

Obnova již vydaného kvalifikovaného certifikátu do elektronického občanského průkazu vybaveného kontaktním čipem

21 a 7 dnů před vypršením platnosti certifikátu je odesláno (na e-mail uvedený v certifikátu) upozornění na blížící se ukončení platnosti certifikátu. Obsahem tohoto e-mailu je URL odkaz, který Vám umožní provést elektronickou obnovu Vašeho certifikátu.

Vložte kartu (Váš eOP) do čtečky připojené k PC / spusťte skript pro obnovu certifikátu (URL) / tlačítkem „Zahájit test PC“ spusťte test kompatibility

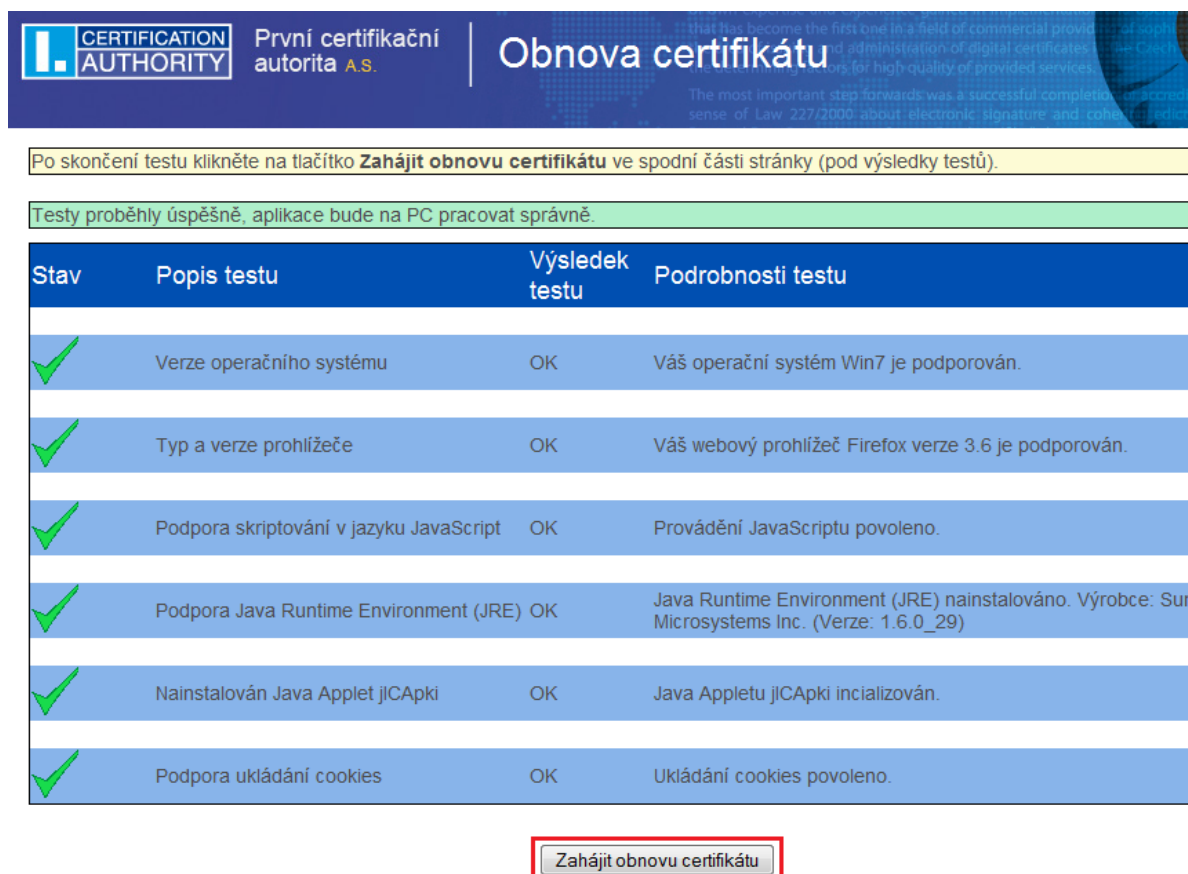


CERTIFICATION AUTHORITY První certifikační autorita A.S. | **Obnova certifikátu**

Nejdříve je nutné otestovat, zda Váš PC splňuje minimální požadavky pro bezproblémové dokončení procesu obnovy certifikátu v této webové aplikaci. Při testech můžete být požádáni o aktualizaci některých softwarových komponent, v takovémto případě prosím potvrďte souhlas s aktualizací komponent. Test zahájíte tlačítkem **Zahájit test PC**.

