ICAReNewZEP v1.2

Užívateľská príručka

19.7.2011

Obsah

1 – Úvod

Tento dokument slúži ako užívateľská príručka k programu ICAReNewZEP. Program je určený pre tvorbu a odoslanie žiadostí o obnovu kvalifikovaných certifikátov a produktov TWINS na server certifikačnej autority, kde sú žiadosti ďalej spracované. Žiadosť je pred odoslaním podpísaná zaručeným elektronickým podpisom. Komunikácia so serverom certifikačnej autority prebieha po zabezpečenom spojení.

2 - Použité skratky

Zkratka	Vysvětlení
ICAReNewZEP	Názov tejto aplikácie
Certifikát	Dátová správa, ktorá je vydaná poskytovateľom certifikačných služieb, spája verejný kľúč s podpisujúcou, šifrujúcou alebo autentizujúcou sa osobou a umožňuje overiť jej identitu
OID	Identifikátor objektu certifikátu
TWINS (platí pre ČR)	Produkt I. CA, obsahujúci dvojicu certifikátov: • kvalifikovaný certifikát - vydaný v súlade s platnou legislatívou vzťahujúci sa k problematike elektronického podpisu • komerčný certifikát - vydaný výhradne na základe zmluvného vzťahu medzi I. CA a koncovým užívateľom
ZEP	Zaručený elektronický podpis
pkcs#10	Formát žiadosti o obnovu certifikátu
pkcs#7	Formát podpísanej žiadosti o obnovu certifikátu
CRL	Zoznam zrušených certifikátov
1.CA	První certifikační autorita, a.s.
SSCD	Zariadenie pre bezpečné vytváranie elektronického podpisu
Key Usage	Použitie kľúča

3 – Požiadavky

3.1 – Požiadavky pre správny chod aplikácie

Aplikácia je určená pre operačný systém Microsoft Windows Vista a vyšší. Pre chod aplikácie je nutné mať v úložisku dôveryhodných koreňových certifikátov nainštalovaný certifikát koreňovej certifikačnej autority Národného bezpečnostného úradu SR. Tento certifikát je možné stiahnuť z URL http://ep.nbusr.sk/kca/certifikat_kca3.html. Ďalej je nutné mať v úložisku sprostredkujúcich certifikačných autorít nainštalovaný certifikát I. CA akreditovanej certifikačnej autority podpísanej Národným bezpečnostným úradom Slovenskej republiky. Tento certifikát je možné stiahnuť z URL http://www.nbusr.sk/ipublisher/files/nbusr.sk/certifikaty/ica_20091124.cer.

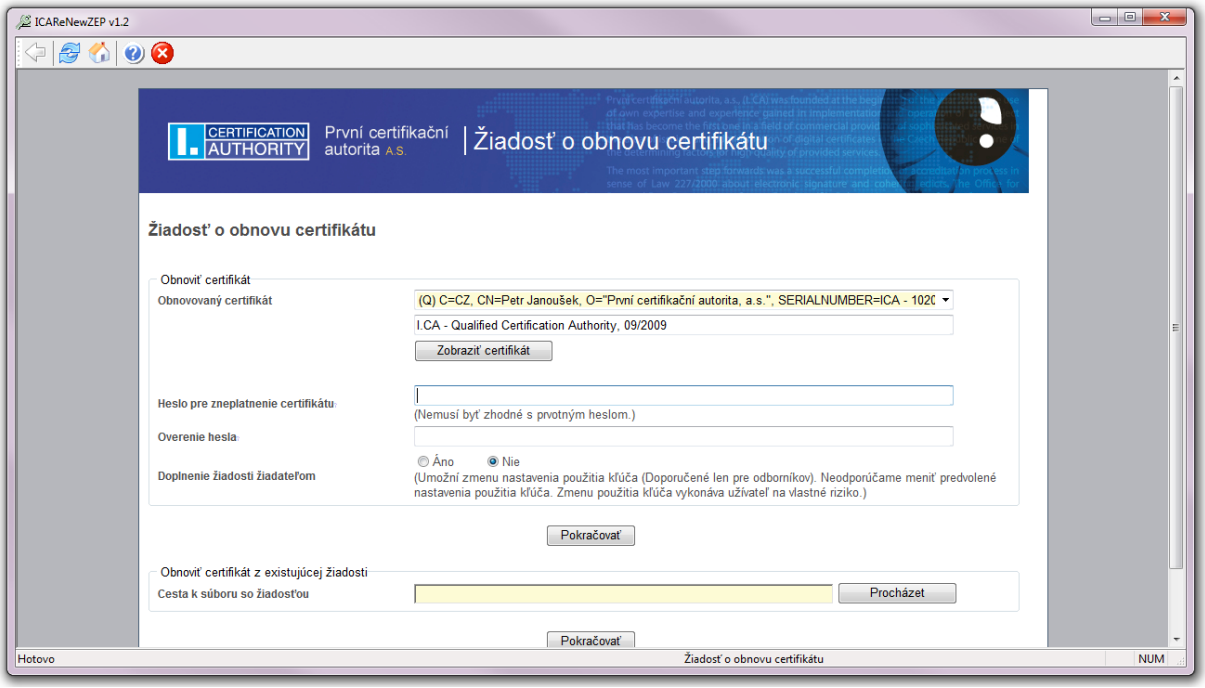
Aplikácia vyžaduje pripojenie k internetu pre overenie platnosti obnovovaného certifikátu a odoslanie žiadosti o obnovu na server certifikačnej autority.

