Uživatelská příručka RA pro ČSOB

Datum: prosinec 2019
Verze: 3.0

Obsah

1. Úvod

Programové vybavení Registrační autority I.CA (dále jen „ICARA“) je instalováno a provozováno na vyhrazených počítačích po uzavření smlouvy o zřízení RA. Instalaci a konfiguraci ICARA může provádět pouze pracovník pověřený I.CA. Obsluha RA musí absolvovat školení organizované I.CA. Přístup k funkcím ICARA je umožněn pouze ve spojení s ověřenou čipovou kartou, tedy pouze držiteli karty. Obsluha RA musí dodržovat platné Certifikační politiky I.CA (dále jen „CP“), platné Směrnice pro operátory RA I.CA (dále jen „Směrnice“), metodické pokyny pro operátory I.CA. Software RA smí být používán pouze pro účely vymezené Certifikačními politikami I.CA.

2. Účel aplikace

Aplikace Registrační autorita představuje klientské rozhraní k systémům I.CA určeným pro vydávání a evidenci digitálních certifikátů pro oblast PKI.
Certifikáty jsou vydávány na základě **žádostí o certifikáty** podle normy PKCS#10 a jsou vyhotovovány dle standardu X509 v souladu s CP.

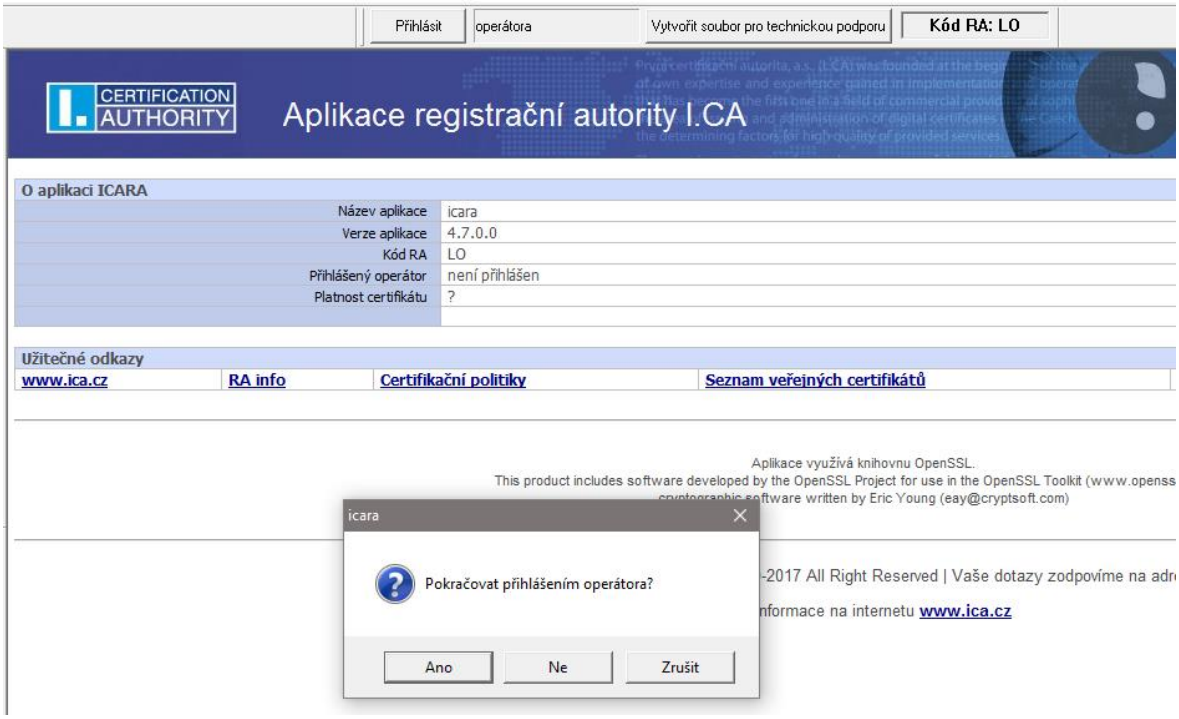
3. Obsluha RA

3.1. Základní myšlenka

Aplikace ICARA je koncipována jako průvodce, tzn. žádost o certifikát prochází při svém zpracování několika oddělenými kroky. Jakmile je jeden krok splněn, je automaticky zpracování žádosti posunuto do následujícího kroku. Typicky průběh zpracování žádosti začíná v kroku 1 (příchod klienta na pobočku a předání žádosti) a končí krokem 10 (odchod klienta s certifikátem - zavření žádosti). Aplikace ICARA umožňuje současné zpracování několika žádostí. Mezi těmito žádostmi lze libovolně přepínat a zpracovávat je v libovolném pořadí. Zpracování žádosti o komerční certifikát se nijak neliší od zpracování žádosti o kvalifikovaný certifikát. Operátor může být pouze vyzván, aby určil typ žádosti po jejím načtení nebo při jejím vytváření.

3.2. Spuštění aplikace a přihlášení operátora RA

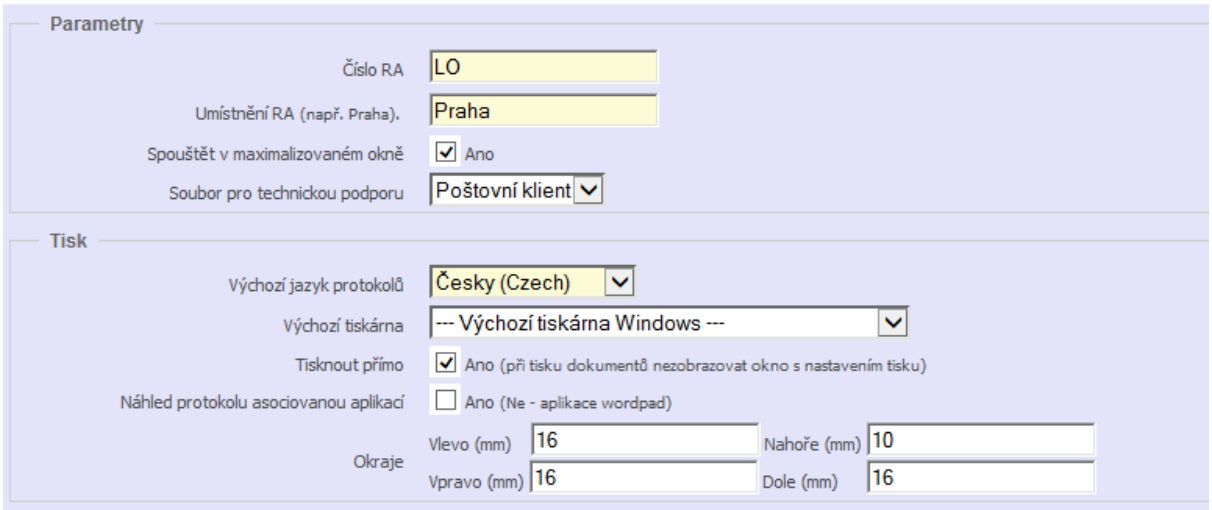
Spuštění programu se provede standardní cestou buď pomocí nabídky Start nebo poklepáním na ikonu zástupce na pracovní ploše. Po spuštění aplikace je pracovník pobočky registrační autority (dále „operátor“) vyzván k přihlášení do aplikace svým jménem, které vybere ze seznamu operátorů, kteří byli ke konkrétní RA přiřazeni v I.CA.
Po přihlášení operátora je aplikace připravena pro přijímání žádostí o certifikáty a vydávání vyhotovených certifikátů. Pokud je nutné práci s RA přerušit a počítač nechat bez dozoru operátora, má tento operátor povinnost se z aplikace odhlásit pomocí volby „Odhlásit operátora“ a vyjmout svou čipovou kartu ze čtečky.
Pro pokračování práce s aplikací provede nové přihlášení pomocí volby „Přihlásit“.
Práce s aplikací je umožněna, i pokud operátor není přihlášen (na přihlašovacím dialogu stiskl tlačítko „Zrušit“). V takovém případě jsou veškeré funkčnosti, které navazují komunikaci s I.CA, umožňují přijímání žádostí nebo vydávání certifikátů apod. znepřístupněny.