Copyright I.CA 2000-2011 All Right Reserved | První certifikační autorita, a.s. | Kontakty

Po úspěšném absolvování testu stiskněte tlačítko „Zahájit obnovu certifikátu“




CERTIFICATION AUTHORITY První certifikační autorita A.S. | **Obnova certifikátu**

Po skončení testu klikněte na tlačítko **Zahájit obnovu certifikátu** ve spodní části stránky (pod výsledky testů).

Testy proběhly úspěšně, aplikace bude na PC pracovat správně.

Stav	Popis testu	Výsledek testu	Podrobnosti testu
✓	Verze operačního systému	OK	Váš operační systém Win7 je podporován.
✓	Typ a verze prohlížeče	OK	Váš webový prohlížeč Firefox verze 3.6 je podporován.
✓	Podpora skriptování v jazyku JavaScript	OK	Provádění JavaScriptu povoleno.
✓	Podpora Java Runtime Environment (JRE)	OK	Java Runtime Environment (JRE) nainstalováno. Výrobce: Sun Microsystems Inc. (Verze: 1.6.0_29)
✓	Nainstalován Java Applet jCapki	OK	Java Appletu jCapki inicializován.
✓	Podpora ukládání cookies	OK	Ukládání cookies povoleno.

Na následující obrazovce zvolte jako typ úložiště klíče (CSP) „Microsoft Base Smart Card Crypto Provider“


První certifikační autorita A.S.

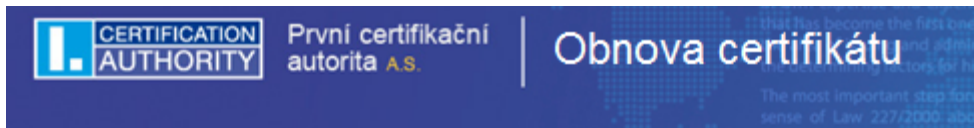
Obnova certifikátu

of own expertise and experience gained in implementation that has become the first one in a field of commercial providers and administration of digital certificates for high quality of provided services. The most important step forwards was a successful completion of a consultation process in sense of Law 227/2000 about electronic signature and related services. The OIA is for

Název položky	Vaše údaje	Popis
Certifikát		
Kvalifikovaný certifikát	<input type="text"/>	
Platnost do	12.10.2012 9:05:27	
Vydavatel	I.CA - Qualified Certification Authority, 09/2009	
Stát	CZ	
Obecné jméno	<input type="text"/>	
Organizace	První certifikační autorita, a.s.	
Pozice ve firmě	<input type="text"/>	
Sériové číslo	ICA - 10222243	
Alternativní jméno předmětu kvalifikovaného certifikátu		
E-mail (rfc822Name)	<input type="text"/>	
OtherName IK MPSV OID: 1.3.6.1.4.1.11801.2.1	<input type="text"/>	
Nastavení obnovy certifikátu		
Heslo pro zneplatnění	<input type="text" value="aaaaa"/>	Heslo pro zneplatnění smí obsahovat pouze číslice a písmena bez diakritiky. Délka hesla musí být 4 až 32 znaků. Pokud nezadáte nové heslo, bude jako heslo pro zneplatnění certifikátu použito heslo platné pro obnovovaný certifikát.
Typ úložiště klíče (CSP)	<input type="text" value="Microsoft Base Smart Card Crypto Provider"/>	

Poté prosím zkontrolujte, zda je opravdu jako typ úložiště klíče (CSP) uložen „**Microsoft Base Smart Card Crypto Provider**“,

dále zkontrolujte údaje v obnovovaném certifikátu a potvrďte vytvoření žádosti o obnovu stiskem tlačítka „**Vytvořit žádost**“



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

Rekapitulace údajů	
Název položky	Zadaná hodnota
Heslo pro zneplatnění	aaaaa
Doba platnosti certifikátu	365
Typ úložiště klíče (CSP)	Microsoft Base Smart Card Crypto Provider
Algoritmus kryptografie	sha256withRSAECNurypoun
Povolit export soukromého klíče	Ne
Povolit silnou ochranu soukromého klíče	Ne
Délka klíče	2048
Položky předmětu	
Kvalifikovaný certifikát	
Stat	CZ
Obecné jméno	
Organizace	První certifikační autorita, a.s.
Pozice ve firmě	
Sériové číslo	ICA - 10222243
Rozšířené položky certifikátu	
Kvalifikovaný certifikát	
E-mail (rfc822Name)	
OtherName IK MPSV OID: 1.3.6.1.4.1.11801.2.1	
Použití klíče	
Kvalifikovaný certifikát	
Non Repudiation	Ano
Digital Signature	Ano
Key Encipherment	Ne
Data Encipherment	Ne
Key Agreement	Ne