3.2 – Požiadavky na obnovovaný certifikát

Aplikáciou ICAReNewZEP je možné obnoviť len kvalifikované certifikáty a certifikáty produktu **TWINS (platí pre ČR),** vydané v súlade so slovenskou legislatívou, tj. uložené na SSCD a obsahujúce OID = 1.3.158.36061701.0.0.0.1.2.2. Obnovovaný certifikát musí byť nainštalovaný v osobnom úložisku certifikátov vo Windows. Pre obnovu je nutné vlastniť privátny kľúč obnovovaného certifikátu.

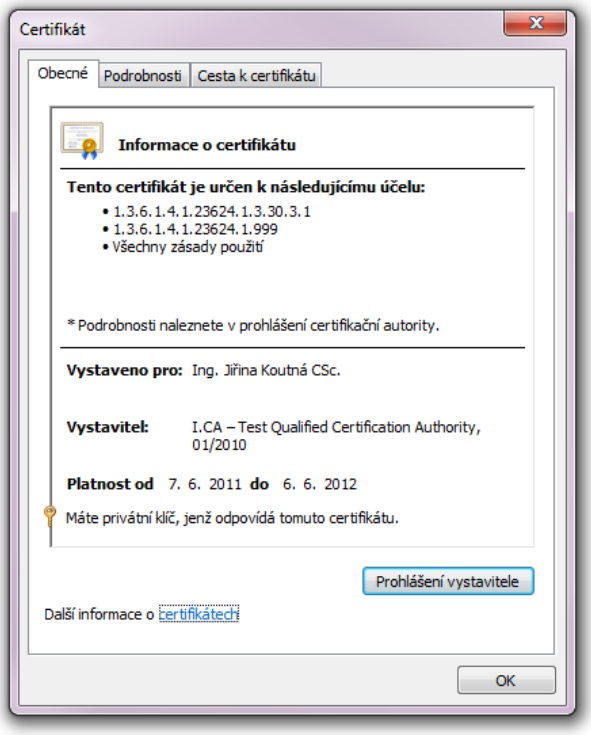
4 - Výber certifikátu pre obnovu

Po spustení aplikácie je zobrazená domovská stránka, kde je možné v odseku *Obnovovaný certifikát* vybrať certifikát k obnove. V ponuke sú zobrazené len certifikáty spĺňajúce požiadavky na obnovu. Certifikáty produktu TWINS (platí pre ČR) sú označené textom *(T)* na začiatku riadku a kvalifikované certifikáty reťazcom *(Q)* na začiatku riadku. Informácie o vydavateľovi certifikátu sú zobrazené v textovom poli pod vybraným certifikátom k obnove.



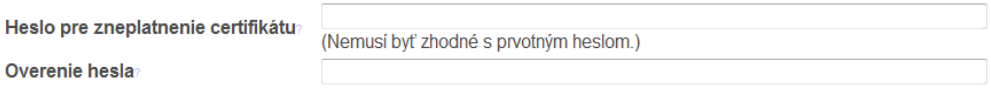
4.1 - Zobrazenie obnovovaného certifikátu

Stlačením tlačidla *Zobraziť certifikát* v kolónke *Obnovovaný certifikát* v domovskej stránke je možné vyvolať štandardné okno s informáciami o certifikáte.



