

# Obnova certifikátu Uživatelská příručka pro prohlížeč Mozilla **Firefox**

První certifikační autorita, a.s. 1.8.2011 Verze 7.07



# Obsah

1.		Úvo	d		3
2.		Poža	adavk	ky na software	1
3.		Inst	alace	kořenového certifikátu I.CA	5
4.		Proc	ces ob	bnovy certifikátu	3
	4.	1.	Kon	trola softwarového vybavení 8	3
		4.1.	1.	Nepodporovaný operační systém	Э
		4.1.	2.	Nepodporovaný internetový prohlížeč	Э
		4.1.	3.	Podpora JavaScriptu	Э
		4.1.	4.	Podpora Java Runtime Environment (JRE)10	)
		4.1.	5.	Nainstalovaný Java Applet ICApki1	1
		4.1.	6.	Ukládání cookies	2
	4.	2.	Výb	ěr certifikátu pro obnovu (volitelné)13	3
	4.	3.	Dop	lnění a změna některých údajů14	1
	4.	4.	Kon	trola zadaných údajů	5
	4.	5.	Gen	erování žádosti o obnovu	7
		4.5.	1.	SecureStoreCSP	7
		4.5.	2.	Microsoft Enhanced RSA and AES Cryptographic Provider se silnou ochranou	
		soul	krom	ého klíče	7
	4.	6.	Pod	pis a odeslání žádosti o obnovu	Э
5.		Inst	alace	Java Runtime Environment (JRE)	1
	5.	1.	Spu	štění instalace JRE pod prohlížečem Mozilla Firefox22	1
6.		Insta	alačn	í program JRE 23	3
7.		Řeše	ení pr	roblémů	5
				ND *	
				•	



# 1. Úvod

Tento dokument slouží jako návod, jak postupovat při obnově certifikátu přes webové stránky.

<text>



# 2. Požadavky na software

Počítač, na kterém se bude provádět generování žádosti o certifikát, musí splňovat následující požadavky:

- Musí mít nainstalovaný a spuštěný operační systém
  - Microsoft Windows XP
  - o Windows Vista
  - o Windows 7
- Musí být nainstalován a použit některý z následujících prohlížečů (pro generování žádosti)
  - Microsoft Internet Explorer (verze 7 a výše).
  - o Mozilla Firefox (verze 3 a výše)
  - Google Chrome (verze 2 a výše)
  - Apple Safari (verze 4 a výše)
  - o **Opera** (verze 10 a výše)
- Musí mít nainstalovaný software Java Runtime Environment (dále JRE), alespoň verze 1.6.0\_21, který je potřebný pro správnou funkci webových stránek pro generování žádosti o certifikát.
  - Doporučujeme používat nejaktuálnější verzi JRE.
  - Přítomnost tohoto softwaru detekují stránky automaticky, pokud zjistí, že software přítomen není, vybídnou uživatele k jeho stažení/instalaci.
  - V případě, že máte nainstalovanou starší verzi JRE, nežli je uvedená v požadavcích, odinstalujte ji před zahájením generování žádosti o certifikát. Následně budete stránkami nasměrováni na stažení nejaktuálnější verze.
- Ve vašem internetovém prohlížeči musíte mít zapnutou podporu skriptování Javascript , zapnutou podporu jazyku Java, podporu ukládání cookies.

¢ N



# 3. Instalace kořenového certifikátu I.CA

Při spuštění stránky pro obnovu certifikátu vás může váš prohlížeč upozornit, že vstupujete na nedůvěryhodné stránky. Tento problém je způsoben tím, že nemáte uloženy v úložišti kořenové certifikáty I.CA.

Zadejte do prohlížeče následující URL: http://www.ica.cz/SHA2-Komercni.aspx

Zobrazí se vám následující stránka:



Pod nadpisem **Kořenový certifikát certifikační autority pro vydávané komerční certifikáty SHA2** klikněte na **DER**. Zobrazí se vám dialog pro stažení souboru. Soubor obsahující certifikát uložte na Váš pevný disk.

V prohlížeči Mozilla Firefox na nástrojové liště zvolte Nástroje a klikněte na nabídku Možnosti...



<u>S</u> oubor Úpr <u>a</u> vy <u>Z</u> obrazení <u>H</u> istorie Zál <u>o</u> žky	<u>Nástroje</u> Nápo <u>v</u> ěda
C X 🏠 🚺 ica.cz htt	Hledání na <u>w</u> ebu Ctrl+K
🔊 Nejnavštěvovanější 🥮 Jak začít 🔜 Přehled z	Správce s <u>t</u> ahování Ctrl+J Správce <u>d</u> oplňků
	Java Console
	Firebug •
	Chybová konzola Ctrl+Shift+J
	Možnosti HTML Validator
	Informace o stránce
	Monitor with <u>F</u> iddler
	Spustit anonymní prohlížení Ctrl+Shift+P
	Vymazat nedávnou <u>h</u> istorii Ctrl+Shift+Del
	<u>M</u> ožnosti
	Tamper Data

Zvolte Rozšířené, vyberte záložku Šifrování a klikněte na tlačítko Certifikáty.