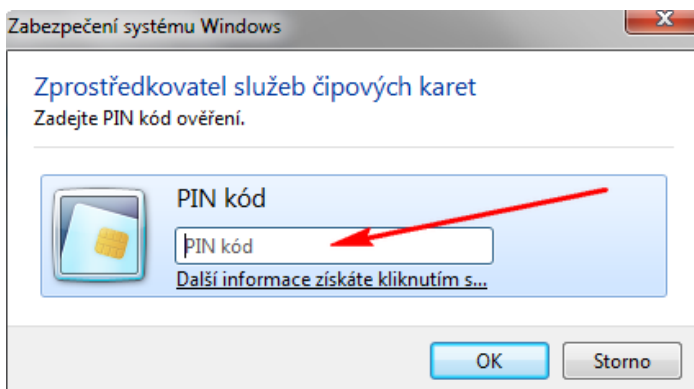
Vystavený certifikát a informaci o obnově certifikátu zaslat na e-mail:

Certifikát zaslat ve formátu ZIP:

Ano
 Ne

Vytvořit žádost

Zadejte svůj PIN (BOK) k Vašemu eOP a stiskněte „**OK**“



Vytvořenou žádost odešlete ke zpracování stiskem tlačítka „Odeslat žádost ke zpracování“



První certifikační autorita, a.s. (CA) was founded at the beginning of 2000. It has been operating since then as a leading provider of own expertise and experience gained in implementation of the first time in a field of commercial production and administration of digital certificates and services for high quality of provided services. The most important step forwards was a successful completion in sense of Law 227/2000 about electronic signature and certificates.

Žádost o obnovu certifikátu byla úspěšně vytvořena.
Kliknutím na tlačítko Odeslat žádost ke zpracování, bude vaše žádost o certifikát podepsána obnovovaným certifikátem a odeslána na zpracování.

Žádost o obnovu kvalifikovaného certifikátu:
-----BEGIN CERTIFICATE REQUEST-----
MIIDQCCAIwCAQAwgaoxCSAIBgNVBAYTAkNaMRswGQYDVQQDDDBJbmcuIFJvbWZuIEt1xI11cmEwLTAxR2RlbnVBAoMjFBydm7DzSBjZKJ0aWZpa2HEjW7DrSBhdXRvcml0YSwgYS5sLjE2MDQ6A1UEDAwT2Jj+G9kbsOtIMWZ2NkpdGVsIHNLZ211bnR1IHZ1x211am7DoSBchLDoX2hMRcwFYDVVQQFEw5JQ0EgLSAxdmIyMjI0MScCAStwDQYJKoZIhvcNAQEBBQAGggEPADCCAQoCggEBANicuwicTe/70dEG88ngwNHL30JnX4fFN029a0zo5UD0H3hbuZP7K0tX6Q874GvuuTJ5UAxWP C00dkXfgciOVw2jmDF4kAI0i1RjNt/Q1utyisit08h14TpuypFm68nXGQk+A9alaPoTW7F3g xvgmAYSTE3YFmeYnas4pFBJD+14jxXWf8tOKLiC+K27oRW3iTRDEzVl/IhDoXKjVVIhsjRMT am7sSVk9+OPsfPp/c++PGtO+XR1Em//JNv5I3uoNRr8u077fVMEJUEW2vHTyNSUV1A2oYEqJ 2GZTtDrXPU0w7v4PkP8L7dM6Q1bdX046UwZAKWZAxXo40G8N016RmrUCAwEAAaBTMFEGCSqG SIB3DQEJJDjFEMEIwCwYDVUR0PBAQDAggbAMDMGA1UdEQQ=MCgBDWt1Y2UyYUByZEUyY3ggGQYJ KwYBBAhcGQIBoAwMCjEaODkxNzQ2NTUwDQYJKoZIhvcNAQELBQADggEBAABNt4Vuu581ebI iQuLMPo001HsSe0Ak19ULPFGVTRnUZOLAjyUzfvk60aMNGLS9Q0W1mapwIT9hNINr25Qrpc p8y8kQdJXufiU112Vpi9Hs+00Aa0oqDR8m1DsZ1vy70rsFqgXSGZstgGDHvbdpNqMPCBI6 tFayQcPr5duhqmU2h7s8MD8nagtio9pQ+NDjQnde2Gp8jFgdi6vXKoP620=yrOB3UGP5eEKJ aPd0PkTEFw91baOTOn+sJ5ZR3qs1Oq45XAPU5dcbR0AJAyLvcinWzBjSCiawNGTm3fI3b1x 2hB2WPaE0sg5Sj5aInfSTJsiOVgDTV35T2x3Q4= -----END CERTIFICATE REQUEST-----

