certifikátu. V případě že tak neučiníte, je možné, že se certifikát nepodaří nainstalovat.

PIN tokenu bude požadován při každém přihlášení, autorizaci příkazů a ostatních aktivních pokynů pro banku. Prosím zapamatujte si tento PIN nebo uschovejte pečlivě na nepřístupném místě mimo dosah tokenu. PIN je možné měnit pomocí programového vybavení (sw CIP utilities), které je nainstalováno ve Vašem PC.

Poté se zobrazí detaily vygenerovaného Certifikátu. Pro jeho uložení do pole **PIN** zadejte PIN k Certifikačnímu Tokenu a klikněte na tlačítko **Uložit**.

## Vytvoření nového certifikátu

Sériové číslo: 2C5D (11357)

Vydán: EMAIL=info@ppfbanka.cz,CN=PPFBWEBRA,OU=InternetBanking,O=PPF banka a.s.,L=Prague,ST=Czech Republic,C=CZ

Vydán pro: O=TESTOVACÍ KLIENT S.R.O. (IBS),L=110 00 PRAHA 1,L=V CELNICI 1031/4,CN=uid: 48363,CN=SERVÁC STŘEDEČNÍ

Platnost od: 17.04.2012 16:42

Platnost do: 17.04.2013 16:42

Otisk: 91:09:CF:1B:B2:94:2A:BC:C0:DC:1E:37:D8:02:B1:17

PIN:

**Uložit**

Následně se zobrazí informace o úspěšném uložení Certifikátu.

## Certifikát byl úspěšně uložen

Certifikát č. 11357 byl úspěšně uložen.  
Informace o certifikátu je možné zobrazit v menu "Seznam platných certifikátů".

Ve volbě **Seznam zneplatněných certifikátů** si můžete prohlédnout detaily již neplatných Certifikátů.

- Vytvoření nového certifikátu
- Seznam platných certifikátů
- Seznam zneplatněných certifikátů
- Uživatelská příručka

### Seznam zneplatněných certifikátů

**!** Platnost zrušena: 17.04.2012 16:42:31

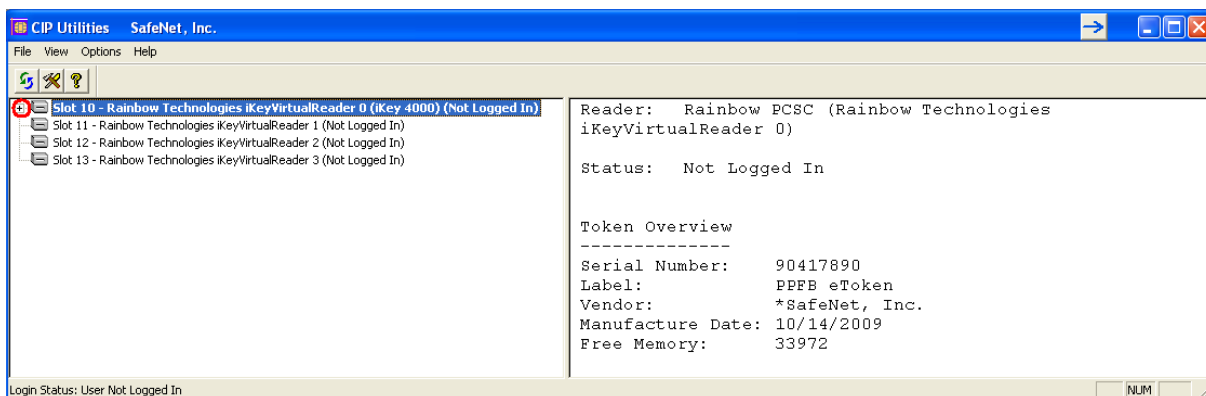
Sériové číslo:	2C5C (11356)
Vydán:	EMAIL=info@ppfbanka.cz,CN=PPFBWEBRA,OU=InternetBanking,O=PPF banka a.s.,L=Prague,ST=Czech Republic,C=CZ
Vydán pro:	O=TESTOVACÍ KLIENT S.R.O. (IBS),L=110 00 PRAHA 1,L=V CELNICI 1031/4,CN=uid: 48363,CN=SERVÁC STŘEDEČNÍ
Platnost od:	17.04.2012 16:32:31
Platnost do:	17.04.2013 16:32:31
Otisk:	4E:A7:37:7F:B8:20:36:AC:E6:A4:FC:B2:28:4B:6B:A2

Již neplatné Certifikáty doporučujeme z Certifikačního Tokenu smazat – zabráníte tak použití neplatného Certifikátu při přihlašování do IB, resp. při autorizaci.

