

Generovanie žiadosti o certifikát Užívateľská príručka pre prehliadač Mozilla Firefox

První certifikační autorita, a.s. 17.1.2011 Verzia 7.06

CERTIFICATION AUTHORITY

1.	Úvo	d		3
2.	Poži	iadavl	ky na software	3
3.	Inšt	alácia	koreňového certifikátu I.CA	4
4.	Pro	ces ge	enerovania žiadosti o certifikát	5
4	l.1.	Kont	rola softwarového vybavenia	7
	4.1.	1.	Nepodporovaný operačný systém	7
	4.1.	2.	Nepodporovaný internetový prehliadač	7
	4.1.	3.	Podpora JavaScriptu	7
	4.1.	4.	Podpora Java Runtime Environment (JRE)	3
	4.1.	5.	Nainštalovaný Java Applet ICApki	Э
	4.1.	6.	Ukladanie cookies1	1
4	1.2.	Vypl	nenie údajov o žiadateľovi12	2
2	1.3.	Kont	rola zadaných údajov14	1
2	1.4.	Gen	erovanie žiadosti o certifikát1	5
	4.4.	1.	SecureStoreCSP	5
	4.4. súki	2. [.] oméł	Microsoft Enhanced RSA and AES Cryptographic Provider so silnou ochranou no kľúča10	6
	4.5.	U	oženie žiadosti o certifikát18	3
5.	Vyst	taveni	ie certifikátu19	Э
6.	Inšt	alácia	Java Runtime Environment (JRE)19	Э
(5.1.	Spus	tenie inštalácie JRE pod prehliadačom Mozilla Firefox19	Э
7.	Inšt	alačny	ý program JRE22	1
8.	Rieš	enie	problémov23	3

1. Úvod

Tento dokument slúži ako návod, ako postupovať pri generovaní žiadosti o certifikát cez webové stránky.

2. Požiadavky na software

Počítač, na ktorom sa bude vykonávať generovanie žiadosti o certifikát, musí spĺňať nasledujúce požiadavky:

- Musí mať nainštalovaný a spustený operačný systém
 - Microsoft Windows XP
 - Windows Vista
 - o Windows 7
- Musí byť nainštalovaný a použitý niektorý z nasledujúcich prehliadačov (pre generovanie žiadosti)
 - Microsoft Internet Explorer (verzia 7 a vyššie).
 - Mozilla Firefox (verzia 3 a vyššie)
 - **Google Chrome** (verzia 2 a vyššie)
 - Apple Safari (verzia 4 a vyššie)
 - **Opera** (verzia 10 a vyššie)
- Musí mať nainštalovaný softvér Java Runtime Environment (ďalej JRE), aspoň verzia 1.6.0_21, ktorý je potrebný pre správnu funkciu webových stránok pre generovanie žiadosti o certifikát.
 - Odporúčame používať najaktuálnejšiu verziu JRE.
 - Prítomnosť tohto softvéru detekujú stránky automaticky, ak zistí, že softvér prítomný nie je, vyzve užívateľa k jeho stiahnutiu / inštaláciu.
 - V prípade, že máte nainštalovanú staršiu verziu JRE, ako je uvedená v požiadavkách, odinštalujte ju pred začatím generovania žiadosti o certifikát. Následne budete stránkami nasmerovaný na stiahnutie najaktuálnejšej verzie.
- Vo vašom internetovom prehliadači musíte mať zapnutú podporu Javascript, zapnutú podporu jazyku Java, podporu ukladanie cookies.



3. Inštalácia koreňového certifikátu I.CA

Pri spustení stránky so žiadosťou o certifikát vás môže váš prehliadač upozorniť, že vstupujete na nedôveryhodné stránky. Tento problém je spôsobený tým, ženemáte uložené v úložisku koreňové certifikáty I.CA.

Zadajte do prehliadača nasledovné URL: <u>http://www.ica.cz/cz/menu/112/prace-s-</u> <u>certifikaty/korenove-certifikaty-i-ca-sha-2/</u>

Zobrazí sa vám nasledujúca stránka:



Pod nadpisom Koreňový certifikát certifikačnej autority pre vydávané komerčné certifikáty kliknite na Formát DER. Zobrazí sa vám dialóg pre stiahnutie súboru. Súbor obsahujúci certifikát uložte na Váš pevný disk.

V prehliadači Mozilla Firefox na nástrojovej lište zvoľte **Nástroje** a kliknite na ponuku **Možnosti ...**



<u>File Edit View History Bookmarks</u>	<u>T</u> ool:	s <u>H</u> elp	
🔇 💽 с х 🏠 🗋		Web <u>S</u> earch	Ctrl+K
Most Visited 🗋 Getting Started 🔜		<u>D</u> ownloads <u>A</u> dd-ons	Ctrl+J
Welcome to Firefox		Error <u>C</u> onsole Page <u>I</u> nfo	Ctrl+Shift+J
		Start <u>P</u> rivate Browsing Clear Recent <u>H</u> istory	Ctrl+Shift+P Ctrl+Shift+Del
		<u>O</u> ptions	

Zvolte Rozšírené, vyberte záložku Šifrovanie a kliknite na tlačítko Certifikáty.

Options							X
		页		90		- Çî	
General	Tabs	Content	Applications	Privacy	Security	Advanced	
General Ne	twork Up	date Encry	ption				
Protoco	ls						_
▼ Use	SSL <u>3</u> .0		V	Use TLS <u>1</u>	.0		
Certifica	ites						51
When a	server req	uests my pe	rsonal certificat	e:			
⊚ Se <u>l</u> e	ct one aut	omatically	Ask me ev	ery t <u>i</u> me			
) []	
View C	ertificate <u>s</u>	<u>R</u> evoca	tion Lists <u>V</u>	alidation	Security	Devices	
				ОК	Cancel	<u>H</u> elp	,

Zvolte záložku Autority a kliknite na tlačítko Importovať...

ou have certificates on file that identify these c	ertificate authorities:	
Certificate Name	Security Device	C,
(c) 2005 TÜRKTRUST Bilgi İletişim ve Bilişim		
TÜRKTRUST Elektronik Sertifika Hizmet Sa AC Camerfirma SA CIF A82743287	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	
AAmorica Opling Inc		
View Edit Import	Export Delete	

Vyberte certifikát, ktorý ste uložili na pevný disk.

