



ICAReNewZEP v1.0

Uživatelská příručka

Obsah

1 - ÚVOD	3
2 - POUŽITÉ ZKRATKY	3
3 – POŽADAVKY.....	4
3.1 – POŽADAVKY PRO SPRÁVNÝ CHOD APLIKACE	4
3.2 – POŽADAVKY NA OBNOVOVANÝ CERTIFIKÁT.....	4
4 - VÝBĚR CERTIFIKÁTU PRO OBNOVU.....	5
4.1 - ZOBRAZENÍ OBNOVOVANÉHO CERTIFIKÁTU	5
4.2 - HESLO PRO ZNEPLATNĚNÍ CERTIFIKÁTU	6
4.3 - ZMĚNA KEY USAGE	6
5 - KONTROLA POLOŽEK CERTIFIKÁTU	7
5.1 - CERTIFIKÁTY UMOŽŇUJÍCÍ KOMUNIKACI SE STÁTNÍ SPRÁVOU SLOVENSKÉ REPUBLIKY	7
5.1.1 - <i>Potřebné dokumenty</i>	8
6 - PODEPSÁNÍ ŽÁDOSTI	9
7 - ODESLÁNÍ ŽÁDOSTI	11
8 - ULOŽENÍ ŽÁDOSTI NA POČÍTAČ	11
9 - OBNOVA CERTIFIKÁTU Z EXISTUJÍCÍ ŽÁDOSTI	12

1 - Úvod

Tento dokument slouží jako uživatelská příručka k programu ICAReNewZEP. Program je určen pro tvorbu a odeslání žádostí o obnovu kvalifikovaných certifikátů a produktů TWINS na server certifikační autority, kde jsou žádosti dále zpracovány. Žádost je před odesláním podepsána zaručeným elektronickým podpisem. Komunikace se serverem certifikační autority probíhá po zabezpečeném spojení.

2 - Použité zkratky

Zkratka	Vysvětlení
ICAReNewZEP	Název této aplikace
Certifikát	Datová zpráva, která je vydána poskytovatelem certifikačních služeb, spojuje veřejný klíč s podepisující, šifrující nebo autentizující se osobou a umožňuje ověřit její identitu
OID	Identifikátor objektu certifikátu
TWINS	Produkt I.CA, obsahující dvojici certifikátů: <ul style="list-style-type: none"> • kvalifikovaný certifikát – vydaný v souladu s platnou legislativou vztahující se k problematice elektronického podpisu • komerční certifikát – vydaný výhradně na základě smluvního vztahu mezi I.CA a koncovým uživatelem
ZEP	Zaručený elektronický podpis
pkcs#10	Formát žádosti o obnovu certifikátu
pkcs#7	Formát podepsané žádosti o obnovu certifikátu
CRL	Seznam zneplatněných certifikátů
1.CA	První certifikační autorita, a.s.
SSCD	Zařízení pro bezpečné vytváření elektronického podpisu
Key Usage	Použití klíče

3 – Požadavky

3.1 – Požadavky pro správný chod aplikace

Aplikace je určena pro operační systém Microsoft Windows Vista a vyšší. Pro chod aplikace je nutné mít v úložišti důvěryhodných kořenových certifikátů nainstalovaný certifikát kořenové certifikační autority Slovenského Národního bezpečnostního úřadu. Tento certifikát lze stáhnout z URL http://ep.nbusr.sk/kca/certifikat_kca3.html. Dále je nutné mít v úložišti zprostředkujících certifikačních autorit nainstalovaný certifikát I.CA kvalifikované certifikační autority podepsaný Národním bezpečnostním úřadem Slovenské republiky. Tento certifikát lze stáhnout z URL http://www.nbusr.sk/ipublisher/files/nbusr.sk/certifikaty/ica_20091124.cer.

Aplikace vyžaduje připojení k internetu pro ověření platnosti obnovovaného certifikátu a k odeslání žádosti o obnovu na server certifikační autority.