4.2 - Heslo pre zneplatnenie certifikátu

Heslo pre zneplatnenie obnovovaného certifikátu je nepovinná položka. V prípade vyplnenia hesla pre zneplatnenie certifikátu musí mať heslo dĺžku v rozmedzí 4–32 znakov a môže byť tvorené znakmi *0-9*, *A-Z* a *a-z*.

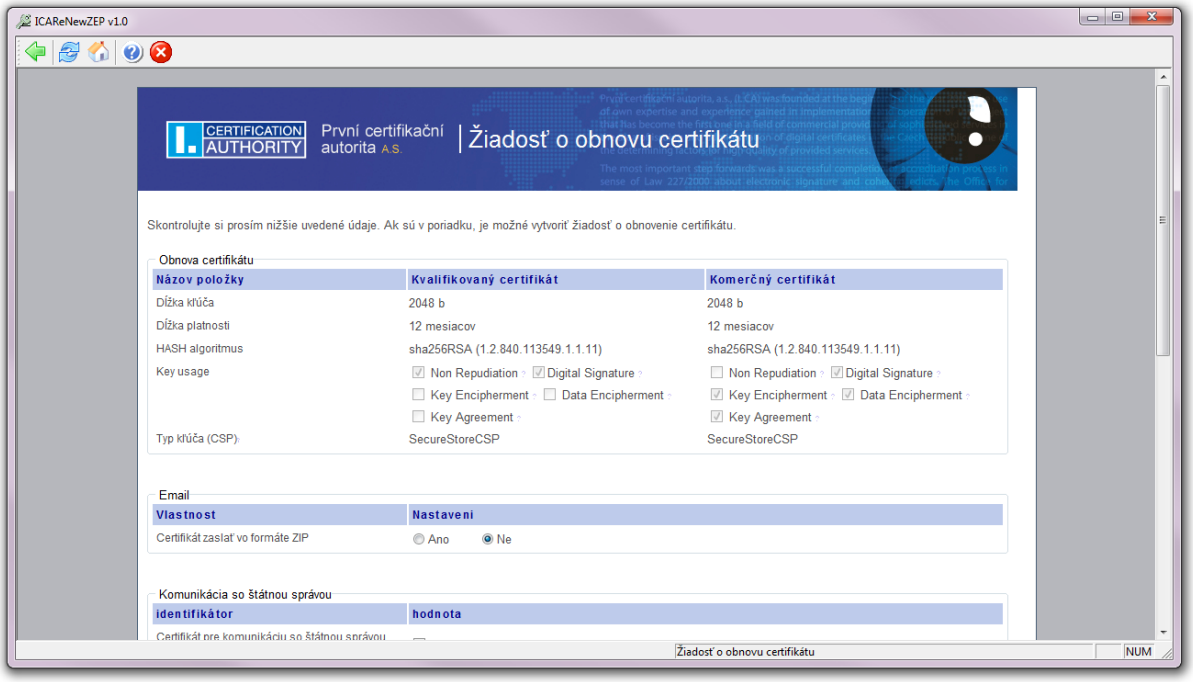


4.3 - Zmena key usage

Zmena key usage je umožnená iba u kvalifikovaných sólo certifikátov zaškrtnutím políčka *Áno* v kolónke *Doplnenie žiadosti žiadateľom* v úvodnej obrazovke. Samotnú zmenu key usage je možné vykonať na obrazovke kontroly položiek certifikátu .