Zaškrtnite **Uznať túto CA pre identifikáciu serverov**, **Uznať túto CA pre identifikáciu užívateľov pošty** a **Uznať túto CA pre identifikáciu výrobcov software**. Stlačte **OK.**

Downloading Certificate
You have been asked to trust a new Certificate Authority (CA).
Do you want to trust "I.CA - Standard Certification Authority, 09/2009" for the following purposes?
Trust this CA to identify web sites.
Trust this CA to identify email users.
Trust this CA to identify software developers.
Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).
View Examine CA certificate
OK Cancel

4. Proces generovania žiadosti o certifikát

Postup generovania žiadosti o prvotný certifikát je rozdelený do niekoľkých krokov:

- Kontrola softvérového vybavenia
- Vyplnenie údajov žiadateľa
- Kontrola vyplnených údajov
- Generovanie žiadosti o certifikát



Uloženie žiadosti o certifikát

4.1.Kontrola softwarového vybavenia

Pre uľahčenie kontroly pripravenosti vášho počítača na generovanie žiadosti, je pri začatí generovania žiadosti zobrazená kontrolná stránka, ktorá overí prítomnosť kľúčových softvérových komponentov.

Checking required software, wait for its termination.

Your operating system WinXP is supported Your browser Firefox version 3.6 is supported. JavaScript enabled.

Stránka otestuje počítač, test môže trvať desiatky sekúnd, a ohlási, či je niečo v neporiadku, prípadne vypíše chybové hlásenie. Ak nie sú detekované problémy, stránka zobrazí formulár pre vyplnenie osobných údajov.

Ak sa pri kontrole vyskytne chyba, nie je zobrazený formulár pre vyplnenie osobných údajov. Najskôr je potrebné odstrániť chybu, ktorá znemožňuje generovanie žiadosti. Význam chybových hlásení je uvedený v nasledujúcich kapitolách.

4.1.1.Nepodporovaný operačný systém

Pre generovanie žiadosti musíte použiť jeden z operačných systémov uvedených v kapitole 2.

4.1.2.Nepodporovaný internetový prehliadač

Pre generovanie žiadosti musíte použiť jeden z prehliadačov uvedených v kapitole 2.

4.1.3.Podpora JavaScriptu

Stránky pre generovanie žiadosti o certifikát vyžadujú podporu skriptovania v jazyku JavaScript. Všetky podporované prehliadače majú túto podporu automaticky povolenú. Ak by táto kontrola zlyhala, znamená to s najväčšou pravdepodobnosťou, že je v nastavení prehliadača podpora skriptovania vypnutá. Povoľte podporu skriptovania v jazyku JavaScript vo vašom prehliadači.

4.1.3.1.Povolenie JavaScriptu v Mozilla Firefox

Na nástrojovej lište zvoľte Nástroje a kliknite na ponuku Možnosti...



<u>File Edit View History B</u> ookmarks	Tools Help	
🔇 💽 с х 🏠 🔲	Web <u>S</u> earch Ctrl+K	
Most Visited 🗋 Getting Started 🔊	Downloads Ctrl+J Add-ons	
	Error <u>C</u> onsole Ctrl+Shift+J Page <u>I</u> nfo	
	Start <u>P</u> rivate Browsing Ctrl+Shift+P Clear Recent <u>H</u> istory Ctrl+Shift+Del	
	Options	

Zvoľte záložku Obsah a zatrhnite Povoliť JavaScript a kliknite na tlačítko OK.

Options						×
		<u>م</u>		90		÷
General	Tabs	Content	Applications	Privacy	Security	Advanced
 ✓ <u>B</u>lock p ✓ Load in ✓ Enable 	oop-up w mages au JavaScrip	vindows tomatically pt				Exceptions Exceptions Advanced
Fonts & Co	olors					
<u>D</u> efault for	nt: Time	es New Rom	an	✓ Size	e: 16 🔻	<u>A</u> dvanced
Languages						
Choose yo	ur preferi	ed language	for displaying	pages		Ch <u>o</u> ose
				OK	Cancel	Help
				UK	Cancel	

4.1.4.Podpora Java Runtime Environment (JRE)

Tieto stránky vyžadujú pre svoju funkčnosť nainštalovanú podporu jazyka Java. Uistite sa, že nemáte vo svojom prehliadači túto podporu vypnutú. Pokiaľ nemáte na svojom počítači JRE nainštalované, mal by vás prehliadač vyzvať na stiahnutie a inštaláciu JRE. Ak sa tak nestalo, kliknite na odkaz uvedený nastránke a manuálne stiahnite a nainštalujte aktuálnu verziu JRE. V každom prípade bude po inštalácii JRE treba zavrieť a znovu spustiť prehliadač, aby sa zmeny prejavili.

Inštalácia JRE je popísaná v Kapitole 6.



4.1.4.1.Povolenie Java v Mozilla Firefox

Na nástrojovej lište zvoľte Nástroje a kliknite na ponuku Správca doplnkov.

<u>File Edit View History B</u> ookmarks	<u>T</u> ool	s <u>H</u> elp	
🔇 🕑 С Х 🏠 🔲		Web <u>S</u> earch	Ctrl+K
🔊 Most Visited 📄 Getting Started 🔊		<u>D</u> ownloads	Ctrl+J
Welcome to Firefox		<u>A</u> dd-ons	
		Error <u>C</u> onsole Page <u>I</u> nfo	Ctrl+Shift+J
		Start <u>P</u> rivate Browsing	Ctrl+Shift+P
		Clear Recent <u>H</u> istory	Ctrl+Shift+Del
		Options	

Zvoľte záložku **Rozšírenie**, vyberte položku **Java** a kliknite na **Povoliť**. Aby sa zmena prejavila, je potrebné reštartovať Firefox.