3.2 – Požadavky na obnovovaný certifikát

Aplikací ICAReNewZEP je možné obnovit pouze kvalifikované certifikáty a certifikáty produktu TWINS, vydané v souladu se slovenskou legislativou, tj. uložené na SSCD a obsahující OID=1.3.158.36061701.0.0.0.1.2.2. Obnovovaný certifikát musí být nainstalován v osobním úložišti certifikátů ve Windows. Pro obnovu je nutné vlastnit privátní klíč obnovovaného certifikátu.

4 - Výběr certifikátu pro obnovu

Po spuštění aplikace je zobrazena domovská stránka, kde je možné v odstavci *Obnovovaný certifikát* vybrat certifikát k obnově. V nabídce jsou zobrazeny pouze certifikáty splňující požadavky na obnovu. Certifikáty produktu TWINS jsou označeny textem (T) na začátku řádku a kvalifikované certifikáty řetězcem (Q) na začátku řádku. Informace o vystaviteli certifikátu jsou zobrazeny v textovém poli pod vybraným certifikátem k obnově.

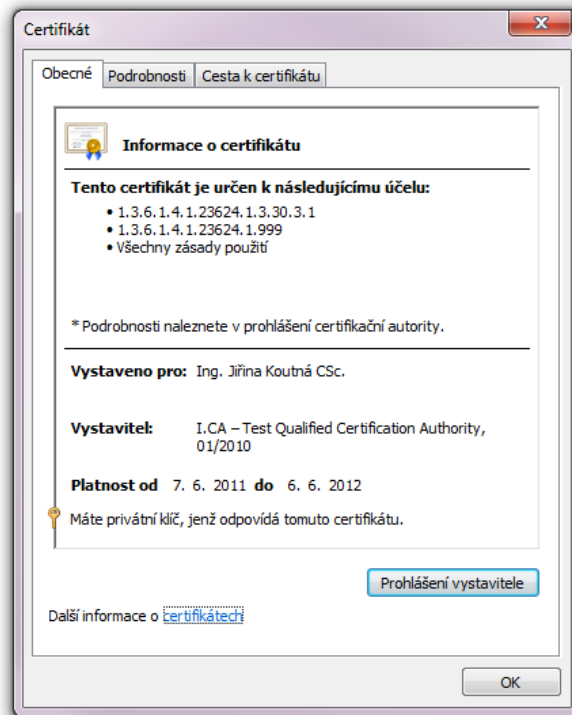
The screenshot shows a web browser window titled 'ICARENewZEP v1.0'. The page header features the 'CERTIFICATION AUTHORITY' logo and the text 'První certifikační autorita A.S.' and 'Žiadosť o obnovu certifikátu'. The main content area is titled 'Žiadosť o obnovu certifikátu' and contains the following form elements:

- Obnovit certifikát**: A section header.
- Obnovovaný certifikát**: A dropdown menu with the selected value '(T) C=CZ, CN=Petr Janousek, S=Praha, L=Praha 9, Slavetinska 5/5, 19014*, O=První certifikát'. Below the dropdown, the text 'ICA - Development qualified root certificate 2009 | ICA - Development standard root certificate 200' is visible, along with a 'Zobrazit certifikát' button.
- Heslo pre zneplatnenie certifikátu**: A text input field with the placeholder '(Nemusi byť zhodné s prvotným heslom.)'.
- Overenie hesla**: A second text input field.
- Doplnenie žiadosti žiadateľom**: Radio buttons for 'Áno' and 'Nie'.
- Pokračovať**: A button below the radio buttons.
- Obnovit certifikát z existujúcej žiadosti**: A section header.
- Cesta k súboru so žiadosťou**: A text input field with a yellow background, followed by a 'Prochádzet' button.
- Pokračovať**: A button below the 'Prochádzet' button.

The status bar at the bottom of the window shows 'Hotovo' on the left and 'NUM' on the right.

4.1 - Zobrazení obnovovaného certifikátu

Stiskem tlačítka *Zobrazit certifikát* v kolonce *Obnovovaný certifikát* v domovské stránce je možné vyvolat standardní okno s informacemi o certifikátu.