Zvolte záložku Autority a klikněte na tlačítko Importovat...

Jméno certifikátu	Bezpečnostní zařízení	E.
(c) 2005 TÜRKTRUST Bilgi İletişim ve Bilişim Güven	liği Hizm	
TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcı AC Camerfirma SA CIF A82743287	sı Builtin Object Token	
Chambers of Commerce Root	Builtin Object Token	
Global Chambersign Root	Builtin Object Token	
AddTrust AB		
AddTrust External CA Root	Builtin Object Token	
AddTrust Class 1 CA Root	Builtin Object Token	
AddTrust Public CA Root	Builtin Object Token	
AddTrust Qualified CA Root	Builtin Object Token	+
COMODO Cartification Authority	Softu harn tačízaní	-
Zobrazit Upravit Importovat E	xportovat <u>S</u> mazat	

Vyberte certifikát, který jste uložili na pevný disk.

Zatrhněte Uznat tuto CA pro identifikaci serverů, Uznat tuto CA pro identifikaci uživatelů pošty a Uznat tuto CA pro identifikaci výrobců software. Stiskněte OK.

0



provide design and the second se	
Stažení certifikátu	×
Byli jste požádáni o uznání nové Certifikační Autority (CA).	
Chcete uznat "I.CA - Standard Certification Authority, 09/2009" pro následující	účely?
📝 Uznat tuto CA pro identifikaci serverů.	
📝 Uznat tuto CA pro identifikaci uživatelů pošty.	
🔽 Uznat tuto CA pro identifikaci výrobců software.	
Před uznáním této CA, a to pro jakýkoliv účel, byste měli prozkoumat její certifi podmínky (pokud jsou dostupné).	ikát, její pravidla a
Zobrazit Zobrazit certifikát CA	
ОК	Zrušit
Možnosti Obecné Panely Obsah Aplikace Soukromi Zabezpečeni Rozšiřené Obecné Siť Aktualizace Sifrování Protokoly Použít SSL <u>2.0</u> Použít TLS <u>1.0</u> Certifikáty Pokud server vyžaduje osobní certifikát: © Zvolit <u>a</u> utomaticky <b>©</b> Vž <u>d</u> y se dotázat Certifikáty Zneplatnění Qvěřování <u>B</u> ezpečnostní zařízení	
OK Zrušit Nápo <u>v</u> ěda	



# 4. Proces obnovy certifikátu

Postup generování žádosti o obnovu certifikátu je rozdělen do několika kroků:

- Kontrola softwarového vybavení
- Výběr certifikátu pro obnovu (volitelné)
- Doplnění a změna některých údajů
- Kontrola zadaných údajů
- Generování žádosti o obnovu
- Podpis a odeslání žádosti o obnovu

# 4.1.Kontrola softwarového vybavení

Pro usnadnění kontroly připravenosti Vašeho počítače pro obnovu certifikátu, je při zahájení obnovy zobrazena kontrolní stránka, která ověří přítomnost klíčových softwarových komponent.

		-
CERTIFICATION AUTHORITY autorita A.S.	<sup>ační</sup> Obnova certifikátu	and the
Nejdříve je nutné otestovat, zda Váš PC webové aplikaci. Test zahajíte tlačítkem 2	splňuje minimální požadavky pro bezproblémové dokončení procesu obnovy certifikátu v této Zahájit test PC.	
	Zahájit test PC	
	Copyright I CA 2000-2011 All Right Reserved   První gertifikační autorita a s   Kontakty	
Kliknutím na tlačítko <b>Zahájit te</b>	est PC, spustíte test Vašeho počítače.	



Stránka otestuje počítač, test může trvat desítky sekund, a ohlásí, zdali je něco v nepořádku, případně vypíše chybové hlášení. Pokud nejsou detekovány problémy, kliknutím na tlačítko **Zahájit obnovu certifikátu** přejdete k samotné obnově certifikátu.

Pokud se při kontrole vyskytne chyba, nelze pokračovat v obnově certifikátu. Nejdříve je potřeba odstranit chybu, která znemožňuje obnovu. Význam chybových hlášení je uvedený v následujících kapitolách.

#### 4.1.1.Nepodporovaný operační systém

Pro generování žádosti musíte použít jeden z operačních systémů uvedených v kapitole 2.

#### 4.1.2.Nepodporovaný internetový prohlížeč

Pro generování žádosti musíte použít jeden z prohlížečů uvedených v kapitole 2.