3.3. Prvotní přihlášení operátora

Při prvotním přihlášení operátora je potřeba aplikaci nakonfigurovat. Do pole číslo RA zadejte přidělený dvoumístný kód registrační autority a umístění pobočky. Volitelně můžete změnit další nastavení, například změnit výchozí tiskárnu. Po uložení nastavení můžete zahájit přihlašování kliknutím na tlačítko **Přihlásit** v horní liště aplikace.

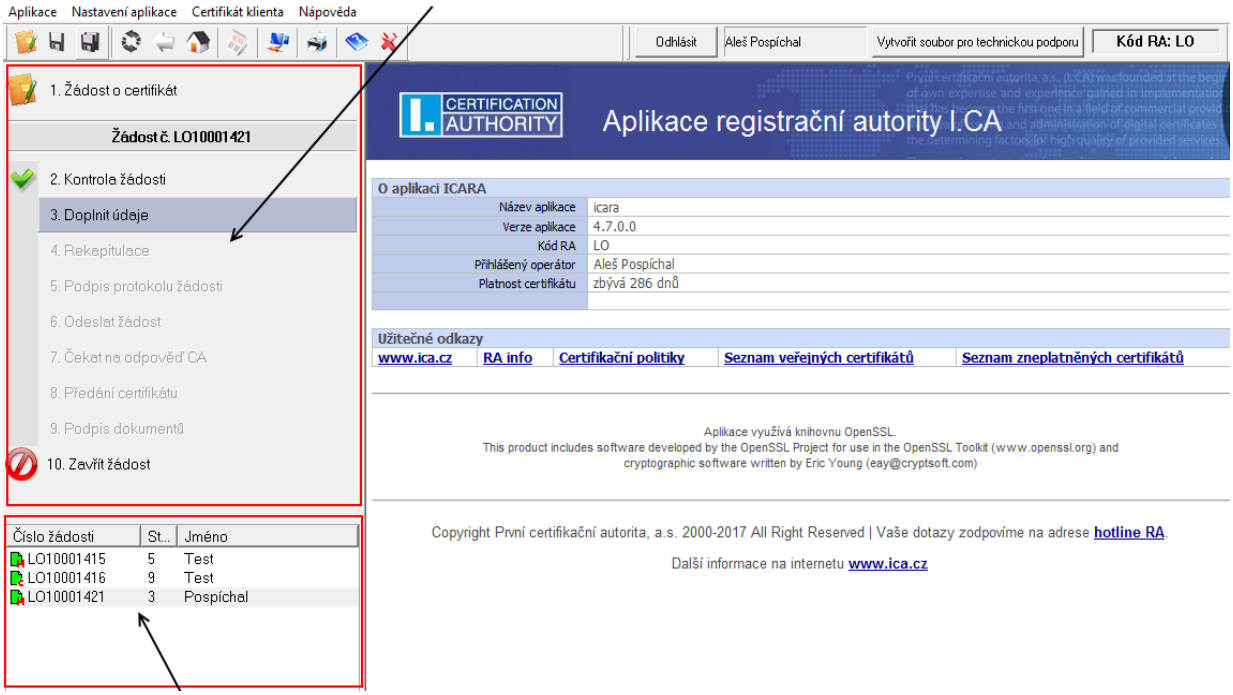
Pro přihlášení do této verze aplikace ICARA budete potřebovat **operátorské TWINS certifikáty**.
V případě, že máte v současné chvíli pouze komerční certifikát, požádejte jiného operátora, aby Vám vystavil certifikáty TWINS. Následně kontaktujte helpdesk ČSOB pro přiřazení role operátora.



3.4. Uživatelské rozhraní

Uživatelské rozhraní aplikace ICARA se mimo hlavní plochu s vestavěným webovým prohlížečem sestává z dvou důležitých panelů, zpravidla umístěných na levé straně.
Jedná se o panely:

„Vyřízení žádosti“ – Panel označuje splnění jednotlivých kroků zpracování žádosti a umožňuje mezi těmito kroky přepínat. Zpracování žádosti lze posunout vpřed i vzad tak, jak to umožňují tlačítka na tomto panelu tím, zda jsou zpřístupněna či nikoliv. Krok, který byl úspěšně dokončen, označuje zelená značka vlevo od příslušného tlačítka.



„Seznam žádostí“ - Panel obsahuje seznam čísel všech žádostí, které byly načteny do RA ke zpracování a slouží k přepínání mezi nimi. Jakmile je žádost uzavřena (krok 10) tak z tohoto seznamu zmizí. Typy žádostí jsou barevně odlišeny ikonou (bílá – komerční certifikát, žlutá – kvalifikovaný certifikát, zelená - TWINS). Žádost, u které vznikla během zpracování závažná chyba, je označena červenou ikonou. Vpravo od čísla žádosti je uveden maximální stav, kterého příslušná žádost při zpracování dosáhla.