🥹 Add-ons						- • •
Get Add-ons	Extensions	No. Themes	Plugins			
Java Co Opti	onsole 6.0.24				<u>E</u> nable	<u>U</u> ninstall
Micros Adds C	oft .NET Fram lickOnce supp	ework Assi ort and the	stant 1.0 ability to re	eport installe	d .NET vers	ions to the
						Eind Updates

4.1.5.Nainštalovaný Java Applet ICApki

V tomto mieste sa kontrolná stránka pokúsi nainštalovať Java Applet ICApki, ktorý je potrebný pre funkčnosť stránok pre generovanie žiadosti o certifikát. Pri prvej inštalácii appletu na počítač, kde prebieha generovanie žiadosti o certifikát, budete vyzvaný na potvrdenie dôvery vydavateľovi Java applet. Vydavateľom appletu je První certifikační autorita, a.s. Dôveru appletu potvrdíte dialógom, ktorý znázorňuje nasledujúci obrázok. V tomto dialógu je dôležitézaškrtnúť voľbu **Always trust content from this publisher** a potom použiť tlačidlo **Yes**.



Name: tbica.ica.cz Publisher: tbica.ica.cz ☑ Always trust content from this publisher: Yes Yes No	Varning - Secur The web s want to co	ity site's certificate cannot be verified. Do ontinue?	you 🔶
Yes No The certificate cannot be verified by a trusted source. More Information	Name: Publisher: V Always to	tbica.ica.cz tbica.ica.cz ust content from this publisher.i	
\checkmark	The	certificate cannot be verified by a trusted source.	Yes No

Nasleduje druhý dialóg, kde sa postupuje obdobne, t.j. zaškrtne sa voľba **Always trust content from this publisher** a potom sa použije tlačidlo **Run.**

he applic Io you wa	ation's digital signature has been v nt to run the application?	erified.
Name:	ICApki	
Publisher:	I.CA - Code Signing	
From:	https://tbica.ica.cz	
🗸 Always t	ust content from this publisher.	
		Run Cancel
The c	ligital signature has been validated by a trusted source.	More Information

Pri ďalšom spustení stránok na počítači, kde táto inštalácia prebehla, už nebudete k opätovnému potvrdzovanie Java Applet ICApki vyzývaný.

V prípade, že bude vydaná nová verzia Java Applet ICApki, bude klientom v tomto mieste okamžite automaticky stiahnutá a nainštalovaná. Táto inštalácia môže chvíľu trvať. Po jej skončení budú stránky pokračovať v normálnej práci.



4.1.6.Ukladanie cookies

Pre správnu prácu stránok pre generovanie žiadostí je potrebné, aby váš prehliadač umožnil stránke ukladať cookies. Ak máte zakázané ukladanie cookies, povoľte ho.

4.1.6.1. Povolenie cookies v Mozilla Firefox

Na nástrojovej lište zvoľte Nástroje a kliknite na ponuku Možnosti...

<u>File Edit View History Bookmarks</u>	<u>I</u> ools <u>H</u> elp	
🔇 🕑 С Х 🕁 🔲	Web <u>S</u> earch Ctrl+K	
Most Visited Getting Started	Downloads Ctrl+J	
Welcome to Filefox	Error <u>C</u> onsole Ctrl+Shift+J Page <u>I</u> nfo	
	Start <u>P</u> rivate Browsing Ctrl+Shift+P Clear Recent <u>H</u> istory Ctrl+Shift+Del	
	Options	

Zvoľte záložku Súkromie. U Nastavenie histórie zvoľte Pamätať si históriu(prípadne zvoľte Použiť pre históriu vlastné nastavenia a zaškrtnite Povoliť serverom nastavovať cookies).

Op	tions							×
			页		90		÷ې	
	General	Tabs	Content	Applications	Privacy	Security	Advanced	
ſ	History							
	Firefox will	Reme	mber history		•			
	Firefo	will rem	ember your b	prowsing, down	load, form	and search	history, and	
	keep o	ookies fr	om Web sites	s you visit.				
	You m	av want i	to clear your	recent history	or remove i	ndividual co	okies	
	Tourn	ay want	to <u>clear your</u>	recent history,	or <u>remove i</u>		JOKICS.	
	Location B	ar						
	When <u>u</u> sin	g the loca	ation bar, sug	gest: History	/ and Bookn	narks 🔻		
					OK	Cancel	Hele	
					UN	Cancer	<u>H</u> eip	

Nastavenie potvrďte kliknutím na tlačidlo **OK**.



4.2.Vyplnenie údajov o žiadateľovi

Ak proces kontroly prebehol bez chýb, stránka zobrazí formulár, do ktorého vyplníte svoje osobné údaje.

Heading	Your information		Example of completion		
Select what type of applicant you are					
 Current user (non-entrepreneurial) 					
Entrepreneur (Self-employed)					
© Employee					
© Pseudonym					
Choose a repository for your private k	ey				
Smart card I.CA					
Other storage (PC, server, USB token, other sma	rt card, etc.)				
Information about the applicant					
Degree (before name)			Ing.		
Name			Jiřina		
Surname			Koutná		
Degree (after name)			Ph.D.		
Generational resolution			MI.		
E-mail *)			jirina_koutna@ica.cz		
The certificate is designed for communication with public authorities of the SR			Mark the item if you require that the certificate can be used for communication with public authorities of the the SR and a private key to generate <u>certified products according to</u>		
			<u>Slovak legislation</u>		
Permanent Address			· · ·		
Street			Ceská		
Street number/building identification number			11/22		
City/town			Brno		
Zip code			11150		
Province			Jihomoravský		
Country	Czech Republic				
Other options	·				
Revocation password					
Key Repository Type (CSP)	SecureStoreCSP -				
Show advanced key usage settings (Recommended for experts). We do not recommend changing the default settings using the key. The change in the use of keys by the user's own risk.					
Certificates for signing	\checkmark				
Certificates for encryption					
*) The item is mandatory only if you intend to use t	the certificate in the email.				