#### 4.1.3.Podpora JavaScriptu

Stránky pro generování žádosti o certifikát vyžadují podporu skriptování v jazyku JavaScript. Všechny podporované prohlížeče mají tuto podporu automaticky povolenu. Pokud by tato kontrola selhala, znamená to s největší pravděpodobností, že je v nastavení prohlížeče podpora scriptování vypnuta. Povolte podporu skriptování v jazyku JavaScript ve Vašem prohlížeči.



#### 4.1.3.1.Povolení JavaScriptu v Mozilla Firefox

Na nástrojové liště zvolte Nástroje a klikněte na nabídku Možnosti...

<u>S</u> oubor Úpr <u>a</u> vy <u>Z</u> obrazení <u>H</u> istorie Zál <u>o</u> žky	<u>N</u> ást	roje Nápo <u>v</u> ěda	
C X 🏠 🚺		Hledání na <u>w</u> ebu	Ctrl+K
🔊 Nejnavštěvovanější 🥮 Jak začít 🔊 Přehled z		Správce s <u>t</u> ahování Správce <u>d</u> oplňků	Ctrl+J
		Java Console	
		Firebug	•
		<u>C</u> hybová konzola	Ctrl+Shift+J
		Možnosti HTML Validator	
		Informace o stránce	
		Monitor with <u>F</u> iddler	•
		Spustit anonymní prohlížení	Ctrl+Shift+P
		Vymazat nedávnou <u>h</u> istorii	Ctrl+Shift+Del
		<u>M</u> ožnosti	
		Tamper Data	

Zvolte záložku Obsah a zatrhněte Povolit JavaScript a klikněte na tlačítko OK.

☑ <u>B</u> lokov ☑ Načíst	vat vyskak	ovací okna				Výji <u>m</u> ky	1
V Povoli	it Java <u>S</u> crip	ot				<u>R</u> ozšířené…	
Písma a Ba √ýchozí <u>p</u> i	arvy ísmo: Ti	mes New Ro	oman	▼ V <u>e</u> lil	cost: 16 💌	R <u>o</u> zšířené B <u>a</u> rvy	
azyky Zvolit jazy	ky pro zoł	razování we	bových str	ánek.		/ybrat jazyky	

#### 4.1.4.Podpora Java Runtime Environment (JRE)

Tyto stránky vyžadují pro svou funkčnost nainstalovanou podporu jazyka Java. Ujistěte se, že nemáte ve svém prohlížeči tuto podporu vypnutou. Pokud nemáte na svém počítači JRE nainstalováno, měl by vás prohlížeč vybídnout ke stažení a instalaci JRE. Pokud se tak nestalo, klikněte na odkaz uvedený na stránce a manuálně stáhněte a nainstalujte aktuální verzi JRE. V každém případě bude po instalaci JRE nutno zavřít a znovu spustit prohlížeč, aby se změny projevily.

Instalace JRE je popsána v Kapitole5.

#### 4.1.4.1.Povolení Java v Mozilla Firefox

Na nástrojové liště zvolte Nástroje a klikněte na nabídku Správce doplňků.



oubor Úpr <u>a</u> vy <u>Z</u> obrazení <u>H</u> istorie Zál <u>o</u> žky <mark>N</mark>	ástroje Nápo <u>v</u> ěda	
🔇 🕞 🗸 🤂 🎯 http://su	Hledání na <u>w</u> ebu	Ctrl+K
Nejnavštěvovanější 🥮 Jak začít 🔊 Přehled 🛥	Správce stahování	Ctrl+J
Žádost o certifikát	Správce <u>d</u> oplňků	
	Java Console Firebug <u>C</u> hybová konzola Možnosti HTML Validator Informace o stránce Monitor with <u>F</u> iddler	ا Ctrl+Shift+J
	Spustit <u>a</u> nonymní prohlížení Vymazat nedávnou <u>h</u> istorii	Ctrl+Shift+P Ctrl+Shift+Del
	<u>M</u> ožnosti	
	Tamper Data	

Zvolte záložku **Rozšíření**, vyberte položku **Java** a klikněte na **Povolit**. Aby se změna projevila, je nutné restartovat Firefox.

(ískat nové doplňky	Rozšíření Motivy vzhledu Zásuvné modu	ly .
📑	60.20	
Java Console	6.0.22	
Java Console	6.0.23	
Možnosti	11.0.1	

#### 4.1.5.Nainstalovaný Java Applet ICApki

V tomto místě se kontrolní stránka pokusí nainstalovat Java Applet ICApki, který je nutný pro funkčnost stránek pro generování žádosti o certifikát. Při první instalaci appletu na počítač, kde probíhá generování žádosti o certifikát, budete vyzváni k potvrzení důvěry vydavateli Java Appletu. Vydavatelem appletu je První certifikační autorita a.s. Důvěru appletu potvrdíte dialogem, který znázorňuje následující obrázek. V tomto dialogu je důležité zaškrtnout volbu **Always trust content from this publisher** a poté použít tlačítko **Yes**.