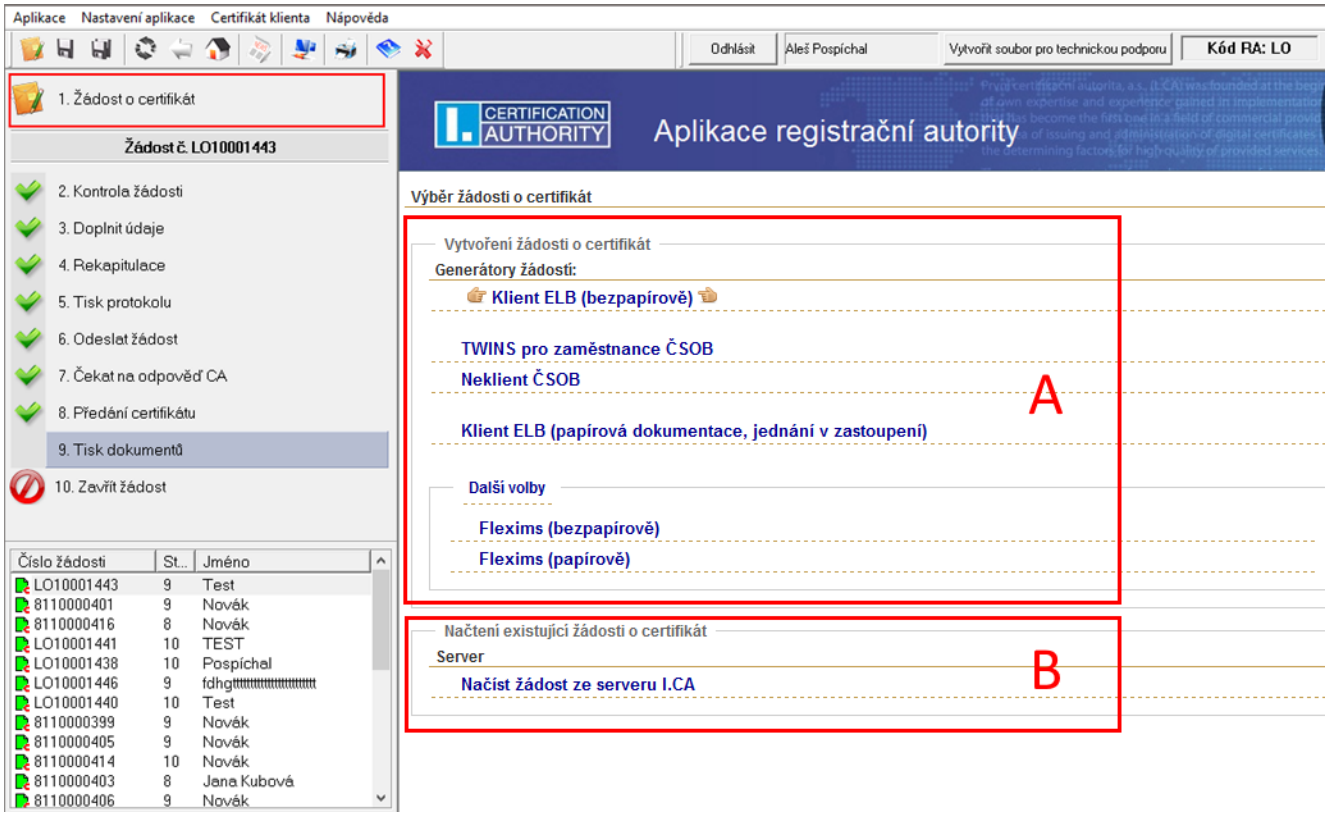
3.5. Zpracování žádosti o prvotní certifikát

Každá žádost při svém zpracování prochází devíti povinnými kroky, přičemž desátým krokem lze žádost uzavřít, jsou to:

1. Žádost o certifikát
2. Kontrola žádosti
3. Doplnit údaje
4. Rekapitulace údajů
5. Tisk protokolu o podání žádosti
6. Odeslání žádosti na Certifikační autoritu (CA)
7. Čekání na odpověď CA
8. Předání certifikátu
9. Tisk dalších protokolů
10. Zavření žádosti

3.5.1. Krok 1 – Žádost o certifikát

Cílem kroku 1 je povoleným způsobem opatřit žádost o certifikát a načíst ji do aplikace ke zpracování. Opatřením žádosti se myslí buď načtení již existující žádosti (z USB zařízení, čipové karty apod.), kterou na pobočku RA donesl klient, nebo vygenerování nové žádosti přímo na pobočce RA.
Po stisku tlačítka pro krok 1 na panelu „Vyřízení žádosti“ dojde k zobrazení dostupných možností pro získání žádosti, viz násl. obrázek.



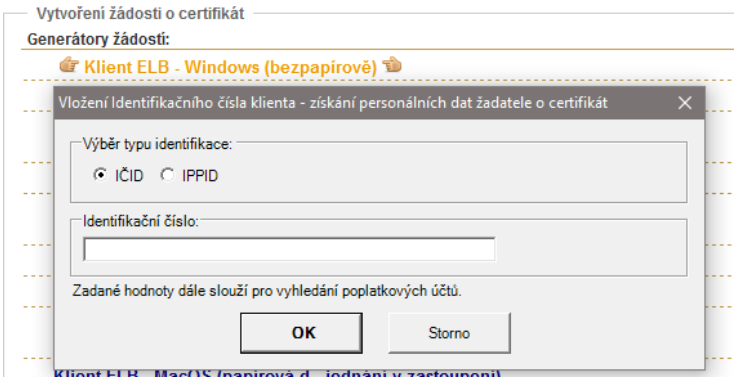
„Vytvoření žádosti o certifikát" "A"

Před samotnou volbou operátor vyzve klienta, aby vložil čipovou kartu do klientské čtečky. Následně dojde k výběru jedné z níže popsaných variant. Během generování samotné žádosti se generují také privátní klíče klienta. Během tohoto procesu bude klient aplikací vyzván, aby zadal PIN.

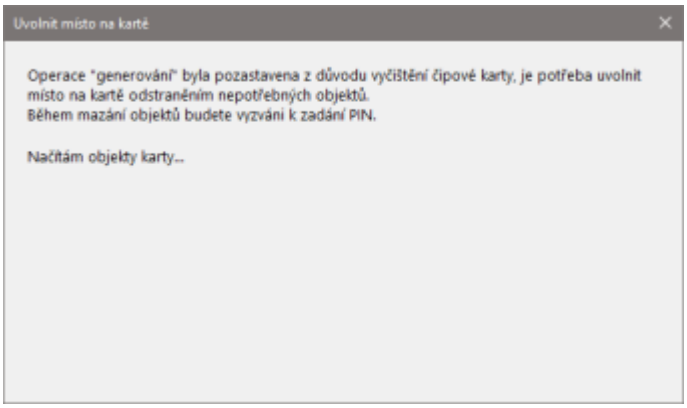
Volba "Klient ELB"

Zobrazená funkce umožní vygenerovat žádost o certifikát přímo na pobočce RA operátorem.

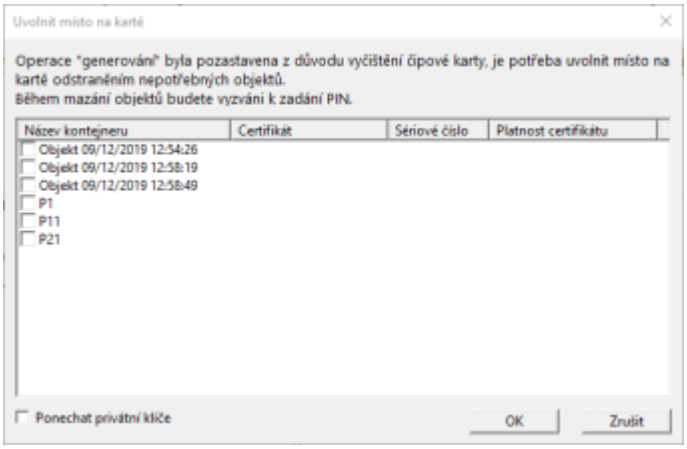
V případě prázdné čipové karty bude tvorba žádosti v prostředí ČSOB zobrazovat dialog pro zadání identifikačních údajů klienta, viz. obrázek níže. Po zadání identifikačních údajů bude kontaktován informační systém pro získání údajů tvorby žádosti o certifikát.