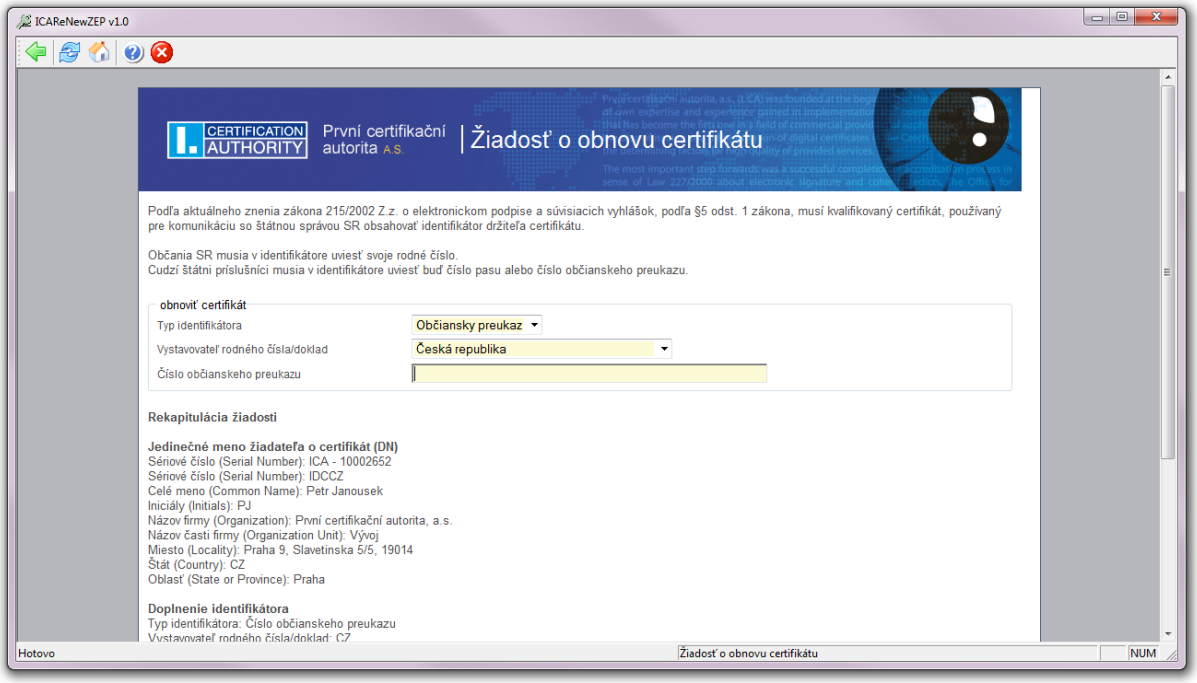
5 - Kontrola položiek certifikátu

Aplikácia prejde na stránku kontroly položiek certifikátu po vybraní obnovovaného certifikátu v domácej stránke a kliknutí na tlačidlo *Pokračovať*. Na stránke kontroly položiek certifikátu je nutné skontrolovať správnosť uvedených údajov. Ak niektorý údaj nesúhlasí, nie je možné v obnove pokračovať. V prípade sólo kvalifikovaného certifikátu je možné na tejto stránke vykonať zmenu key usage, ak bola táto možnosť povolená v domácej stránke aplikácie. Ak obnovovaný certifikát neobsahuje identifikátor pre komunikáciu so štátnou správou Slovenskej Republiky, je možné ho na tejto stránke do obnovovaného certifikátu doplniť, zaškrtnutím políčka *Certifikát pre komunikáciu so štátnou správou SR*. Ďalej je tu možné zvoliť, či má byť obnovený certifikát zaslaný na e-mail v archíve ZIP alebo nie.



5.1 - Certifikáty umožňujúce komunikáciu so štátnou správou slovenskej republiky

V prípade, že obnovovaný certifikát neobsahuje identifikátor pre komunikáciu so štátnou správou Slovenskej Republiky, je možné na stránke kontroly položiek certifikátu tento identifikátor do obnoveného certifikátu doplniť zaškrtnutím príslušného políčka. V prípade doplnenia identifikátora a potvrdenie položiek obnovovaného certifikátu, prejde aplikácia po stlačení tlačidla *doplniť údaje* SK na stránku doplnenie informácií o držiteľovi certifikátu. Občania Slovenskej Republiky musia ako identifikátor vyplniť svoje rodné číslo.