Continue

Položky zdôraznené tučným písmom a žltým podfarbením vstupného polia sú povinné. Napríklad meno a priezvisko sú povinné, tituly povinné nie sú.

Heslo pre zneplatnenie:

Pokiaľ dôjde počas používania certifikátu ku kompromitácii privátneho kľúča, zmene údajov (zmena mena, bydliska ...) alebo sa vyskytnú ďalšie dôvody, prečo by nemal byť certifikát ďalej používaný, je Vašou zákonnou povinnosťou certifikát zneplatniť. Certifikát je možné zneplatniť cez webové rozhranie. Pri zneplatnenie budete vyzvaný na zadanie hesla pre zneplatnenie. Toto heslo pre zrušenie určujete pri generovaní žiadosti o certifikát.

Dĺžka hesla pre zneplatní certifikátu musí byť 4 až 32 znakov. Povolené sú iba veľké a malé písmená bez diakritiky a číslice.

Typ úložisko kľúča (CSP):

Pri položke **Typ úložisko kľúča (CSP)** vyberte z ponuky SW modul zaisťujúci kryptografické služby (CSP), ktorý vygeneruje váš privátny kľúč. Všetky tu zobrazené CSP podporujú podpisový algoritmus SHA2 a sú nainštalované vo vašom počítači.

Export privátneho kľúča:

Ak vami zvolený typ úložiska kľúča (CSP) podporuje export privátneho kľúča, je vám ponúknutá voľba **povoliť export privátneho kľúča**. Táto voľba umožní vykonať export certifikátu vrátane súkromného kľúča. Súkromný kľúč tak budete môcť prenášať medzi úložiskami. Správa kľúča vyžaduje v takom prípade zvýšenú opatrnosť z dôvodu vyššieho rizika jeho krádeže / zneužitia.

Silná ochrana privátneho kľúča:

Ak vami zvolený typ úložiska kľúča (CSP) podporuje silnú ochranu privátneho kľúča, je vám ponúknutá voľba **povoliť silnú ochranu privátneho kľúča**. Pred každým použitím vášho kľúča budete upozornený, že je váš kľúč používaný.Následne máte možnosť vybrať si medzi: Stredná - vždy budete len upozornený informatívnym hlásením; Silná - pred každým použitím po Vás bude vyžadované zadanie hesla.

Po stlačení tlačidla **pokračovať** stránka vykoná kontrolu vami vyplnených údajov. Ak niektoré zadané údaje nespĺňajú podmienky, budete vyzvaný na ich opravu.Údaje vyžadujúce zmenu alebo doplnenie sú podfarbené červenou farbou.