Pokud by čipová karta klienta obsahovala už nějaké certifikáty a privátní klíče, může dojít ke spuštění průvodce automatickým mazáním. V takovém případě by se zobrazilo okno, viz. obrázek níže. Během tohoto procesu budou z čipové karty klienta automaticky odstraněny již vypršené kvalifikované certifikáty a vypršené certifikáty certifikační autority. Během procesu mazání se zobrazí okno pro zadání PIN – v tomto případě ho zadává klient ke své čipové kartě.



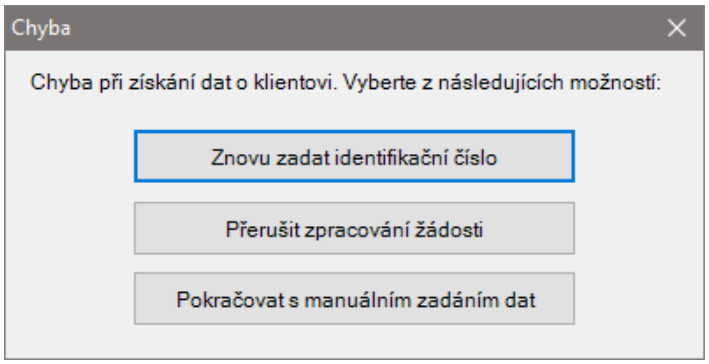
Po automatickém odmazání kvalifikovaných certifikátů se operátorovi zobrazí další obrazovka, kde uvidí další objekty (vypršené komerční certifikáty a privátní klíče bez certifikátu). Zde můžete ručně vybrat objekty, které se z čipové karty odstraní. Pouze v případě, že klient používá komerční certifikát za účelem šifrování e-mailů nebo jiných dat, pak zvolte v levém dolním rohu volbu Ponechat privátní klíče.



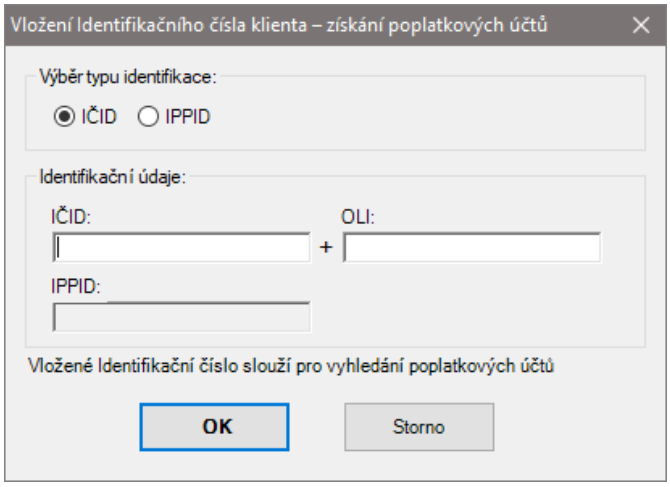
Po odstranění nepotřebných dat z čipové karty se zobrazí obrazovka pro zadání identifikačních údajů klienta (o dva obrázky výše). Další kroky jsou již shodné.

Na další stránce doplní, resp. ověří (pokud se údaje načetly automaticky), údaje o klientovi a stiskne tlačítko „Pokračovat“. Veškeré údaje se zadávají s diakritikou.
Po ověření údajů na následující stránce vytvoří žádost kliknutím na stejnojmenné tlačítko.

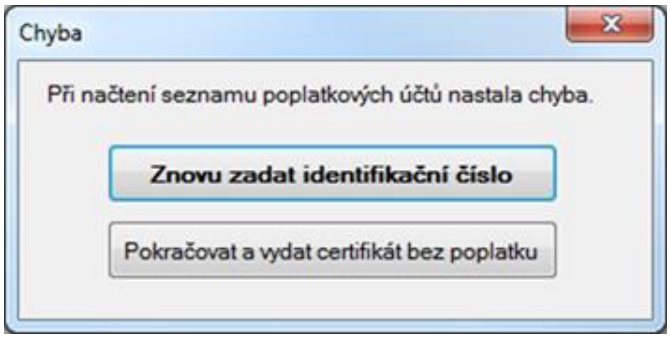
V případě, že by došlo při načítání údajů o žadateli k chybě, například z důvodu nedostupnosti služby, operátorovi se zobrazí tato hláška, kde má možnost opakování, aby zkontroloval, že zadal správné identifikační údaje, případně pokračoval dále s manuálním zadáním dat.



Při pokračování s manuální zadáním dat bude nutné ručně vyplnit také údaje pro vyhledání seznamu poplatkovacích účtů.



Pokud by nastala situace, že se nezdaří získat ani seznam poplatkovacích účtů, pak má operátor možnost opětovného zadání identifikačního čísla, aby vyloučil chybu překlepu. V případě opakování chyby může pokračovat a vydat certifikát bez poplatku.

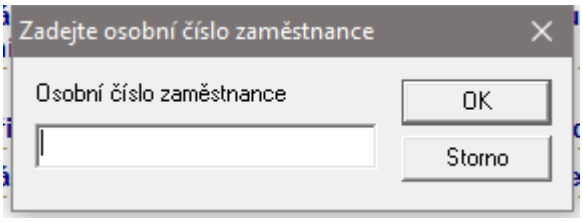


Volba "Klient Fleximus"

Postup je totožný jen s tím rozdílem, že okno se zadáním IPPID a datum narození operátor vyplní nebo přeskočí (to podle toho, jestli žadatel IPPID má nebo ne).

Volba "TWINS pro zaměstnance ČSOB"

Po zvolení jedné z těchto třech možností je operátor vyzván, aby vyplnil osobní číslo zaměstnance ČSOB.



Na další stránce ověří (pokud se údaje načetly automaticky), resp. doplní, údaje o klientovi a stiskne tlačítko „Pokračovat“. Veškeré údaje se zadávají s diakritikou. Po ověření údajů na následující stránce vytvoří žádost kliknutím na stejnojmenné tlačítko.

Volba "Neklient ČSOB"

Po zvolení vybere operátor příslušný typ certifikátu, doplní údaje o klientovi a po ověření údajů vytvoří žádost kliknutím na stejnojmenné tlačítko.

„Načtení existující žádosti o certifikát“ "B"

Týká se zejména ne-klientských certifikátů.

Volba „Načíst žádost ze serveru I.CA“

Umožní načtení žádosti pomocí šestimístného číselného identifikátoru, která byla generována prostřednictvím webových stránek I.CA.

3.5.2. Krok 2 – Kontrola žádosti

Při generování žádosti na pobočce RA je tento krok přeskočen a na panelu „Vyřízení žádosti“ je označen automaticky jako splněný.