4.2 - Heslo pro zneplatnění certifikátu

Heslo pro zneplatnění obnovovaného certifikátu je nepovinná položka. V případě vyplnění hesla pro zneplatnění certifikátu musí mít heslo délku v rozmezí 4–32 znaků a může být tvořeno znaky 0-9, A-Z a a-z.

Heslo pre zneplatnenie certifikátu:

(Nemusi byť zhodné s prvotným heslom.)

Overenie hesla:

4.3 - Změna key usage

Změna key usage je umožněna pouze u kvalifikovaných sólo certifikátů zaškrtnutím políčka *Áno* v kolonce *Doplnenie žiadosti žiadateľom* v úvodní obrazovce. Samotnou změnu key usage je možné provést na obrazovce kontroly položek certifikátu.

Doplnenie žiadosti žiadateľom Áno Nie

5 - Kontrola položek certifikátu

Aplikace přejde na stránku kontroly položek certifikátu po vybrání obnovovaného certifikátu v domácí stránce a kliknutí na tlačítko *Pokračovať*. Na stránce kontroly položek certifikátu je nutné zkontrolovat správnost uvedených údajů. Pokud některý údaj nesouhlasí, není možné v obnově pokračovat. V případě sólo kvalifikovaného certifikátu je možné na této stránce provést změnu key usage, byla-li tato možnost povolena v domácí stránce aplikace. Pokud obnovovaný certifikát neobsahuje identifikátor pro komunikaci se státní správou Slovenské Republiky, je možné jej na této stránce do obnovovaného certifikátu doplnit, zaškrtnutím políčka *Certifikát pre komunikáciu so štátnou správou SR*. Dále je zde možné zvolit, zda má být obnovovaný certifikát zaslán na e-mail v archivu ZIP nebo nikoliv.

Skontrolujte si prosím nižšie uvedené údaje. Ak sú v poriadku, je možné vytvoriť žiadosť o obnovenie certifikátu.

Názov položky	Kvalifikovaný certifikát	Komerčný certifikát
Dĺžka kľúča	2048 b	2048 b
Dĺžka platnosti	12 mesiacov	12 mesiacov
HASH algoritmus	sha256RSA (1.2.840.113549.1.1.11)	sha256RSA (1.2.840.113549.1.1.11)
Key usage	<input checked="" type="checkbox"/> Non Repudiation · <input checked="" type="checkbox"/> Digital Signature · <input type="checkbox"/> Key Encipherment · <input type="checkbox"/> Data Encipherment · <input type="checkbox"/> Key Agreement ·	<input type="checkbox"/> Non Repudiation · <input checked="" type="checkbox"/> Digital Signature · <input checked="" type="checkbox"/> Key Encipherment · <input checked="" type="checkbox"/> Data Encipherment · <input checked="" type="checkbox"/> Key Agreement ·
Typ kľúča (CSP)	SecureStoreCSP	SecureStoreCSP

Email

Vlastnosť	Nastavení
Certifikát zaslať vo formáte ZIP	<input type="radio"/> Ano · <input checked="" type="radio"/> Ne

Komunikácia so štátnou správou

Identifikátor	hodnota
Certifikát pre komunikáciu so štátnou správou	

5.1 - Certifikáty umožňujúci komunikaci se státní správou slovenské republiky

V prípade, že obnovovaný certifikát neobsahuje identifikátor pro komunikaci se státní správou Slovenské Republiky, je možné na stránce kontroly položek certifikátu tento identifikátor do obnovovaného certifikátu doplnit zaškrtnutím příslušného tlačítka. V případě doplnění identifikátoru a potvrzení položek obnovovaného certifikátu, přejde aplikace po stisku tlačítka *Doplniť údaje SK* na stránku doplnění informací o držiteli certifikátu. Občané Slovenské Republiky musejí jako identifikátor vyplnit své rodné číslo.