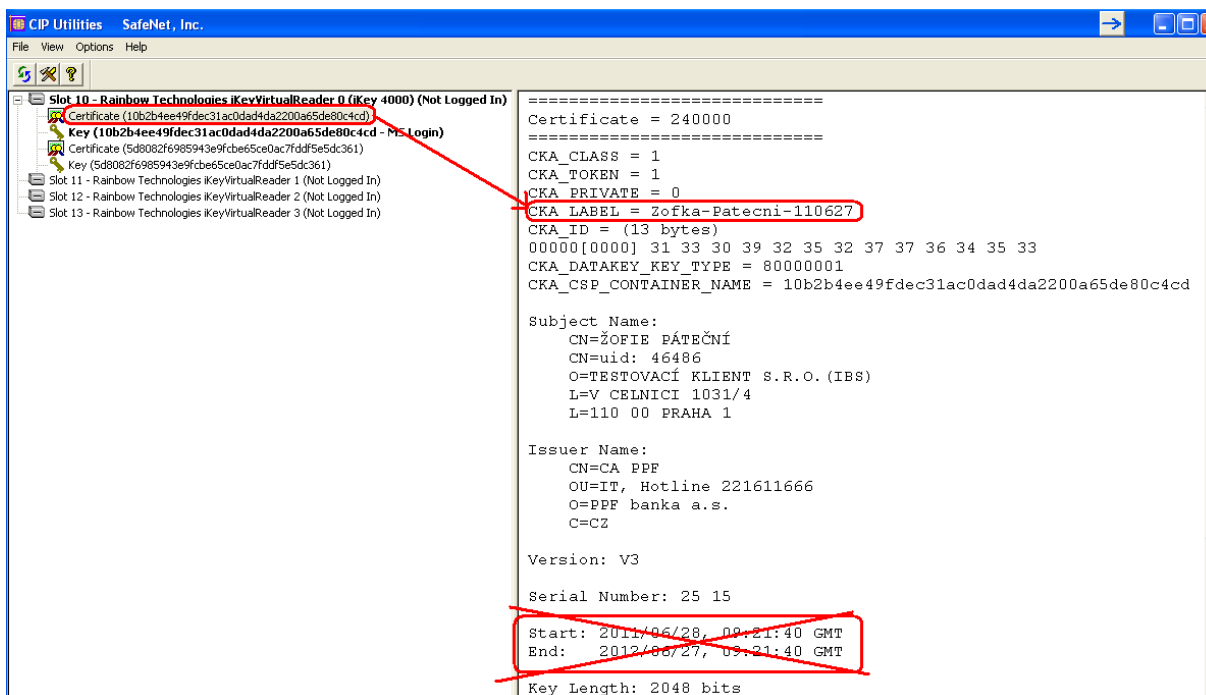
## 4.9. Smazání neplatného Certifikátu

Pro smazání neplatného Certifikátu vložte Certifikační Token do PC a spusťte SW pro Certifikační Token (Start, Všechny programy, SafeNet, Borderless Security PK, SafeNet CIP Utilities). Po otevření SW klikněte na křížek u řádku – „Slotu“ v levé části obrazovky. Může se stát, že je každý Certifikát uložen v jiném Slotu – pak je křížek zobrazen před každým Slotem, ve kterém je Certifikát uložen, a pro smazání neplatného Certifikátu je nutné zkontrolovat všechny takto označené Sloty.