Select what type of applicant you are © Current user (non-enterpreneurial) © Enterpreneurial) © Enterpreneurial) © Enterpreneurial) © Enterpreneurial) © Beaudonym Choose a repository for your private key ® Smart card 1CA © Other storage (PC, server, USB token, other smart card, etc.) Information about the applicant © our must enter a tame. Jilina Surname Doe Koutná Cenerational resolution Mil Cenerational resolution Mil Cenerational resolution Mil Cenerational resolution Mil Cenerational resolution Permanent Address Street Ceská Street Centry Ceck Republic Contry (Ceck Republic Province Jiling Contry (Ceck Republic Ceneration password for revocation may contain only the numbers and letters Key Repository Type (CSP) Secure Store CSP Centricates for engryton Store of revocation may contain only the numbers and letters Key Repository Type (CSP) Secure Store CSP Store a storage (Recommended for engrets). We do not recommend changing the default settings using the key. The change in the use of keys by the user's centricates for engryton Centry Centry (SP) Secure Store CSP Centricates for engryton Centry (Section Republic Centry (Heading	Your information	Example of completion				
Current user (non-entrepreneurial) Chapter preduct (Self-employed) Paeudonym Choces a repository for your private key Senar card (CA Cother storage (PC, sever, USB token, other smart card, etc.) Information about the applicant Cother storage (PC, sever, USB token, other smart card, etc.) Information about the applicant Cother storage (PC, sever, USB token, other smart card, etc.) Information about the applicant Cother storage (PC, sever, USB token, other smart card, etc.) Information about the applicant Cother storage (PC, sever, USB token, other smart card, etc.) Information about the applicant Cother storage (PC, sever, USB token, other smart card, etc.) Information about the applicant Cother storage (PC, sever, USB token, other smart card, etc.) Information about the applicant Cother storage (PC, sever, USB token, other smart card, etc.) Information about the applicant Cother storage (PC, sever, USB token, other smart card, etc.) Information about the applicant Cother storage (PC, sever, USB token, other smart card, etc.) Information about the applicant Cother storage (PC, sever, USB token, other smart card, etc.) Information about the applicant Cother storage (PC, sever, USB token, other smart card, etc.) Information about the applicant Cother storage (PC, sever, USB token, other smart card, etc.) Information about the applicant Information about the storage (PC, sever, USB token, etc.) Information about the applicant Information about the a	Select what type of applicant you are						
Entrepreneur (Self-employed) Employee Pesudown Choose a repository for your private key Smat card LCA Other softage (PC, server, USB bloken, other smart card, etc.) Information about the applicant Oegree (before name) Oegree (before name) Degree (der name) Degree (der name) Degree (der name) Degree (der name) E-mail * Info. Centratione of the softage (Component of the SR and the SR	 Current user (non-entrepreneurial) 						
Enployee Enployee Choose a repository for your private key Smart card I.CA Other storage (PC, sever, USB token, other smart card, etc.) Information about the applicant Ing. Ing. Using the applicant Using the applicant Ing. Using the applicant Using the applicant Ing. Using the applicant of the applicant Using the applicant of the applicant Using the applicant of the	Entrepreneur (Self-employed)						
Peeudonym ChOces a repository for your private key @ Smart card LOA @ Other storage (PC, server, USB token, other smart card, etc.) Information about the applicant	© Employee	Employee					
Chocse a repository for your private key Smatt card LCA Control Conserved Co	© Pseudonym						
Strat card LCA Other storage (PC, ever, USB token, other and card, etc.) Information about the applicant Information about the applicant Vou must enter a name. Jifina Ougree (after name) Degree (after name) Degree (after name) E-mail 7 Cenerational resolution Mick The certificate is designed for communication with public autorities of the the SR and box autoritie	Choose a repository for your private	key					
Other storage (PC, server, USB token, other smart card, etc.) Information about the applicant Degree (before name) ing. Our must enter a name. Jilina Our must enter a name. Kouthá Degree (aler name) Ph.D. Generational resolution Mul The certificate is designed for communication with public authorities of the SR and a private key to generate certified products according to Street number/building identification number Óeskiá Street number/building identification number 11/22 Other options Bino Revocation password for revocation may contain only the numbers and letters without accords. The password must be 4-32 characters. Jinomoravský Chertificates for signing Street for expression (CSP) Street services on the set on the	Smart card I.CA						
Information about the applicant	Other storage (PC, server, USB token, other sma	irt card, etc.)					
Degree (before name) ing. Vur unst enter a name. Jifina Surmano Doe Kouthá Ph.D. Cenerational resolution Mi. E-mail */ jifina_koutha@jca.cz The certificate is designed for communication mark the item if you require that the certificate can be used for communication with public authorities of the SR and a private key to generate certified products according to Slowak legislation Permanent Address Certificate is designed for communication Street Cesisiá Street Cesisiá Street Cesisiá Street Street Citytown Brmo Citytown Brmo Jifno arswig) Jihomorawský Country Czech Republic Jihomorawský Cher options Breword for revocation may contain only the numbers and letters without accents. The password must be 4-32 characters. Key Repository Type (CSP) SecureStoreCSP Show advanced key usage settings (Recomment-defore specifis). We do not recommend changing the default settings using the key. The change in the use of keys by the user's on risk. Certificates for signing Certificates for signing	Information about the applicant						
Name Jilina Vou must enter a name. Jilina Surname Doe Certificate a password for recommend of password for recommend changing the default settings using the key. The change in the use of keys by the user's own risk. Jilina	Degree (before name)		Ing.				
You must enter a name. Koutná Surname Doe Koutná Degree (after name) Ph.D. Generational resolution MI. The certificate is designed for communication with public authorities of the SR and a private key to generate certified products according to street for communication numbers of the SR and a private key to generate certified products according to street certified certificates for street certified certificates for street certified certificate certified certificate certified certificates for street certified certificates for street certified certificates for encryption	Name		Jiřina				
Surname Doe Kouthá Degree (after name) Ph.D. Generational resolution MI. Image: Control of the set of th		You must enter a name.					
Degree (after name) Ph.D. Generational resolution Mil. E-mail Y jirina_koutna@ica.cz The certificate is designed for communication with public authonties of the SR and a private key to generate certified products according to Slovak legislation Permanent Address Citybow Street Citybow Citybow Citybow Province Differentiation on the password for revocation may contain only the numbers and letters withouts accents. The password for experts). We do not recommend changing the default settings using the key. The change in the use of keys by the user's own risk.	Surname	Doe	Koutná				
Generational resolution MI. Image: Communication jirina_koutha@ica.cz The certificate is designed for communication Mark the item if you require that the certificate can be used for communication with public authorities of the the SR and a private key to generate certified products according to a private key to a private key to a private key to a private key to a private key. The change in the use of keys by the user's or risk. Other options a private key to a sprivate key to a spriv	Degree (after name)		Ph.D.				
E-mail *) jirina_koutna@ica.cz The certificate is designed for communication with public authorities of the SR and a private key to generate certified products according to Slovak legislation Permanent Address Permanent Address Ceská Street Cityitown Cityitown Country Cecch Republic Other options Revocation password for revocation may contain only the numbers and letters. Key Repository Type (CSP) Scuere Storee CSP Show advanced key usage settings (Recommended for experts). We do not recommend changing the default settings using the key. The change in the use of keys by the user's own risk. Certificates for signing	Generational resolution		MI.				
E-mail * jirina_koutna@ica.cz Mark the item if you require that the certificate can be used for communication with public authorities of the the SR and a private key to generate certified products according to Slovak legislation Permanent Address Permanent Address City/town Street City/town City/town Province Jino Defense (Control City/town Street number/building identification number City/town City/town City/town Control City/town Control City/town Control City/town Province Dimonary Sky Control City/town Province Province Province Province Province Street number/building identification number City/town City/town Street number/building identification number Province Street number/building identification number Street number/building identification number City/town Street number/building identification number Province Street number/building identification number Province Street number/building identification number Street number/building identification number Province Street number/building identification number Province Street options Province Province Street options <td></td> <td></td> <td>-</td>			-				
The certificate is designed for communication with public authorities of the SR and a private key to generate certified products according to Slovak tegislation Permanent Address Street Ceská Street number/building identification number 11/22 Cityhtown Brmo 11/20 11/120 Verter options Jihomoravský Country Czech Republic Other options Password for revocation must be 4-32 characters. Key Repository Type (CSP) SecureStoreCSP • Show advanced key usage settings (Recommented for experts). We do not recommend changing the default settings using the key. The change in the use of keys by the user's own risk. Certificates for encryption Certificates for encryption	E-mail *)		jirina_koutna@ica.cz				
Permanent Address Street Česká Street number/building identification number 11/22 City/town Brno Zip code 11150 Province Jihomoravský Country Czech Republic Other options Image: Street of the password for revocation may contain only the numbers and letters without accents. The password must be 4-32 characters. Key Repository Type (CSP) SecureStoreCSP Show advanced key usage settings (Recommended for experts). We do not recommend changing the default settings using the key. The change in the use of keys by the user's own risk. Certificates for signing Image: Certificates for encryption	The certificate is designed for communication with public authorities of the SR		Mark the item if you require that the certificate can be used for communication with public authorities of the the SR and a private key to generate <u>certified products according to</u> <u>Slovak legislation</u>				
Street Česká Street number/building identification number 11/22 City/town Brno City/town Jinomoravský Zip code Jinomoravský Country Czech Republic Other options Image: Construction password Revocation password g Password for revocation may contain only the numbers and letters without accents. The password must be 4-32 characters. Key Repository Type (CSP) SecureStoreCSP v Show advanced key usage settings (Recommended for experts). We do not recommend changing the default settings using the key. The change in the use of keys by the user's own risk. Certificates for signing Certificates for encryption	Permanent Address						
Street number/building identification number 11/22 City/town Brno Zip code 11150 Province Jihomoravský Country Czech Republic	Street		Česká				
City/town Brno Zip code 11150 Province Jihomoravský Country Czech Republic Other options Image: Control of the password for revocation may contain only the numbers and letters without accents. The password must be 4-32 characters. Key Repository Type (CSP) SecureStoreCSP v Image: Show advanced key usage settings (Recommended for experts). We do not recommend changing the default settings using the key. The change in the use of keys by the user's own risk. Certificates for signing Image: Certificates for encryption	Street number/building identification number		11/22				
Zip code 11150 Province Jihomoravský Country Czech Republic Other options Revocation password Password for revocation may contain only the numbers and letters without accents. The password must be 4-32 characters. Key Repository Type (CSP) SecureStoreCSP	City/town		Brno				
Province Jihomoravský Country Czech Republic Other options Revocation password a Password for revocation may contain only the numbers and letters without accents. The password must be 4-32 characters. Key Repository Type (CSP) Show advanced key usage settings (Recommended for experts). We do not recommend changing the default settings using the key. The change in the use of keys by the user's own risk. Certificates for signing Certificates for encryption	Zip code		11150				
Country Czech Republic Other options Revocation password Password for revocation may contain only the numbers and letters without accents. The password must be 4-32 characters. Key Repository Type (CSP) Show advanced key usage settings (Recommended for experts). We do not recommend changing the default settings using the key. The change in the use of keys by the user's own risk. Certificates for signing Certificates for encryption	Province		Jihomoravský				
Other options Revocation password Password for revocation may contain only the numbers and letters without accents. The password must be 4-32 characters. Key Repository Type (CSP) Show advanced key usage settings (Recommended for experts). We do not recommend changing the default settings using the key. The change in the use of keys by the user's own risk. Certificates for signing Certificates for encryption	Country	Czech Republic 🔹					
a Revocation password for revocation may contain only the numbers and letters without accents. The password must be 4-32 characters. Key Repository Type (CSP) SecureStoreCSP • Show advanced key usage settings (Recommended for experts). We do not recommend changing the default settings using the key. The change in the use of keys by the user's own risk. Certificates for signing Certificates for encryption	Other options						
Revocation password password for revocation may contain only the numbers and letters without accents. The password must be 4-32 characters. Key Repository Type (CSP) Secure Store CSP • Show advanced key usage settings (Recommended for experts). We do not recommend changing the default settings using the key. The change in the use of keys by the user's own risk. Certificates for signing Certificates for encryption		а					
Minor decision in the positive interest in a positive interest. Key Repository Type (CSP) Show advanced key usage settings (Recommended for experts). We do not recommend changing the default settings using the key. The change in the use of keys by the user's own risk. Certificates for signing Certificates for encryption	Revocation password	Password for revocation may contain only the numbers a without accents. The password must be 4.32 characters	nd letters				
Show advanced key usage settings (Recommended for experts). We do not recommend changing the default settings using the key. The change in the use of keys by the user's own risk. Certificates for signing Certificates for encryption	Key Repository Type (CSP)	SecureStoreCSP					
Certificates for signing Certificates for encryption	Show advanced key usage settings (Recommen own risk.	ded for experts). We do not recommend changing the defaul	t settings using the key. The change in the use of keys by the user's				
Certificates for encryption	Certificates for signing						
	Certificates for encryption						