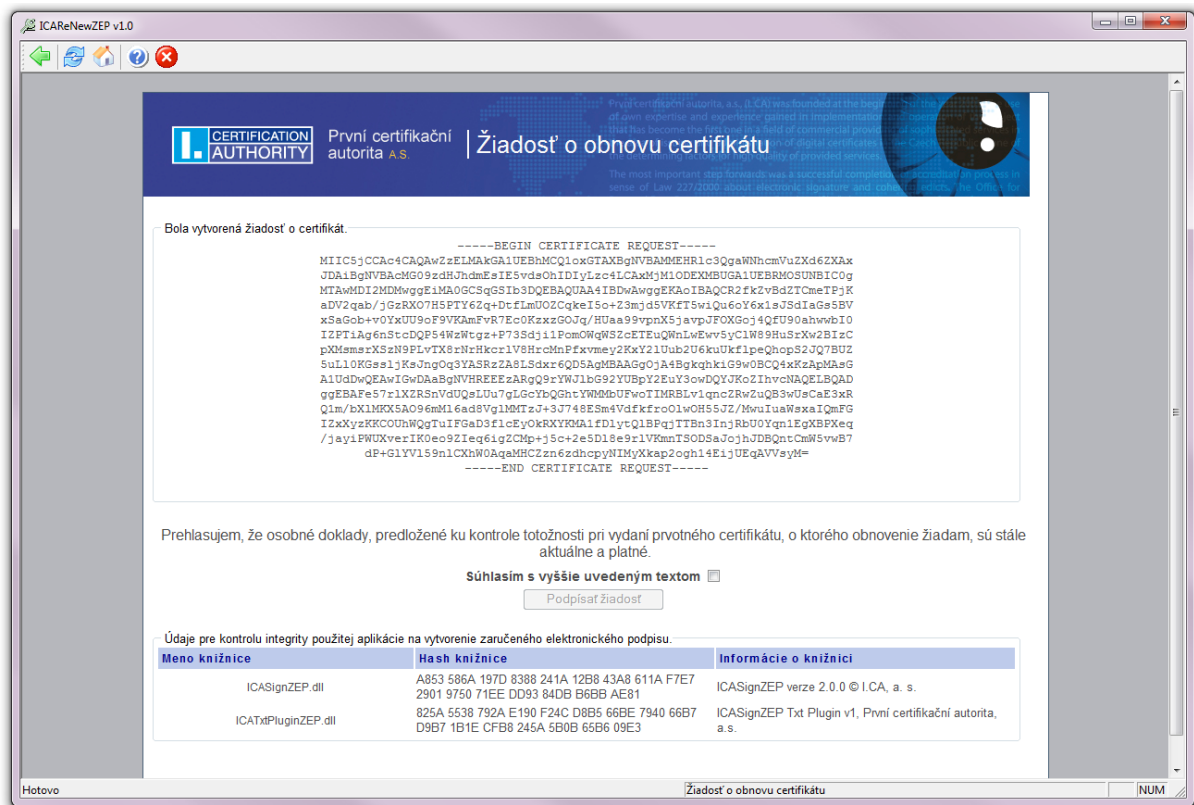
The screenshot shows a web browser window titled "ICAReNewZEP v1.0". The page header includes the logo for "První certifikační autorita a.s." and the title "Žiadosť o obnovu certifikátu". Below the header, there is a paragraph of text in Slovak explaining the legal requirements for electronic signatures. A form titled "obnoviť certifikát" contains three input fields: "Typ Identifikátora" (set to "Občiansky preukaz"), "Vystavovateľ rodného čísla/doklad" (set to "Česká republika"), and "Číslo občianskeho preukazu" (empty). Below the form is a "Rekapitulácia žiadosti" section listing details for the certificate holder, including name, serial numbers, and address. At the bottom, a "Doplnenie identifikátora" section shows the selected identification type and issuer. The browser's status bar at the bottom indicates "Hotovo" and "NUM".

5.1.1 - Potřebné dokumenty

Občané Slovenské republiky musejí jako identifikátor pro komunikaci se státní správou Slovenské republiky vyplnit své rodné číslo. Příslušníci ostatních států musejí jako identifikátor vyplnit číslo svého cestovního pasu nebo číslo svého občanského průkazu.