Warning - Security The web site's certificate cannot be verified.	Do you
want to continue?	
Name: tbica.ica.cz	
Publisher: tbica.ica.cz	
Always trust content from this publisher.	
	Yes No
The certificate cannot be verified by a trusted source.	More Information

Následuje druhý dialog, kde se postupuje obdobně, a sice zaškrtne se volba **Always trust content from this publisher** a poté se použije tlačítko **Run**.

lhe applie Do you wa	cation's digital signature has been v ant to run the application?	verified.
Name:	ICApki	
Publisher:	I.CA - Code Signing	
From:	https://tbica.ica.cz	
V Always	trust content from this publisher.	
		Run Cancel
â .		

Při dalším spuštění stránek na počítači, kde tato instalace proběhla, již nebudete k opětovnému potvrzování Java Appletu ICApki vyzýváni.

V případě, že bude vydána nová verze Java Appletu ICApki, bude klientem v tomto místě okamžitě automaticky stažena a nainstalována. Tato instalace může chvíli trvat. Po jejím skončení budou stránky pokračovat v normální práci.

#### 4.1.6.Ukládání cookies

Pro správnou práci stránek pro generování žádostí je nutné, aby váš prohlížeč umožnil stránce ukládat cookies. Pokud máte zakázáno ukládání cookies, povolte jej.



#### 4.1.6.1.Povolení cookies v Mozilla Firefox

Na nástrojové liště zvolte Nástroje a klikněte na nabídku Možnosti...

Soubor Úpr <u>avy Z</u> obrazení <u>H</u> istorie Zál <u>o</u> žky	<u>Nápov</u> ěda	
C X 🏠 🚺 ica.cz htt	Hledání na <u>w</u> ebu	Ctrl+K
🔊 Nejnavštěvovanější 🥮 Jak začít 🔜 Přehled z	Správce s <u>t</u> ahování	Ctrl+J
	Správce <u>d</u> oplňků	
	Java Console	
	Firebug	+
	<u>C</u> hybová konzola	Ctrl+Shift+J
	Možnosti HTML Validator	
	Informace o stránce	
	Monitor with <u>F</u> iddler	•
	Spustit <u>a</u> nonymní prohlíže	ení Ctrl+Shift+P
	Vymazat nedávnou <u>h</u> istori	ii Ctrl+Shift+Del
	<u>M</u> ožnosti	
	Tamper Data	

Zvolte záložku Soukromí. U Nastavení historie zvolte Pamatovat si historii (případně zvolte Použít pro historii vlastní nastavení a zatrhněte Povolit serverům nastavovat cookies).

Nastavení potvrďte kliknutím na tlačítko OK.

ožnosti							x		
Obecné	Panely	) 反 Obsah	Aplikace	Soukromi	Zabezpečení	Rozšířené			
Historie Nastavení	<u>h</u> istorie:	Pamatova	ıt si historii		ŀ				
Firefo navští	x si bude j ív <mark>ených st</mark>	pamatovat ránek bude	historii strán uchovávat	iek, s <mark>tahování</mark> cookies.	, formulářů a hl	edání. U		3	
Může	te <u>vymaza</u>	t nedávnou	<u>ı historii</u> neb	oo <u>odebrat në</u> l	<u>cterá cookies</u> .				
Adresní řá	dek								
<u>P</u> ři použití	adresního	o řádku naš	eptávat: H	listorii a zálož	ky 👻	1			69
				OK	Zrušit	Nápo <u>v</u> é	èda		))°

4.2.Výběr certifikátu pro obnovu (volitelné)

Nejdříve je třeba vybrat certifikát, který chcete obnovovat.



•

Vyberte certifikát, který chcete obnovit.

#### Zvolte, kde je váš certifikát uložen (registrován)

Osobní úložiště certifikátů ve Windows

Jiné úložiště (např. I.CA čipová karta)

0

#### Certifikát

Ing. Zdeněk Test [2012-03-03][0425C1](I.CA - Development standard root certificate 2009)

Pokračovat

Pokud je Váš certifikát registrován ve Windows, nechte zvoleno **Osobní úložiště** certifikátů Windows. Pokud se nachází Váš certifikát na příklad na čipové kartě I.CA a tento certifikát nebyl zaregistrován do Windows, zvolte možnost **Jiné úložiště**.

Podle Vaší předchozí volby je Vám nabídnut seznam certifikátů, které můžete obnovit. Pokud jste zvolili možnost **Jiné úložiště**, musíte mít připojenu čtečku a vloženu čipovou kartu.

Obnovit lze pouze takové certifikáty, kterým ještě neskončila platnost a které nejsou umístěny na CRL!