Ak Vami zadané údaje spĺňajú podmienky, zobrazí sa vám stránka rekapitulujúca vami zadané údaje.

4.3.Kontrola zadaných údajov

Na tejto stránke prosím skontrolujte vami zadané údaje.

Recapitulated application	
Heading	Specified Value
Revocation password	aaaa
Period of validity	365 days
Key Repository Type (CSP)	SecureStoreCSP
Algorithm thumbnails	sha256WithRSAEncryption
Allow exporting the private key	No
Allow the strong private key protection	No
Key length	2048
Certificates for signing	Yes
Certificates for encryption	No
Key name	4d75ee7d94084
Encoding type	UTF8_STRING
Items of the certificate request	
Full name	Jane Doe
E-mail	doe@ica.cz
Country	CZ
The issued certificate is sent to the e-ma	ail:
Certificate sent in the ZIP format:	
	Yes
	© No
Save the application in the card	
Make request	
Makerequest	

Ak si prajete zaslať vydaný certifikát na e-mail, zadajte e-mailovú adresu, na ktorú vám bude certifikát zaslaný (položka **Vystavený certifikát zaslať na e-mail**:). Pozor: táto emailová adresa nie je súčasťou žiadosti o certifikát, teda nebude uvedená ani v samotnom certifikáte. E-mailovú adresu, ktorá bude obsiahnutá v certifikáte, je nutné vyplniť v údajoch o žiadateľovi (položka žiadosti o certifikát)!

Ak vami zvolený typ úložiska kľúča (CSP) podporuje uloženie žiadosti na kartu,môžete zatrhnúť možnosť **Uložiť žiadosť na kartu**. Ak zvolíte túto možnosť, stránka sa po vygenerovaní žiadosti pokúsi uložiť vygenerovanú žiadosť na kartu. Uistite sa, že na vašej karte je dostatok voľného miesta pre uloženie žiadosti. Ak uložíte žiadosť na kartu, operátor registračnej autority I. CA bude môcť načítať vašu žiadosť priamo z karty (nemusíte nosiť žiadosť na USB disku alebo inom médiu).

Kliknutím na tlačidlo Vytvoriť žiadosť spustíte generovanie žiadosti o certifikát.