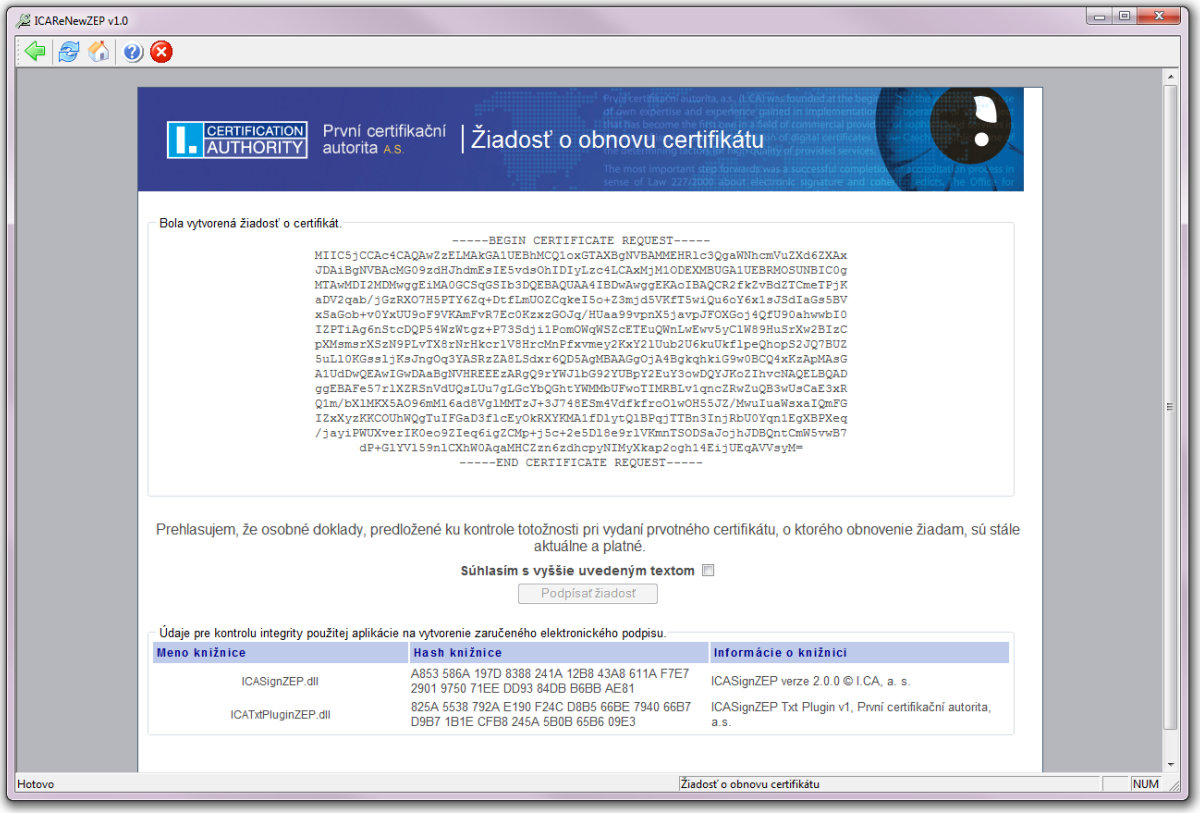


5.1.1 - Potrebné dokumenty

Občania Slovenskej republiky musia ako identifikátor pre komunikáciu so štátnou správou Slovenskej republiky vyplniť svoje rodné číslo. Príslušníci ostatných štátov musia ako identifikátor vyplniť číslo svojho pasu alebo číslo svojho občianskeho preukazu.