Pokud obdržíte email s upozorněním na konec platnosti Vašeho certifikátu, je v tomto emailu uvedeno URL, na kterém můžete obnovit certifikát. Součástí URL je i sériové číslo certifikátu. Pokud zadáte toto URL do Vašeho prohlížeče, certifikát je pro obnovu vybrán automaticky.

# 4.3.Doplnění a změna některých údajů

V tomto kroku můžete ovlivnit některé údaje, které bude obsahovat váš obnovený certifikát.

Název položky	Vaše údaje	Popis
Certifikát		
Ko	merční certifikát 271809 (0425C1 hex)	
	Platnost do 3.3.2012 18:34:24	
	Vydavatel I.CA - Development standard root certit	icate 2009
	Stát CZ	
	Obecné jméno Ing. Zdeněk Test	
	Sériové číslo ICA - 14568	
Alternativní jméno předmětu kom	erční certifikátu	
OtherName Microsoft Universal Prin 1.3.6	ncipal Name OID: i.1.4.1.311.20.2.3	
E-m	nail (rfc822Name) hochman@ica.cz	
Nastavení obnovy certifikátu		
Heslo	pro zneplatnění	Heslo pro zneplatnění smí obsahovat pouze číslice a písmena bez dlakritiky. Dělka hesla musí být 4 až 32 znaků. Pokud nezadáte heslo bude jako heslo pro zneplatnění certifikátu použito heslo, kterým se zneplatňuje obnovovaný certifikát.
Typ úlo	žiště klíče (CSP) Microsoft Enhanced RSA and AE	S Cryptographic Provider
Povolit export :	soukromého klíče 🔽	Tato volba umožní provést export certifikátu včetně soukromého klíče. Budete moci přenášet soukromý klíč mezi úložšti. Správa klíče vyžatuje zvýšenou opatrnost z důvodu vyššiho rizika jeho krádežeznaužití.
Povolit silnou ochranu s	soukromého klíče 📝	Před každým použitím Vašeho klíče budete upozorněni, že je váš klíč používán. Nasledně máte možnost vybrat si mezi : Střední - vždy budete pouze upozorněn informativním hlašením; Silná - před každým použitím po Vas bude vyžadováno zadání hesia.
Rozšířená nastavení		
Změnit použití klíče a rozšířené použití klíče (Do uživatel na vlastní riziko.	oporučeno pro odborníky). Pokud neprovedete žádné zm	ny, bude nastavení použití klíče a rozšířeného použití klíče stejné jako u obnovovaného certifikátu. Změny provádí
Zobrazit odebírání alternativního jména předmě (Pouze položky v souladu s certifikační politikou). Z	tu (Doporučeno pro odborníky). Pokud neprovedete žádn měny provádí uživatel na vlastní riziko.	é změny, bude váš obnovený certifikát obsahovat stejná alternativní jména předmětu jako certifikát obnovovaný

Pokračovat



V části **Certifikát** jsou zobrazeny některé údaje z obnovovaného certifikátu. Zobrazeno je jeho sériové číslo, platnost, jméno vydavatele certifikátu, jednotlivé položky předmětu a všechna alternativní jména.

V části Nastavení obnovy se nachází údaje:

#### Heslo pro zneplatnění:

Pokud dojde během používání certifikátu ke kompromitaci privátního klíče, změně údajů (změna jména, bydliště...) nebo se vyskytnou další důvody, proč by neměl být certifikát dále používán, je Vaší zákonnou povinností certifikát zneplatnit. Certifikát lze zneplatnit přes webové rozhraní. Při zneplatnění budete vyzváni k zadání hesla pro zneplatnění.

Pokud nezadáte heslo, bude jako heslo pro zneplatnění certifikátu použito heslo, kterým se zneplatňuje obnovovaný certifikát.

Pokud se rozhodnete zadat jiné heslo, musí být délka hesla 4 až 32 znaků. Povoleny jsou pouze velká a malá písmena bez diakritiky a číslice.

#### Typ úložiště klíče (CSP):

U položky **Typ úložiště klíče (CSP)** zvolte z nabídky SW modul, zajišťující kryptografické služby (CSP), který vygeneruje váš privátní klíč.

#### Export privátního klíče:

Pokud Vámi zvolený typ úložiště klíče (CSP) podporuje export privátního klíče, je Vám nabídnuta volba **Povolit export privátního klíče**. Tato volba umožní provést export certifikátu včetně soukromého klíče. Soukromý klíč tak budete moci přenášet mezi úložišti. Správa klíče vyžaduje v takovém případě zvýšenou opatrnost z důvodu vyššího rizika jeho krádeže/zneužití.