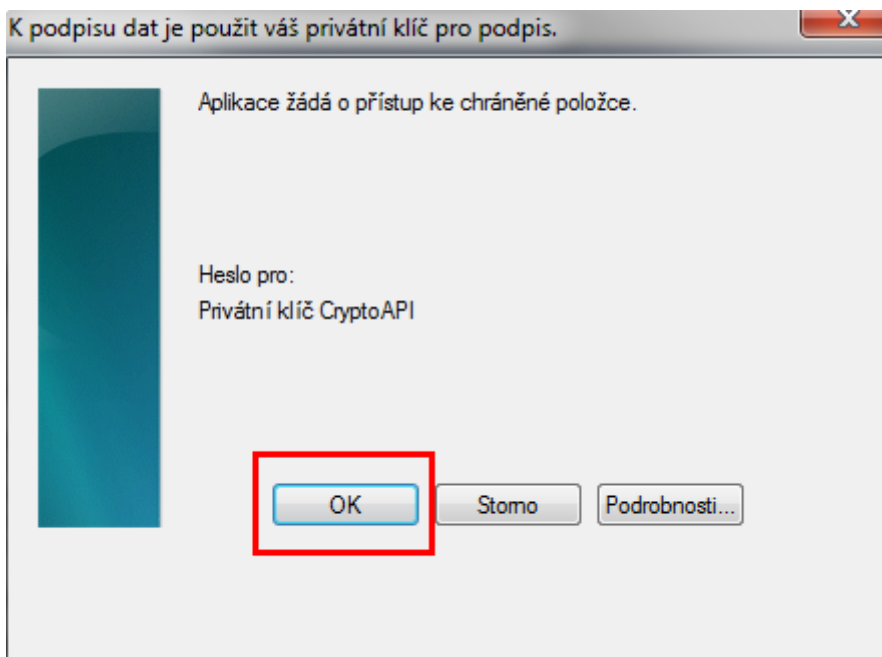
Odeslat žádost ke zpracování

Pokud si přejete vygenerovanou žádost uložit na Váš pevný disk klikněte na tlačítko Uložit žádost na disk.

Uložit žádost na disk

Parametry klíče, kterým bude podepsána žádost o obnovu certifikátu:
Jméno úložště klíče (CSP): Microsoft Enhanced RSA and AES Cryptographic Provider
Typ úložště klíče (CSP): PROV_RSA_AES
Jméno klíče: Objekt 13/10/2011 09:52:41
Typ klíče: AT_SIGNATURE

Žádost je třeba před odesláním **podepsat** obnovovaným certifikátem



K podpisu dat je použit váš privátní klíč pro podpis.

Aplikace žádá o přístup ke chráněné položce.

Heslo pro:
Privátní klíč CryptoAPI

OK Stomo Podrobnosti...

Žádost o obnovu certifikátu byla odeslána na I.CA ke zpracování.



CERTIFICATION AUTHORITY První certifikační autorita a.s. **Obnova certifikátu**

Žádost o obnovu certifikátu byla úspěšně přijata. ←

ID žádosti o kvalifikovaný certifikát: 5708610077742
Zde může sledovat stav Vaší žádosti s ID 5708610077742.
 Čas přijetí žádosti: 13.01.2012 12:44:33
 Po splnění fakturačních podmínek certifikační autority pro získání certifikátu, bude obnovený certifikát zaslán na e-mail - [redacted]

Copyright I.CA 2000-2011 All Right Reserved | První certifikační autorita, a.s. | Kontakt

Po splnění fakturačních podmínek (zaplacení zálohové faktury) bude certifikát obnoven.

Pokud jste při tvorbě žádosti o obnovu certifikátu uvedli svoji e-mailovou adresu, obdržíte zprávu, ve které je Váš nový (obnovený) certifikát.

Vážený kliente,

zasíláme Vám kvalifikovaný certifikát č. 10034244 (991C44 hex), vydaný pro žádost č. 5707010004671.