4.4.Generovanie žiadosti o certifikát

Nasledujúci postup sa pre jednotlivé typy úložiska kľúča (CSP) mierne líši.

4.4.1.SecureStoreCSP

Ak pri vyplňovaní údajov o žiadateľovi zvolíte ako typ úložiska kľúča SecureStoreCSP, je postup generovania žiadosti nasledovný:

Najskôr sa vám zobrazí nasledujúci dialóg. V tomto momente sa generuje váš privátny kľúč. Tvorba privátneho kľúča môže trvať niekoľko desiatok sekúnd.

SecureSt	oreCSP	1
ca	rd operation is in progress	l
		1

Potom, čo je privátny kľúč vytvorený, ste vyzvaný na zadanie PINu k vašej karte.

SecureStoreCSP - enter PIN	23		
It is necessary to enter PIN to process this operation. Operation : Signature of data by key located on card			
PIN:			
Remember PIN			
OK Cancel			

Ak ste zvolili, že žiadosť má byť uložená na kartu, ste informovaný o výsledku uloženia. Ak bolo na karte dostatok miesta a žiadosť sa podarilo uložiť, je Vám zobrazený nasledujúci dialóg:

Sdělení s	Sdělení stránky https://s.dev.ica.cz:		
	The application was stored in the card.		
	ОК		

Ak na karte nebol dostatok voľného miesta a žiadosť sa nepodarilo uložiť, zobrazí sa nasledujúci dialóg (váš privátny kľúč je na karte uložený v poriadku a nie je potreba znovu kľúč generovať):



Sdělení s	tránky https://s.dev.ica.cz:
	Error: The request could not be saved to the card.
	ОК

V takom prípade sa žiadosť na karte nenachádza. Musíte žiadosť uložiť na USB flash disk alebo iné médium, ktoré predložíte na registračnej autorite I.CA.

4.4.2.Microsoft Enhanced RSA and AES Cryptographic Provider so silnou ochranou súkromého kľúča.

Ak pri vyplňovaní údajov o žiadateľovi zvolíte ako typ úložisko kľúče Microsoft Enhanced RSA and AES Cryptographic Provider (prípadne Microsoft Enhanced RSA and AES Cryptographic Provider / prototype /) a zaškrtnete voľbu Povoliť silnú ochranu kľúča, je postup generovania žiadosti nasledovný:



Ak kliknete na Nastaviť úroveň zabezpečenia ..., budete môcť zmeniť úroveň zabezpečenia.



Creating a new RSA signa	ture key 🗾
	Choose a security level appropriate for this item.
	 High Request my permission with a password when this item is to be used.
	Medium Request my permission when this item is to be used.
	< Back Next > Cancel

Ak zvolíte vysokú úroveň zabezpečenia, budete vyzvaný na zadanie hesla. Toto heslo bude potrebné zadať vždy, keď budete používať súkromný kľúč.

Creating a new RSA signat	Creating a new RSA signature key			
	Create a password to	protect this item.		
	Create a new passwo	ord for this item.		
	Password for:	CryptoAPI Private Key		
	Password:			
	Confirm:			
	< Back	Finish Cance	el	

Po kliknutí na tlačidlo **Dokončiť** dôjde k zmene úrovne zabezpečenia. Teraz kliknite na tlačidlo **OK.**



Creating a new	RSA signature key
	An application is creating a Protected item.
	CryptoAPI Private Key
	Security level set to Medium Set Security Level
	OK Cancel Details

V ďalšom dialógovom okne vyberte **Prideliť privilégiá**. Ak ste zvolili vysokú úroveň zabezpečenia, musíte zadať aj heslo.

📀 Request For Permission to Use a	Кеу	
Grant or deny this applica	tion permission to use this key	
Key name:	Application supplied name for the key Grant permission Deny permission	
Key protection password:		
View key details	OK Cance	el

4.5. Uloženie žiadosti o certifikát

Ak nedošlo pri generovaní žiadosti k chybe, stránka vám zobrazí vygenerovanú žiadosť vo formáte PKCS10. Kliknutím na tlačidlo **Uložiť žiadosť na disk** bude žiadosť uložená na váš pevný disk alebo iné médium, ktoré zvolíte.



The certificate request has been generated.

BEGIN	CERTIFICATE	REQUEST
-------	-------------	---------

MIICnTCCAYUCAQAwIDERMA8GA1UEAwwISmFuZSBEb2UxCzAJBgNVBAYTAkNaMIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAi496mTv+wq8V1H/el/hdWiNytyMsoVxjgREL9uQt
kq8WIgI5kak64Cvw6n+e0/cRHKspUIB8xvswWqJJ/j94bp2b9JtdWIDuPRtkFluhSzEgx4Gm
7X39UWAhTW1zVE+cwjr1UKESJm0Md+ZfnIYNTuV6A+ieyzCk9fbsJXay09T3F2smBbgIejj0
LJdLNUoWMDNSZqst2GED1Md+cYdEU1e0GuVjhuhKWxchX0JkxyIpy3zgxkt1REnUIVDKNJ1M
aDAXCbQYT1s82pF03rUZHvw3VRokLD+0I66YeqHxW2rh1YHU/jj6Jg0E+vq8mNvQgmFkw1dI
bzUlWVaCaSPzpQIDAQABoDgwNgYJKoZIhvcNAQkOMSkwJzAOBgNVHQ8BAf8EBAMCBsAwFQYD
VRORBA4wDIEKZG91QG1jY35jejANBgkqhkiG9w0BAQsFAAOCAQEAhCbQX3M9/ZaBoPpi1h5U
08Kt2ZFdHeL7EuyG+E6itf2IB4SOCxJFifB7JNFqBGL1i2h6aoBZ4gpWQfuRGLUIdo8QwAX1
XXenfT0WLq0RM2j03FUZnnokgQ+KBL7Tv1EClyiDi0Nz5ZEgpiYzfh1YX/5ul1uoVYniPrN7
hbgAxi8BYBIhK8uEpUqN3D1Gs3MvwsYS/xSWhRkCIRrPazVJ2m6GR6djk7zCJBE11GJFTtZm
PnMn5qdcUyh/pV1+cZian3kXCGfqKxiWx4Toq9VRE5ia4Vr31XheaRpsxU8wGXSw8bF188P4
D0VIQIokI+/Uq/qWY+YUv5q8HeAIDVDbfw==
END CERTIFICATE REQUEST
Save request to the disc