#### Silná ochrana privátního klíče:

Pokud Vámi zvolený typ úložiště klíče (CSP) podporuje silnou ochranu privátního klíče, je Vám nabídnuta volba **Povolit silnou ochranu privátního klíče**. Před každým použitím Vašeho klíče budete upozorněni, že je Váš klíč používán. Následně máte možnost vybrat si mezi: Střední - vždy budete pouze upozorněn informativním hlášením; Silná - před každým použitím po Vás bude vyžadováno zadání hesla.

#### Nepovolený obsah certifikátu

V některých výjimečných případech může Váš certifikát obsahovat rozšířená použítí klíče a alternativní jména předmětu, která již nesmí být podle certifikační politiky přítomna v certifikátu. V takovém případě je zobrazeno upozornění:

Komerční certifikát Nepovolená hodnota rozšířeného použití kliče Smartcard Logon OID: 1.3.6.1.4.1.311.20.2.2 Vámi obnovovaný certifikát obsahuje v rozšířeném použití klíče položku, která není v souladu s certifikátn politikou. Pokud chcete obnovit certifikát musí být tyto položky z certifikátu odstraněny. Pokud chcete pokračovat v obnově odsouhlaste odebrání položek.

Nebo



Nepovolená hodnota rozšířených položek certifikátu

Komerční certifikát OtherName Microsoft Universal Principal Name OID: 1.3.6.1.4.1.311.20.2.3 hochman@bmo.ica.cz Souhlasim s odebráním

Várni obnovovaný certifikát obsahuje v rozšířených položkách certifikátu - položku, která není v souladu s certifikáční politikou. Pokud chcete obnovi certifikát musí být tyto položky z certifikátu odstraněny. Pokud chcete pokračovat v obnové odsouhlaste odebrání položek.

Abyste mohli pokračovat v obnově, musíte odsouhlasit odebrání nepovolených položek.

Po stisknutí tlačítka **Pokračovat** stránka provede kontrolu Vámi vyplněných údajů. Pokud některé zadané údaje nesplňují podmínky, budete vyzvání k jejich opravě. Údaje, vyžadující změnu nebo doplnění, jsou podbarveny červeně.

Pokud Vámi zadané údaje splňují podmínky, zobrazí se Vám stránka, rekapitulující Vámi zadané údaje.

# 4.4.Kontrola zadaných údajů

Na této stránce prosím zkontrolujte Vámi zadané údaje.

Zkontrolujte si prosím níže uvedené údaje. Pokud jsou níže uvedené údaje v pořádku, je možné vytvořit žádost o obnovu certifikátu.

Rekapitulace údajů	
Název položky	Zadaná hodnota
Doba platnosti certifikátu	365
Typ úložiště klíče (CSP)	Microsoft Enhanced RSA and AES Cryptographic Provider
Algoritmus miniatury	sha256WithRSAEncryption
Povolit export soukromého klíče	Ano
Povolit silnou ochranu soukromého klíče	Ano
Dělka klíče	2048
Položky předmětu	Komerční certifikát
Stát	CZ
Obecné jméno	Ing. Zdeněk Test
Sériové číslo	ICA - 14568
Rozšířené položky certifikátu	Komerční certifikát
OtherName Microsoft Universal Principal Name OID: 1.3.6.1.4.1.311.20.2.3	hochman@brno.ica.cz
E-mail (rfc822Name)	hochman@ica.cz
Použití klíče	Komerční certifikát
Non Repudiation	Ano
Digital Signature	Ano
Key Encipherment	Ano
Data Encipherment	t Ano
Key Agreement	Ano
Rozšířené použití klíče	Komerční certifikát
TLS WWW client authentication OID: 1.3.6.1.5.5.7.3.2	Ano
E-mail protection OID: 1.3.6.1.5.5.7.3.4	Ano
Smartcard Logon OID: 1.3.6.1.4.1.311.20.2.2	Ano
Vystavený certifikát zaslat na e-mail: hochman@ica.cz	
Certifikát zaslat ve formátu ZIP:	

🔘 Ano

Ne

#### Vytvořit žádost

Zadejte e-mailovou adresu, na kterou Vám bude certifikát zaslán (Položka **Vystavený certifikát zaslat na e-mail:**). Pozor: tato emailová adresa není součástí žádosti o certifikát, tudíž nebude uvedena ani v samotném certifikátu.

Kliknutím na tlačítko Vytvořit žádost spustíte generování žádosti o obnovu.



#### 4.5.Generování žádosti o obnovu

Následující postup se pro jednotlivé typy úložiště klíče (CSP) mírně liší.

#### 4.5.1.SecureStoreCSP

Pokud při vyplňování údajů o žadateli zvolíte jako typ úložiště klíče SecureStoreCSP, je postup generování žádosti následující:

Nejdříve se Vám zobrazí následující dialog. V tomto okamžiku se generuje Váš privátní klíč. Tvorba privátního klíče může trvat několik desítek sekund.

ecureStoreCSP	
probíhá prác	e s kartou

Poté, co je privátní klíč vytvořen, jste vyzváni k zadání PINu k vaší kartě.