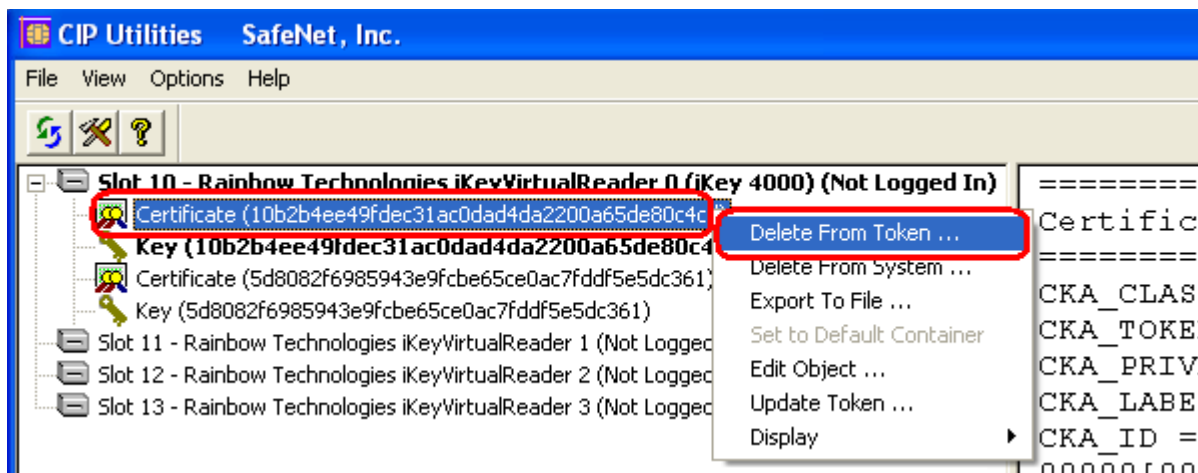




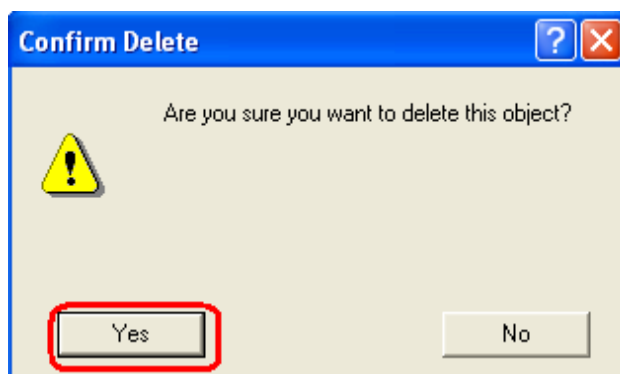
Po kliknutí na křížek se rozbalí seznam všech Certifikátů uložených na Certifikačním Tokenu ve vybraném Slotu (na Certifikačním Tokenu by měly být uloženy pouze dva Certifikáty – jeden platný a jeden neplatný). Klikněte na řádek s Certifikátem – na pravé straně obrazovky se zobrazí jeho details. Při mazání neplatného Certifikátu se vždy řiďte jeho názvem (pole **CKA LABEL**), nikoli údaji o platnosti Certifikátu (pole **Start** a **End**) – tyto údaje se odvíjí od data vygenerování Certifikátu a zejména údaj o konci platnosti nemusí být aktuální.



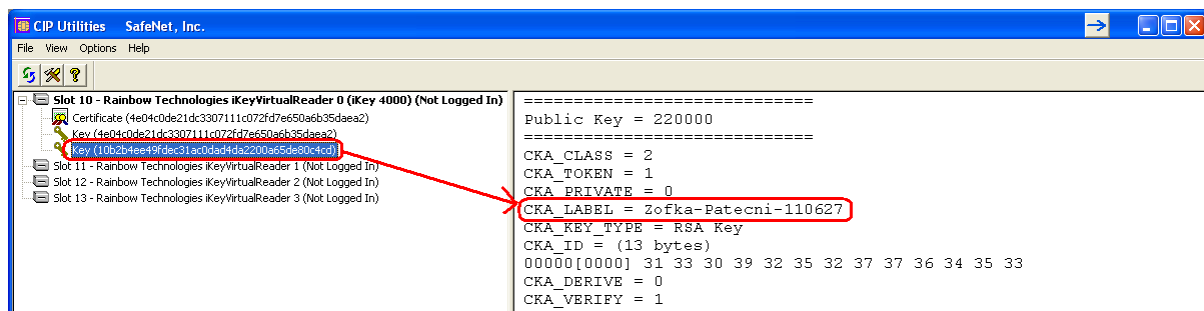
Vyberte neplatný Certifikát a klikněte na něj pravým tlačítkem myši. Ze zobrazené nabídky klikněte na volbu **Delete From Token**.



Zobrazí se dotaz, zda si skutečně přejete smazat Certifikát z Certifikačního Tokenu – klikněte na tlačítko Yes.



**!!! POZOR !!! Smazání Certifikátu trvá několik sekund!!!** Po dobu jeho mazání neprovádějte žádné další akce na PC. Po smazání neplatného Certifikátu se elektronický klíč ke smazanému Certifikátu zařadí za elektronický klíč k platnému Certifikátu.



Program poté ukončete volbami File a Exit.