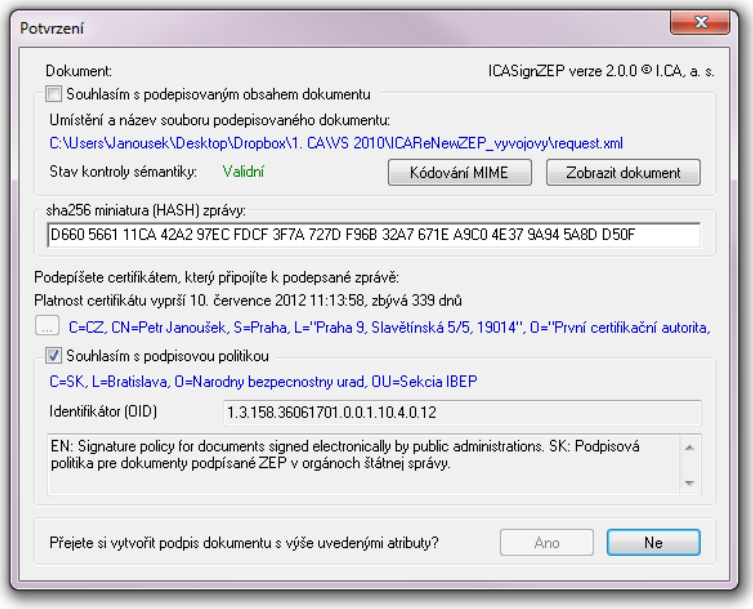
6 - Podpísanie žiadosti

Po potvrdenie položiek certifikátu a prípadného doplnenia informácií o držiteľovi certifikátu pri doplnení identifikátora pre komunikáciu so Štátnou Správou Slovenskej republiky prejde aplikácia na stránku podpísanie žiadosti o obnovu certifikátu. Na stránke podpisu žiadosti je zobrazená žiadosť vo formáte pkcs#10. V prípade obnovy TWINS sú zobrazené dve žiadosti (platí pre ČR). Aplikácia pred podpisom žiadostí kontroluje pravosť knižníc použitých pri tvorbe zaručeného elektronického podpisu. Dodatočnú kontrolu je možné vykonať porovnaním zobrazených hodnôt odtlačkov voči hodnotám odtlačkov zverejnených certifikačnou autoritou.



Pred podpísaním žiadosti je nutné súhlasiť s uvedeným textom zaškrtnutím políčka pri texte „Súhlasím s vyššie uvedeným textom“. Žiadosť je podpísaná po kliknutí na tlačidlo *Podpísať žiadosť*.

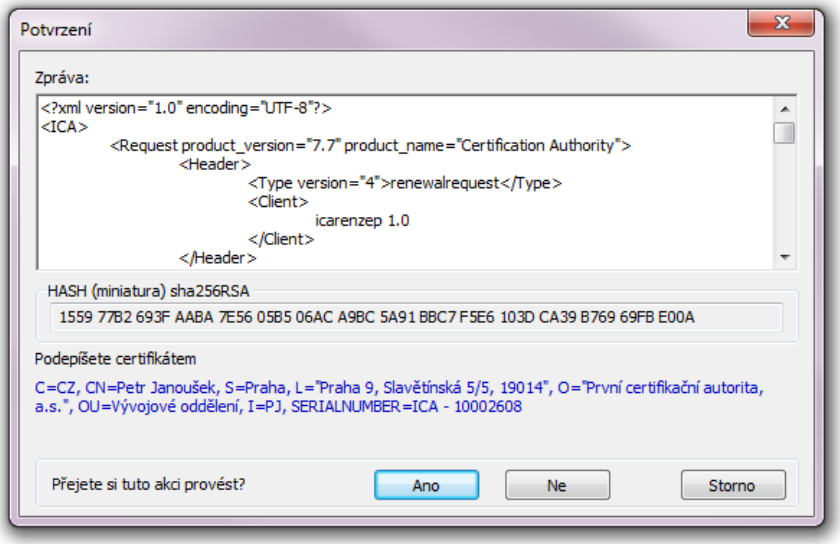
Po kliknutí na tlačidlo *Podpísať žiadosť* je zobrazený dialóg v ktorom je nutné potvrdiť súhlas s obsahom podpisovaného dokumentu. V dialógu je možné zobraziť obsah podpisovaného dokumentu, obnovovaný certifikát, ktorým bude žiadosť podpísaná a podpisovú politiku.



Podpísanie je možné vtedy, keď podpisujúci odsúhlasil podpisovaný obsah dokumentu zaškrtnutím políčka pri texte „Souhlasím s podepisovaným obsahem dokumentu“ a je tiež zaškrtnutý súhlas s podpisovou politikou, t.j. zaškrtnuté políčko pri texte „Souhlasím s podpisovou politikou“.

V referencii na podpisovú politiku má byť uvedená aktuálne platná podpisová politika Národného bezpečnostného úradu SR, ktorá je zverejnené na webe NBU SR, tu: http://www.nbusr.sk/sk/elektronicky-podpis/podpisove-politiky/zoznam-schvalenych-podpisovych-politik/index.html. Kontrola je možná porovnaním identifikátorov OID.

V prípade obnovy TWINS je tiež pred podpisom komerčného certifikátu zobrazený dialóg podpisu (platí pre ČR). V dialógu je zobrazený obsah podpisovaného dokumentu a je tu možné zobraziť obnovovaný certifikát, ktorým bude žiadosť podpísaná.