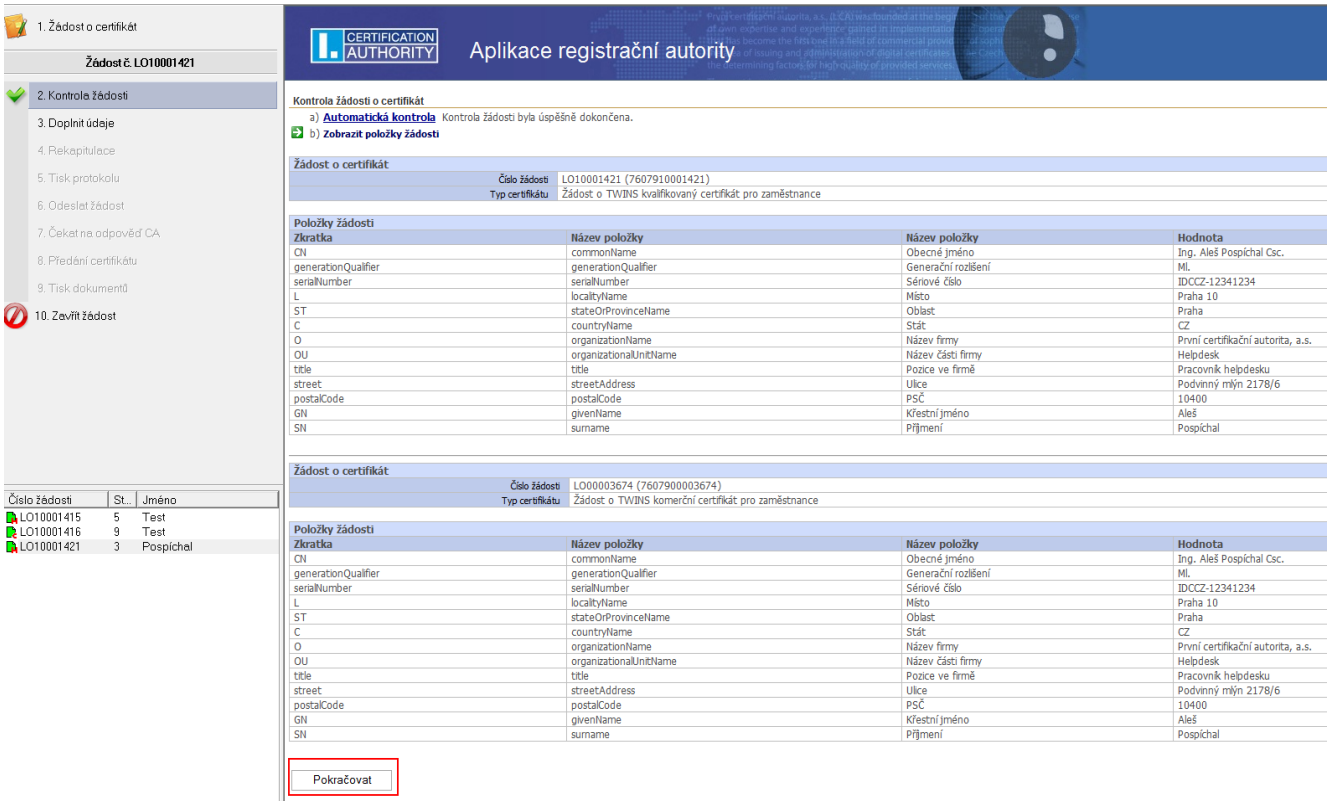
V případě vydávání ne-klientského certifikátu či v případě načtení existující žádosti, např. z čipové karty donesené klientem, je v tomto kroku provedena:

Automatická kontrola žádosti programem – pokud žádost nevyhovuje požadovaným normám nebo Certifikačním politikám I.CA, je zobrazen soupis nalezených chyb s podrobným vysvětlením, proč není možné žádost přijmout

Optická kontrola položek žádosti operátorem podle dokladu totožnosti klienta.

Pokud některá z položek nesouhlasí s předloženými doklady, je operátor povinen žádost odmítnout

Jakmile operátor provedl kontrolu žádosti, musí ručně přepnout na další krok zpracování pomocí tlačítka „Pokračovat“. Tímto přepnutím potvrdil, že položky žádosti souhlasí.

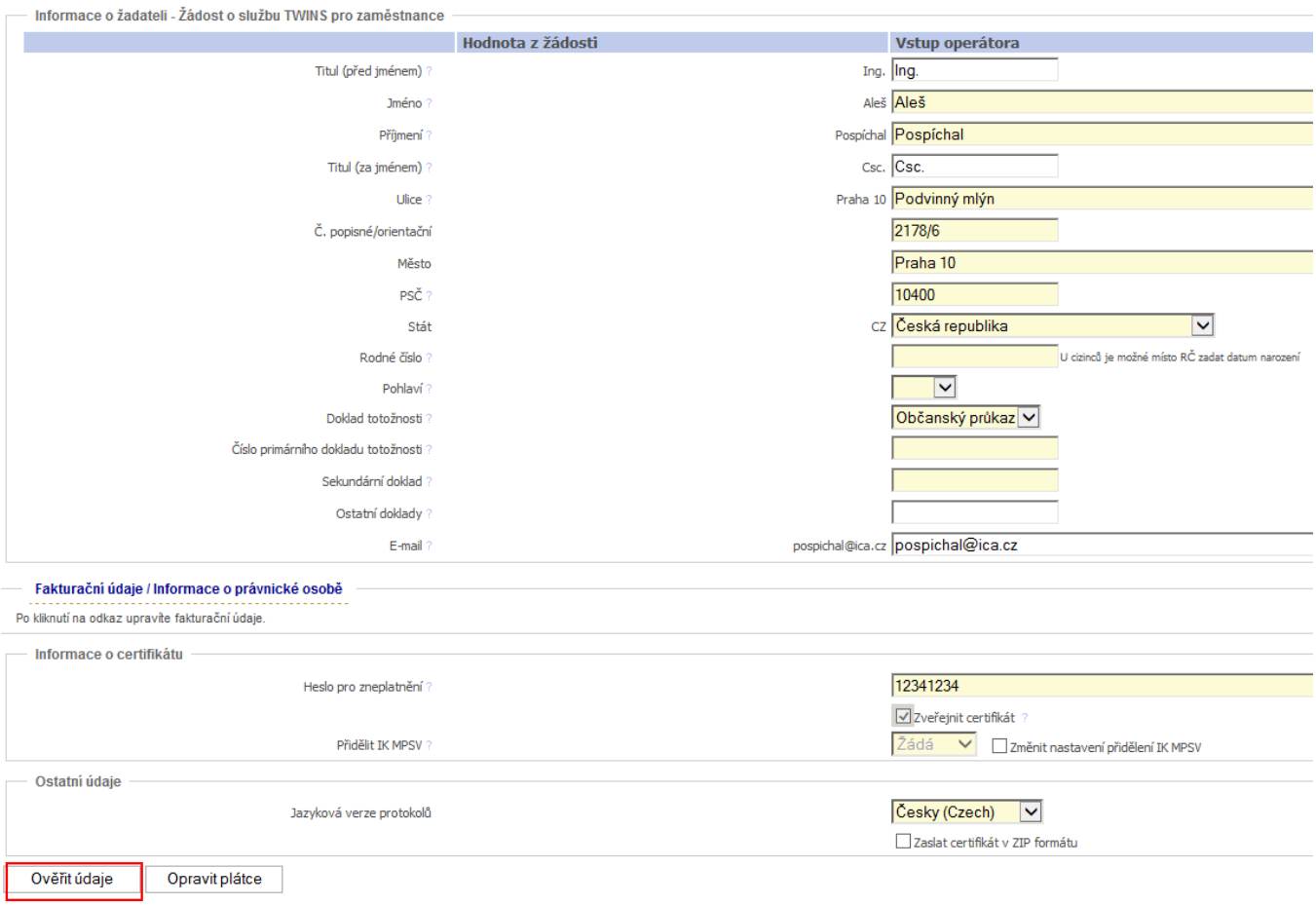


Grafické rozlišení typů žádosti o certifikát

- žádost o službu TWINS
- vydané certifikáty služby TWINS
- žádost o kvalifikovaný certifikát
- vydaný kvalifikovaný certifikát
- žádost o komerční certifikát
- vydaný komerční certifikát
- typ žádosti o certifikát nebyl určen
- chyba při kontrole žádosti