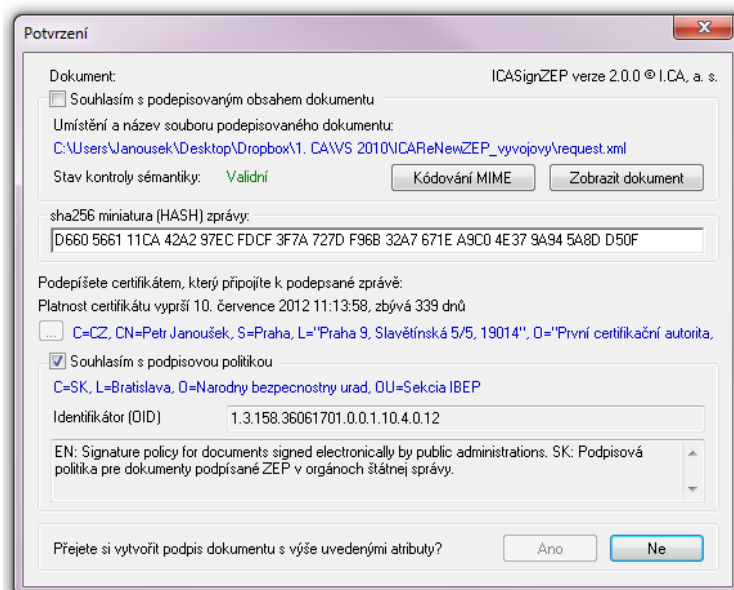
6 - Podepsání žádosti

Po potvrzení položek certifikátu a případného doplnění informací o držiteli certifikátu při doplnění identifikátoru pro komunikaci se Státní Správou Slovenské republiky přejde aplikace na stránku podepsání žádosti o obnovu certifikátu. Na stránce podpisu žádosti je zobrazena žádost ve formátu pkcs#10. V případě obnovy TWINS jsou zobrazeny dvě žádosti. Aplikace před podpisem žádostí kontroluje pravost knihoven použitých při tvorbě zaručeného elektronického podpisu. Dodatečnou kontrolu je možné provést porovnáním zobrazených hodnot otisků vůči hodnotám otisků zveřejněných certifikační autoritou.

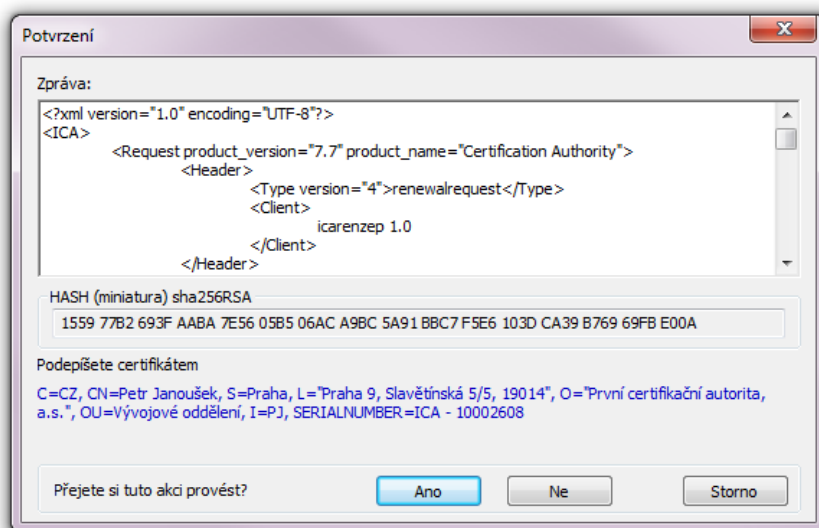


Před podepsáním žádosti je nutné souhlasit s uvedeným textem zaškrtnutím tlačítka. Žádost je podepsána po kliknutí na tlačítko *Podepsat žádost*.

Po kliknutí na tlačítko *Podepsat žádost* je zobrazen dialog v němž je nutno potvrdit souhlas s obsahem podepisovaného dokumentu. V dialogu je možné zobrazit obsah podepisovaného dokumentu, obnovovaný certifikát, kterým bude žádost podepsána a podpisová politika.



V případě obnovy TWINS je před podpisem komerčního certifikátu zobrazen dialog podpisu. V dialogu je zobrazen obsah podepisovaného dokumentu a je zde možné zobrazit obnovovaný certifikát, kterým bude žádost podepsána.