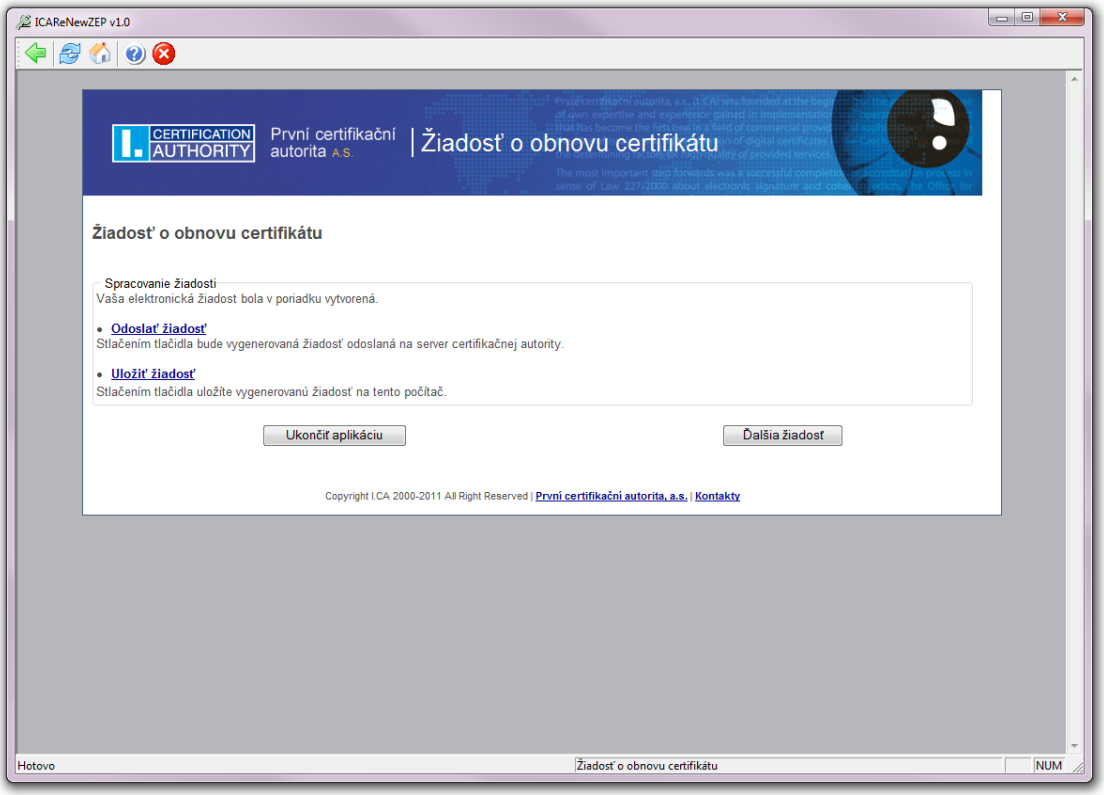


7 - Odoslanie žiadosti

Po podpísaní žiadostí o obnovu certifikátu, alebo po načítaní vopred pripravenej žiadosti prejde aplikácia na stránku, kde je možné odoslať žiadosť na spracovanie a žiadosť uložiť. Žiadosť sa odošle kliknutím na tlačidlo *Odoslať žiadosť.*

Po úspešnom odoslaní žiadosti na server certifikačnej autority je zobrazený text o úspechu a číslo, pod ktorým bola žiadosť prijatá.

Po neúspešnom odoslaní žiadosti na server certifikačnej autority je zobrazený text o neúspechu a konkrétne chybové hlásenie. Je možné, pokúsiť sa o ďalšie odoslania.



8 - Uloženie žiadosti na počítač

Po vytvorení žiadosti o obnovu certifikátu, alebo jej nahraním z lokálneho počítača je možné žiadosť uložiť na lokálny počítač. Uloženie žiadosti sa vykoná kliknutím na tlačidlo *Uložiť žiadosť* v záverečnej obrazovke.

9 - Obnova certifikátu z existujúcej žiadosti

Vopred pripravenú žiadosť o obnovu certifikátu je možné načítať v kolónke *Obnoviť certifikát z existujúcej žiadosti* úvodnej obrazovky.