Pro instalaci osobního certifikátu klienta do operačního systému Windows (Internet Explorer) klikněte na tuto URL adresu:

https://testq.ica.cz/cgi-bin/certman_qpub.cgi?action=findcert&sn=10034244


Zobrazení této stránky dále umožňuje:

- import certifikátu na čipovou kartu STARCOS
- import certifikátu na elektronický občanský průkaz (eOP)
- registraci kořenových certifikátů
- nastavení certifikátu do MS Outlook
- vytvoření zálohy certifikátu s privátním klíčem do formátu PFX (pouze pro certifikát s úložištěm v PC)

Pro instalaci do jiné aplikace (SCP, RM-S, ...) instalujte dle návodu dodaného k danému produktu využívajícímu certifikáty.

V případě, že chcete certifikát instalovat bez návštěvy výše uvedené URL adresy, je možné využít příložené formáty certifikátu.

Děkujeme, že využíváte služeb První certifikační autority, a.s.

 10034244.zip

Kliknutím na zvýrazněný odkaz spustíte v internetovém prohlížeči aplikaci, která Vám umožní uložení certifikátu do elektronického občanského průkazu.

:: 1 :: Instalace certifikátu na čipovou kartu Starcos nebo eOP

V případě, že máte klíč k certifikátu uložen na čipové kartě Starcos nebo elektronickém občanském průkazu (eOP), klikněte na tlačítko "Importovat certifikát na kartu". Automaticky se Vám vyhledají chybějící certifikáty, uloží se na kartu a zaregistrují do Windows. V případě, že nemáte klíč k certifikátu uložen na čipové kartě nebo eOP, postupujte podle bodu 2 - "Zaregistrovat certifikát do Windows".

[Importovat certifikát na kartu](#)

Stisknutím tlačítka „**Importovat certifikát na kartu**“ zahájíte ukládání. V následující obrazovce stiskněte tlačítko **Instalovat**.

Zde si můžete provést instalaci certifikátů vydaných I.CA na čipovou kartu.
Stiskem tlačítka Instalovat zahájíte instalaci certifikátů na vaši čipovou kartu.
Před zahájením instalace vložte kartu do čtečky a na vyzvání zadejte PIN.
Po stisku tlačítka Instalovat vyčkejte dokončení instalace.

Registrovat certifikáty do MS Windows

Instalovat

Průběh instalace je popsán v následující obrazovce. Na konci výpisu je uvedena informace o výsledku instalace.

Zde si můžete provést instalaci certifikátů vydaných I.CA na čipovou kartu.
Stiskem tlačítka Instalovat zahájíte instalaci certifikátů na vaši čipovou kartu.
Před zahájením instalace vložte kartu do čtečky a na vyzvání zadejte PIN.
Po stisku tlačítka Instalovat vyčkejte dokončení instalace.

Registrovat certifikáty do MS Windows

Instalovat

Probíhá čtení obsahu čipové karty...

Název CSP: Microsoft Base Smart Card Crypto Provider

Čtení kontejneru "Objekt 04/01/2012 16:44:52": OK (identifikace klíče: 192F807E75698096A892E1D47328FFA13FDAB6C7)

Čtení kontejneru "20111221144814": OK (klíč nenalezen)

Čtení kontejneru "20111223104742": OK (klíč nenalezen)

Čtení kontejneru "Objekt 05/01/2012 09:49:16": OK (nalezen certifikát 10034244: C=CZ, CN=Alena Kvalifikovaný eOP, L="Praha", SERIALNUMBER=ICA - 10009209)

Čtení kontejneru "20111223105726": OK (identifikace klíče: AA40BE5F0BB44103EC0EF7FB333320D85AACC020)

Čtení kontejneru "20111223105837": OK (klíč nenalezen)

Čtení kontejneru "Objekt 03/01/2012 09:04:16": OK (nalezen certifikát 10034231: C=CZ, CN=Alena Kvalifikovaný eOP, L="Praha", SERIALNUMBER=ICA - 10009196)

Čtení kontejneru "Objekt 05/01/2012 13:26:12": OK (identifikace klíče: 08EC4117E62B8119BC93E5FFCC78DA80899F4A99)

Počet chybějících certifikátů: 3

Probíhá komunikace s certifikační autoritou...

Počet získaných platných certifikátů: 1

Probíhá import certifikátů na čipovou kartu...

Zápis certifikátu 10034249: OK (C=CZ, CN=Alena Kvalifikovaný eOP, SERIALNUMBER=ICA - 10009214)

Probíhá registrace certifikátů do MS Windows...

Zápis kořenových certifikátů: OK

Zápis certifikátu 10034249: OK

Instalace certifikátů byla úspěšně dokončena.

Pokud jste v žádosti neuvedli Vaši e-mailovou adresu, použijte k uložení certifikátu na elektronický občanský průkaz aplikaci na adrese <http://s.ica.cz/getcert4card.html>.