3.5.3. Krok 3 – Doplnit údaje

V tomto kroku operátor doplňuje všechny údaje, které jsou nutné pro identifikaci držitele certifikátu v souladu s CP I.CA. V případě, kdy dojde k načtení údajů ze žádosti, mohou být již některé údaje na formuláři předvyplněny. Na všech formulářích jsou povinné položky podbarveny žlutě, nepovinné bíle.
Ke všem polím je připojena nápověda, která se zobrazí kliknutím na otazník u příslušného pole. Během vyplňování údajů má operátor možnost srovnávat zadané údaje s položkami žádosti. Položky žádosti jsou zobrazeny vedle adekvátních políček k vyplnění. Po vyplnění všech potřebných údajů operátor stiskne tlačítko „Ověřit údaje“. Na stisk tohoto tlačítka se zkontrolují vložené údaje a zobrazí se úplná rekapitulace položek žádosti a údajů doplněných operátorem (Krok 4).



Zkratky pro nejčastější doklady:

CP - cestovní pas,

ŘP – řidičský průkaz,

VK – vojenská knížka,

SP – studentský průkaz,

ZP – zbrojní průkaz,

PZP – průkaz zdravotního pojištění

PHD – průkaz hromadné dopravy, atd.

Ostatní doklady

Ostatní relevantní doklady totožnosti, které byly použity pro kontrolu totožnosti nebo zmocnění žadatele. Uvádí se zkratkou, např.:

PM - notářsky ověřená plná moc,

POZP - Potvrzení o zaměstnaneckém poměru,

VOR – výpis z obchodního rejstříku,

PZ – notářsky ověřené pověření k zastupování jednatele právnické osoby;

ID MPSV - číslo existujícího identifikátoru Ministerstva práce a sociálních věcí, které má bude vloženo do rozšířených položek certifikátu tak, aby bylo možné certifikát využít pro komunikaci s MPSV.

Přidělení ID MPSV

Výběr z několika možností připojení identifikátoru Ministerstva práce a sociálních věcí (MPSV) do vydaného certifikátu. Volby znamenají:

Nežádá - Identifikátor nebude vložen.

Žádá - Klient požaduje identifikátor, pokud bude jeho přidělení zamítnuto ze strany MPSV, bude zamítnuta i žádost o certifikát.

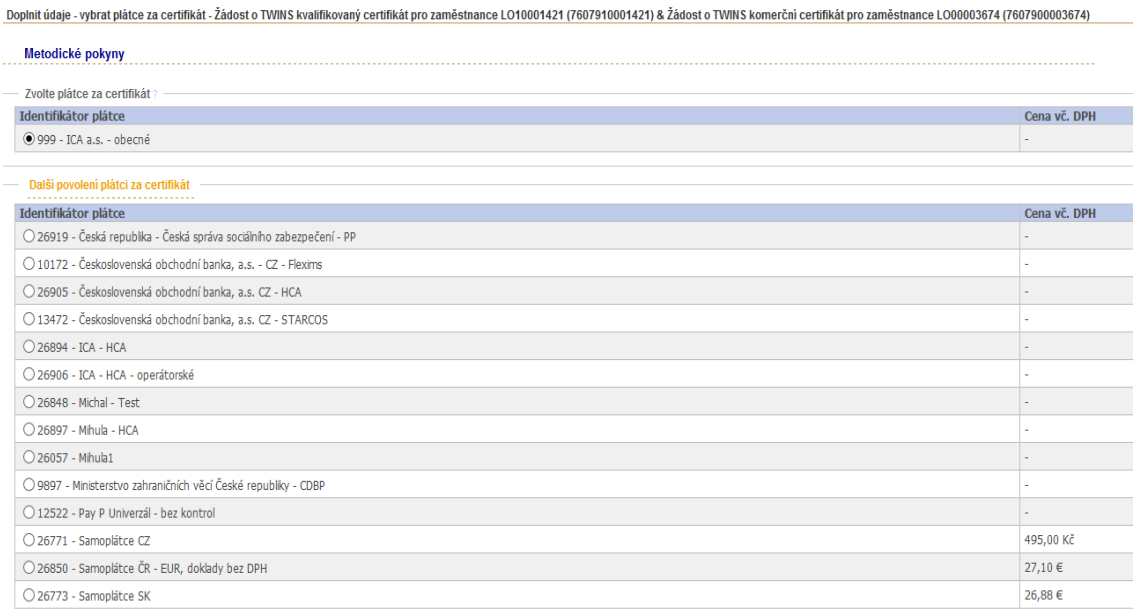
Pozn. ID MPSV není možné vložit do certifikátu dodatečně!

<u>Dále jen pro ne-klientské certifikáty:</u>

Pro ne-klientské certifikáty je nejprve v tomto kroku nutné nastavit plátce. Na první obrazovce aplikace navrhne podle položek žádosti způsob platby za certifikát:

V případě, že žádost nevyhovuje podmínkám žádného ze smluvních partnerů I.CA, je možno vydat certifikát na tzv. samoplátce.