5. Vystavenie certifikátu

Potom, čo vytvoríte žiadosť o certifikát, je nutné navštíviť niektorú registračnú autoritu I. CA (<u>zoznam</u> <u>tu</u>). So sebou na registračnú autoritu I. CA prineste žiadosť, ktorú ste vygenerovali (napríklad na USB flash disku, alebo uloženú na čipovej karte), a dokumenty potrebné na vystavenie certifikátu. Zoznam potrebných dokumentov nájdete <u>tu.</u>

6. Inštalácia Java Runtime Environment (JRE)

Inštalácia JRE prebieha v rámci jednotlivých prehliadačov rôznymi spôsobmi. Na jednom počítači nie je potrebné inštalovať JRE v každom prehliadači zvlášť, lebo po nainštalovaní funguje podpora JRE v rámci celého operačného systému a teda aj v prehliadači, v ktorom ste inštaláciu JRE nevykonávali.

6.1.Spustenie inštalácie JRE pod prehliadačom Mozilla Firefox

Ak nemáte nainštalovanú podporu Java Runtime Environment, budete pri prvom vstupe na stránky pre generovanie žiadosti o certifikát vyzvaný k jej inštalácii. V prehliadači Mozilla Firefox sa zobrazí varovná lišta v hornej časti obrazovky prehliadača informujúca o nutnosti doinštalovať zásuvný modul.

🚆 Additional plugins are required to display all the media on this page.

Install Missing Plugins...

Kliknutím na tlačidlo varovnej lišty Inštalovať chýbajúci zásuvný modul sa zobrazí inštalačný dialóg.



Plugin Finder Service	×
Completing the Plugin Finder Service	
No suitable plugins were found.	
Unknown Plugin (application/x-java-applet;version=1.6)	Manual Install
Find out more about Plugins or manually find missing plugins.	
< <u>B</u> a	ck Finish Cancel

V tomto inštalačnom dialógu kliknite na tlačidlo **Ručná inštalácia**, čím budete v prehliadači presmerovaný na webové stránky, kde sa dá stiahnuť inštalačný program JRE.

Poznámka:

V prípade, že by sa tak z nejakého dôvodu nestalo, zadajte nasledujúcu internetovú adresu do svojho prehliadača <u>http://java.com/en/download/index.jsp</u>



oubor Úpr <u>a</u> vy <u>Z</u> obrazení <u>I</u>	<u>H</u> istorie Zál <u>o</u> žky <u>N</u> ástroje Nápo <u>v</u> ěda
< 🔁 - C 🗙 🏠	🖞 🔮 http://java.com/en/download/index.jsp 🏠 🚽 🚼 - Google 🔎 🕮 -
🖉 Nejnavštěvovanější 📋 Jak :	začít 🚮 Přehled zpráv
🔮 Download Free Java Soft	ware ÷
	Search
Java	Java in Action Downloads Help Center
Attention PC OEMs	Free Java Download
Include Java software with	Download Java for your desktop computer now!
distribute Java on your	Version 6 Update 21
Windows PCs.	Free Java Download
All Java Downloads	
If you want to download Java for another computer or Operating System, click	» What is Java? » Do I have Java? » Need Help?
the link below. All Java Downloads	Why download lave?
	lave technology allows you to work and play in a conversion provisionment
	Sava technology allows you to work and play in a secure comparing 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
Hotovo	

Na tejto stránke kliknite na červené tlačidlo **Free Java Download** a na nasledujúcej stránke **Agree and Start Free Download**, čím zahájite sťahovanie inštalačného programu. Po dokončení sťahovania ho spustite; priebeh inštalačného programu je popísaný v **Kapitole 7.**

7. Inštalačný program JRE

Po spustení inštalačného programu JRE sa zobrazí prvé okno inštalačného programu.

الله الله الله الله الله الله الله الله	Sun Sun
Welcome to Java	a™
Java provides safe and secure access to the From business solutions to helpful utilities an your internet experience of	world of amazing Java content. d entertainment, Java makes ome to life.
Note: No personal information is gathered a Click here for more information on	as part of our install process. what we do collect.
Click Install to accept the license agree	ment and install Java now.
Change destination folder	Cancel Install >

Na úvodnej obrazovke zvoľte tlačidlo **Install**. Ďalej je proces inštalácie až do konca automatický. Inštalačný program si následne stiahne z internetu dodatočné súbory, ktoré potrebuje zavedenie JRE do vášho počítača.



Downloadi	ng Java Installer		×
Java ⁻	Downloading Instal Java installer files are b	l er being downloaded.	Sun
Estimate	d time left. 24 sec		
Java is fi Disc play	ound everywhere - on mol yers, set top boxes, and e	bile phones, desktop co ven in your car.	omputers, Blu-ray
By instal to you by	ling Java, you will be able / Sun Microsystems, Inc.	to experience the powe	er of Java, brought
Visitus e	t java.com		
		C	ancel install >





Na záverečnej obrazovke kliknite na tlačidlo **Close**. V tejto chvíli odporúčame prehliadač vypnúť a zapnúť, aby sa prejavili zmeny.



8. Riešenie problémov

V prípade vzniku chyby počas procesu generovania žiadosti budete informovaný chybovou hláškou.



V treťom odseku nájdete popis chyby.

Niektoré chyby môžu byť závažnejšieho technického rázu. Môžu súvisieť so stavom hardvérového alebo softvérového vybavenia vášho počítača. Je dôležité opísať, urobiť screenshot, alebo inak uchovať informácie z podrobného výpisu chybového hlásenia, pretože tieto informácie sú kritické pre rýchle vyriešenie problémov s helpdeskom.