K provedení operace je třeba zadat PIN. Operace : Podpis dat klíčem umístěným na kartě		
PIN:		
Zapamatovat PIN		
OK	Storno	

# 4.5.2.Microsoft Enhanced RSA and AES Cryptographic Provider se silnou ochranou soukromého klíče.

Pokud při vyplňování údajů o žadateli zvolíte jako typ úložiště klíče Microsoft Enhanced RSA and AES Cryptographic Provider (případně Microsoft Enhanced RSA and AES Cryptographic Provider /prototype/) a zatrhnete volbu **Povolit silnou ochranu klíče**, je postup generování žádosti následující:

Aplikace vytváří chráněnou položku.
Privátní klíč CryptoAPI
Je nastavena střední úroveň Nastavit úroveň zabezpečení.



0

Pokud kliknete na Nastavit úroveň zabezpečení..., budete moci změnit úroveň zabezpečení.

1.11	Zvolte úroveň zabezpečení požadovanou pro tuto položku.
	<ul> <li>Vysoká</li> <li>Při použití této položky požadovat oprávnění s heslem</li> </ul>
	Střední Při použití této položky požadovat oprávnění
	< Zpět Další > Stomo

Pokud zvolíte vysokou úroveň zabezpečení, budete vyzváni k zadání hesla. Toto heslo bude potřeba zadat vždy, když budete používat soukromý klíč.

20

Vytvořte heslo, jím	iž bude tato položka chráněna.
Vytvořit nové hesla Heslo pro:	o k této položce Privátní klíč CryptoAPI
Heslo: Potvrdit:	
 < Zpě	it Dokončit Storno

Po kliknutí na tlačítko **Dokončit** dojde ke změně úrovně zabezpečení. Nyní klikněte na tlačítko **OK**.



Aplikace vytváří chráněnou položku.
Privátní klíč Crypto API
Je nastavena vysoká úroveň Nastavit úroveň zabezpečení

V dalším dialogovém okně zvolte **Udělit oprávnění**. Pokud jste zvolili vysokou úroveň zabezpečení, musíte zadat i heslo.

<ul> <li>Požadovat oprávnění k použití k</li> </ul>	díče	×
Udělit nebo odepřít této a klíče	plikaci oprávnění k pou	žití tohoto
Název klíče:	Název klíče zadaný aplikací Udělit oprávnění   Odepřít oprávnění	
Heslo ochrany klíče:		
Sobrazit podrobnosti o kliči	ОК	Storno

## 4.6.Podpis a odeslání žádosti o obnovu

Pokud nedošlo při generování žádosti k chybě, stránka vám zobrazí vygenerovanou žádost ve formátu PKCS10.

Po kliknutí na tlačítko **Odeslat žádost ke zpracování**, se vám zobrazí dialog, obsahující Vaši žádost o obnovu certifikátu. Tuto žádost je nutné podepsat certifikátem, který obnovujete.

	CERTIFICATI
	AUTHORI
vrzení	<u> </u>
práva:	
<pre><?xml version="1.0" encoding="iso-8859-2"?> <ica> <request product_name="Certification Authority" product_version="7.06"> <header version="3"> <type>renewalrequest</type> </header>  <body> <request type="PKCS10">BEGIN CERTIFICATE REQUEST MIIDDzCCAfcCAQAwPzELMAkGA1UEBhMCQ10xGjAYBgNVBAMMEUluZy4gWmRlbsSbayBUZXN0</request></body></request></ica></pre>	
HASH (miniatura) sha512 2868 7F9D 60C5 9782 035D 1F8D 5043 8CBB 5C74 8DDC 86E8 78F1 B1B5 EB94 F01B A923 C	D60 6ED8 (
odepíšete certifikátem =CZ, CN=Ing. Zdeněk Test, SERIALNUMBER=ICA - 14568	
Přejete si tuto akci provést? Ano Ne	Storno

Podepište prosím žádost.

V některých případech budete požádáni o více podpisů. V případě, že obnovujete TWINS certifikát, je nutné podepsat jak žádost o obnovu kvalifikované, tak i komerční žádost o obnovu.