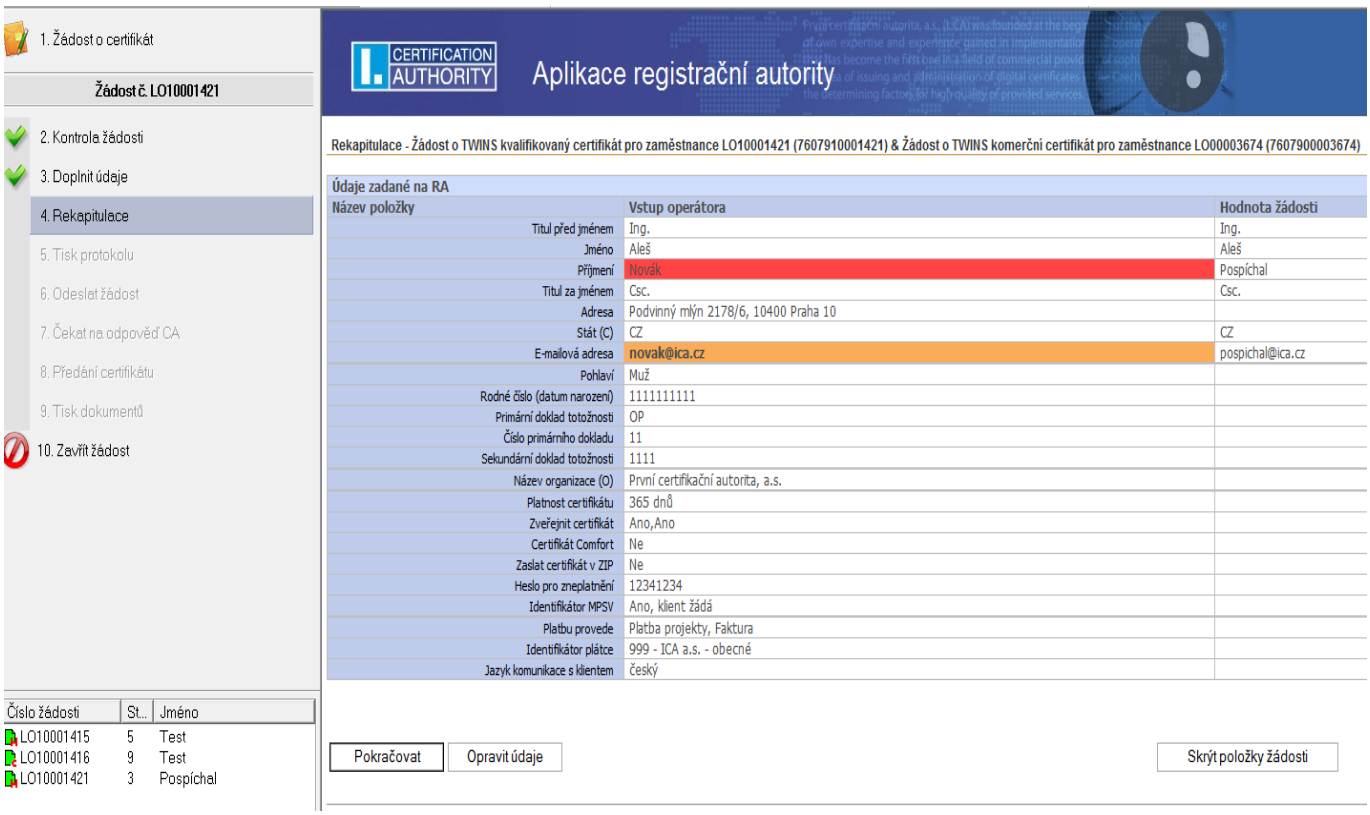
Pokud položky žádosti vyhovují některému ze smluvních partnerů I.CA, aplikace automaticky vybere a vyplní plátce. V opačném případě vybere operátor plátce (PP) ze seznamu plátců prostřednictvím volby „Vybrat plátce“



Výběr plátce je nutno potvrdit tlačítkem „Souhlasím“.
Typ formuláře, který se v následném kroku zobrazí, závisí na typu a variantě žádosti o certifikát. Existuje několik variant tohoto formuláře, které nabízí pro vyplnění vždy jen potřebné údaje, které musí být vyplněny. Po doplnění údajů operátor pokračuje stisknutím tlačítka „Ověřit údaje“. V případě změny plátce, se může operátor vrátit k předešlé obrazovce stisknutím tlačítka „Opravit plátce“.

3.5.4. Krok 4 – Rekapitulace

V tomto kroku má operátor možnost pohledové kontroly položek žádosti a doplněných údajů. Pokud se některé položky žádosti neshodují s doplněnými údaji, je o tom operátor informován barevným zvýrazněním. Oranžová barva je pro drobnou neshodu, červená barva indikuje vážnou neshodu nebo porušení formátu vložených údajů.

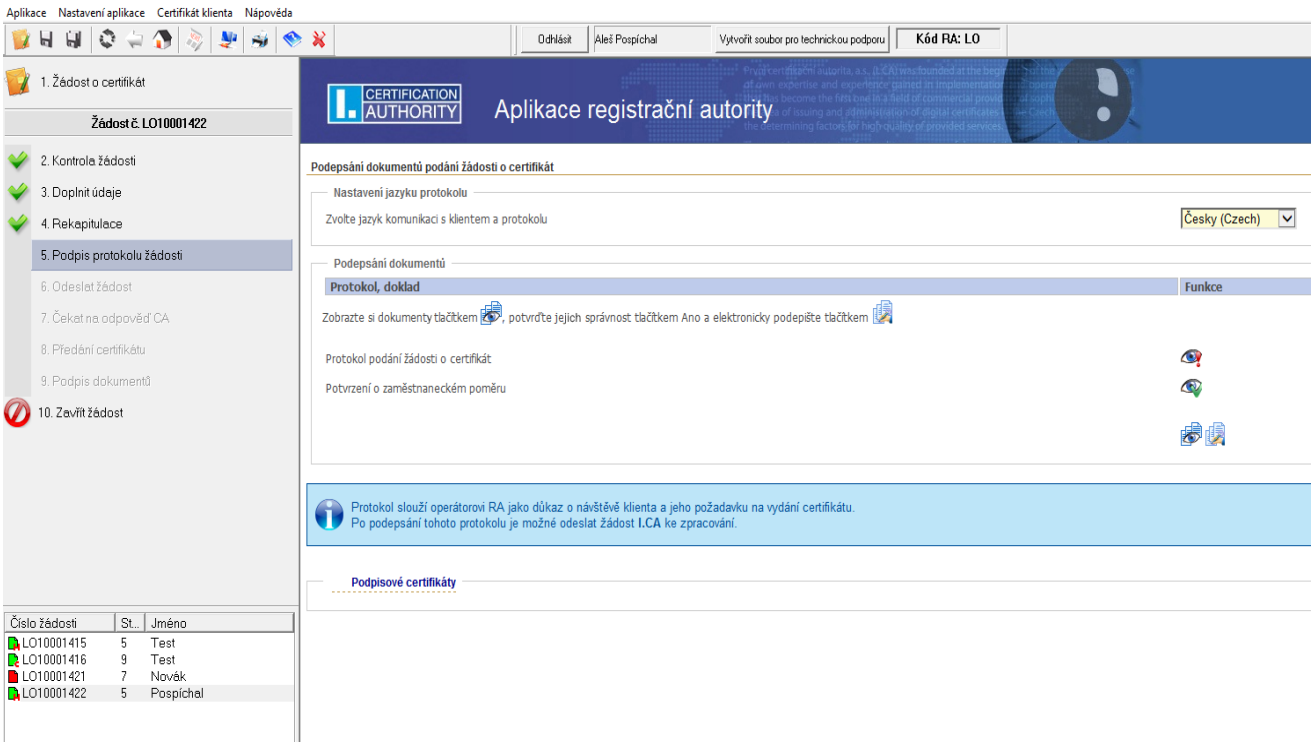


Volba „Opravit údaje“ umožní opravit položky, které se vyplňovaly na předešlém formuláři. V případě červených - závažných chyb nesouhlasí položky uvedené v hodnotě žádosti se vstupem operátora. Aby kontrola proběhla korektně, je nutné, aby položky byly shodné. Pokud se tak stane, pokračuje operátor stisknutím tlačítka „Pokračovat“. V opačném případě nelze certifikát vydat a operátor RA žádost zamítne.