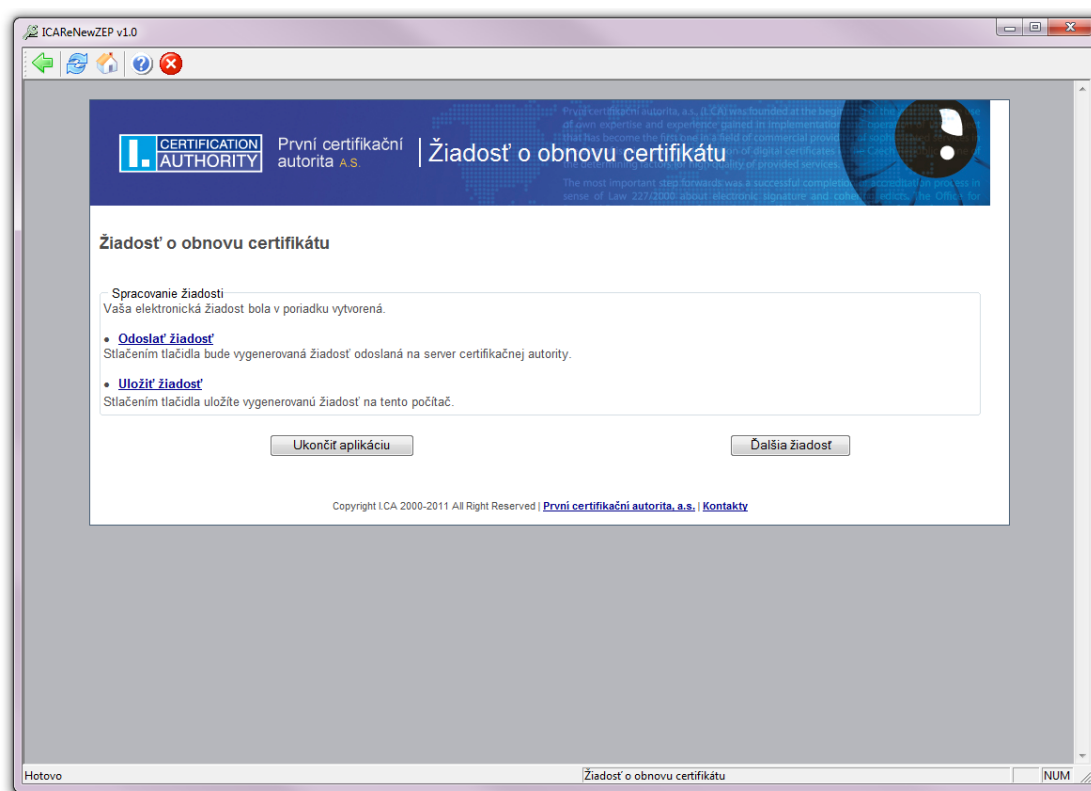


7 - Odeslání žádosti

Po podepsání žádostí o obnovu certifikátu, nebo po načtení předvytvořené žádosti přejde aplikace na stránku, kde je možné odeslat žádost ke zpracování a žádost uložit. Žádost se odešle kliknutím na tlačítko *Odeslat žádost*.

Po úspěšném odeslání žádosti na server certifikační autority je zobrazen text o úspěchu a číslo, pod kterým byla žádost přijata.

Po neúspěšném odeslání žádosti na server certifikační autority je zobrazen text o neúspěchu a konkrétní chybové hlášení. Je možné, pokusit se o další odeslání.



8 - Uložení žádosti na počítač

Po vytvoření žádosti o obnovu certifikátu, nebo jejím nahrání z místního počítače je možné žádost uložit na místní počítač. Uložení žádosti se provede kliknutím na tlačítko *Uložit žádost* v závěrečné obrazovce.

9 - Obnova certifikátu z existující žádosti

Předvytvořenou žádost o obnovu certifikátu je možné načíst v kolonce Obnovit certifikát z existující žádosti úvodní obrazovky.

Obnovit certifikát z existující žádosti

Cesta k souboru so žádostí

Procházet

Pokračovat