V případě úspěšného odeslání žádosti se Vám zobrazí následující stránka:

CERTIFICATION AUTHORITY První certifikační autorita A.S. Obnova certifikátu
Žádost o obnovu certifikátu byla úspěšně přijata.
ID žádosti o komerční certifikát: 7607900002068 Zde může sledovat stav Vaší žádosti s ID 7607900002068. Čas přijeti žádosti: 01.08.2011 09:09:31 Po splnění fakturačních podmínek certifikační autority pro získání certifikátu, bude obnovený certifikát zaslán na e-mail - hochman@ica.cz Copyright I.CA 2000-2011 All Right Reserved   <u>První certifikáční autorita, a.s.   Kontakty</u>



# 5. Instalace Java Runtime Environment (JRE)

Instalace JRE probíhá v rámci jednotlivých prohlížečů různými způsoby. Na jednom počítači není zapotřebí instalovat JRE v každém prohlížeči zvlášť, neboť po nainstalování funguje podpora JRE v rámci celého operačního systému, a tedy i v prohlížeči, ve kterém jste instalaci JRE neprováděli.

## 5.1.Spuštění instalace JRE pod prohlížečem Mozilla Firefox

Pokud nemáte nainstalovanou podporu Java Runtime Environment, budete při prvním přístupu na stránky pro generování žádosti o certifikát vyzváni k její instalaci. V prohlížeči Mozilla Firefox se zobrazí varovná lišta v horní části obrazovky prohlížeče, informující o nutnosti doinstalovat zásuvný modul.

Pro zobrazení veškerého obsahu na stránce jsou vyžadovány dodatečné zásuvné moduly.	Instalovat chybějící zásuvný modul 🗙

Kliknutím na tlačítko varovné lišty Instalovat chybějící zásuvný modul se zobrazí instalační dialog.

Vyhledávač zásuvných modulů 🛛 🛛 🔀	1
Dokončuji Yyhledávač zásuvných modulů	
Nebyl nalezen žádný odpovídající zásuvný modul	
Neznámý zásuvný modul Ruční instalace	
	137
Zobrazit více informací o zásuvných modulech a tetich ruční instalaci.	
< Zpět Dokončk Zrušit	5
	97

V tomto instalačním dialogu klikněte na tlačítko **Ruční instalace**, čímž budete v prohlížeči přesměrování na webové stránky, kde se dá stáhnout instalační program JRE.

#### Poznámka:

V případě, že by se tak z nějakého důvodu nestalo, zadejte následující internetovou adresu do svého prohlížeče <u>http://java.com/en/download/index.jsp</u>



Download Free Java Software	e - Mozilla Firefox	
Soubor Úpravy Zobrazení E	fistorie Zál <u>o</u> žky <u>N</u> ástroje Nápo <u>v</u> éda	_
🔇 🔁 - C 🗙 🔬	a 🔬 http://java.com/en/download/index.jsp 🏫 🚽 🚮 🛪 Google 刘	e 🚥 -
👝 Nejnavštěvovanější 📄 Jak z	začít 🔜 Přehled zpráv	
🔬 Download Free Java Softv	vare +	-
چن Java	Search Java in Action Downloads Help Center	0
Attention PC OEMs	Free Java Download	
Include Java software with your PCs! Find out how to distribute. Java on your	Download Java for your desktop computer now!	
Windows PCs.	Version 6 Update 21 Free Java Download	E
All Java Downloads		
If you want to download Java for another computer or Operating System, click the link below	» Whatis Java? » Dolhave Java? » Need Heip?	_
All Java Downloads	Why download Java?	
	Java technology allows you to work and play in a secure computing environment.	
	Java allows you to play online games, chat with people around the world, calculate your mortgage interest, and view images in 3D, just to name a few.	
	After you've downloaded Java, visit java.com to check out <u>Java in Action</u> in your daily life.	_
	Java software for your computer, or the Java Runtime Environment, is also referred to as the Java Runtime, Runtime Environment Runtime, IRE, Java Virtual Machine, Midual Machine, Java Vit, 1847	
Hotovo		

Na této stránce klikněte na červené tlačítko **Free Java Download** a na následující stránce **Agree and Start Free Download,** čímž zahájíte stahování instalačního programu. Po dokončení stahování jej spusťte; průběh instalačního programu je popsán v **Kapitole 6**.



# 6. Instalační program JRE

Po spuštění instalačního programu JRE se zobrazí první okno instalačního programu.



Na úvodní obrazovce zvolte tlačítko **instali**. Dále je proces instalace až do konce automatický. Instalační program si následně stáhne z internetu dodatečné soubory, které potřebuje k zavedení JRE do Vašeho počítače.





Na závěrečné obrazovce klikněte na tlačítko **Close**. V tuto chvíli doporučujeme prohlížeč vypnout a následně zapnout, aby se projevily změny.



# 7. Řešení problémů

V případě vzniku chyby během procesu obnovy certifikátu budete informováni chybovou hláškou.



Některé chyby mohou být závažnějšího technického rázu. Mohou souviset se stavem hardwarového či softwarového vybavení Vašeho počítače. Je důležité opsat, udělat screenshot, nebo jinak uchovat informace z podrobného výpisu chybového hlášení, neboť tyto informace jsou kritické pro rychlé vyřešení problémů s helpdeskem ICA.