3.5.5. Krok 5 – Tisk protokolu o podání žádosti

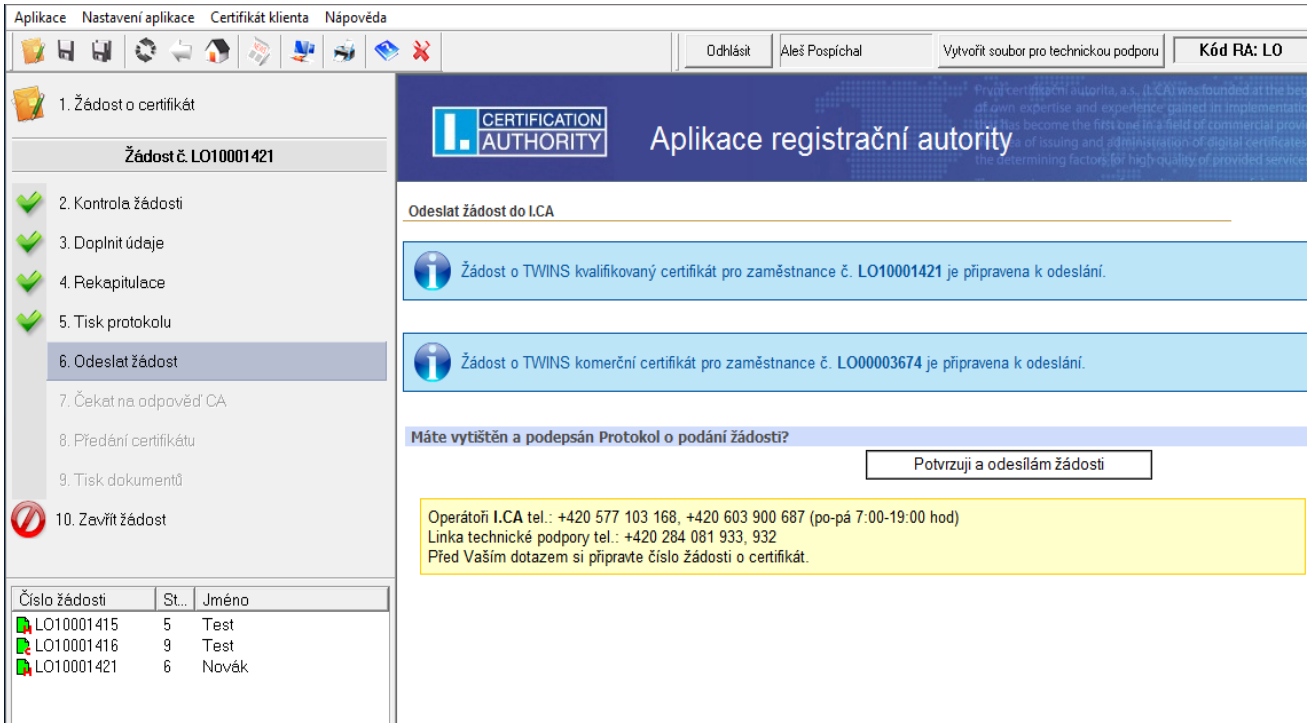
V tomto kroku operátor podepisuje protokol o podání žádosti o certifikát svým certifikátem operátora a privátním klíčem klienta, který byl zapsán na čipovou kartu. U vydávání certifikátů s papírovou dokumentací, operátor vytiskne protokol ve 2 vyhotoveních a předá klientovi ke kontrole. Před tiskem může protokol zobrazit v náhledovém okně. Operátor může zvolit jiný jazyk tisku protokolu, pokud si jej žadatel přeje. Také může změnit počet vytištěných kopií, ale implicitně je nastaven počet kopií Protokolu podle požadavku I.CA.

Pozn.: Protokol o podání žádosti o certifikát musí být vždy zkontrolován žadatelem. Bez souhlasu (a u tištěného protokolu i podpisu protokolu) nelze pokračovat ve vyřízení žádosti o certifikát.



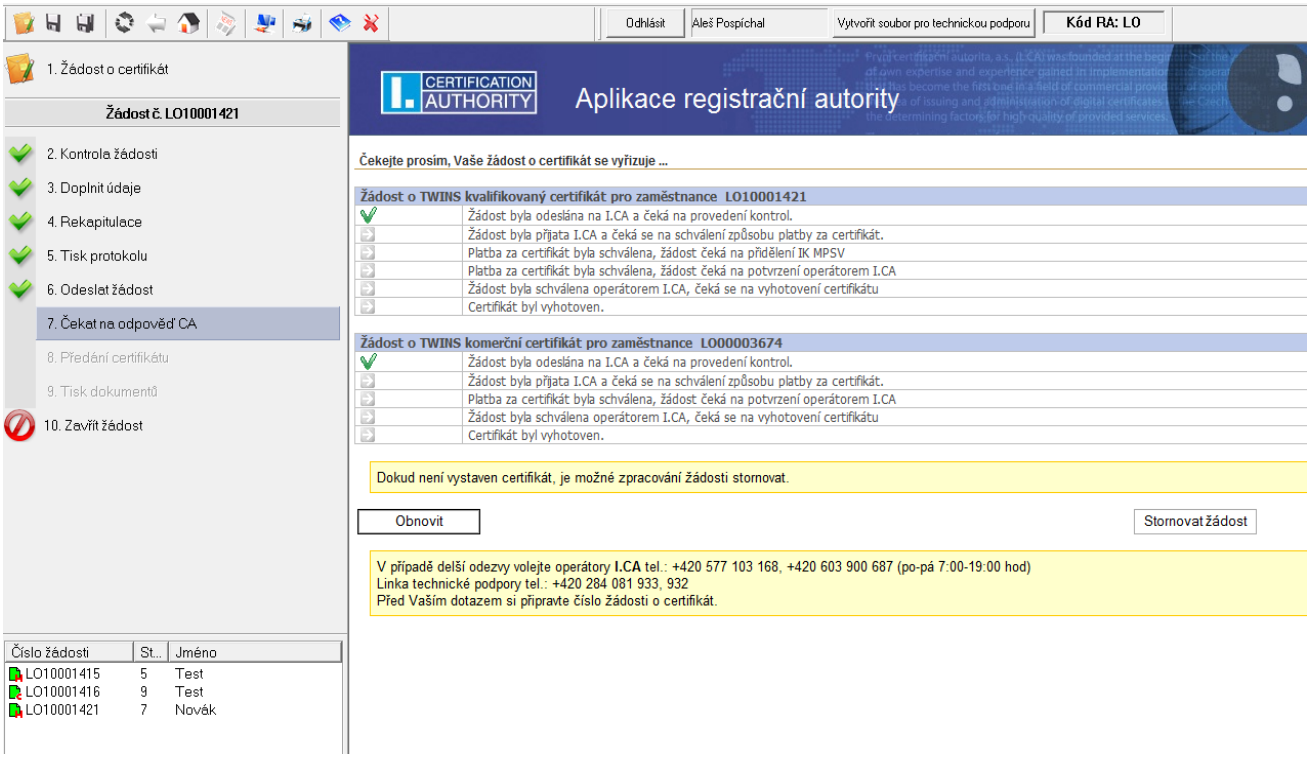
3.5.6. Krok 6 - Odeslat žádost

V tomto kroku operátor odesílá žádost ke zpracování do I.CA. Jakmile je žádost odeslána, nelze již vložené údaje klienta změnit. Před odesláním žádosti na I.CA je nutno potvrdit, že operátor má vytištěný a žadatelem podepsaný Protokol o podání žádosti o certifikát. Žádost operátor odešle stisknutím tlačítka „Potvrzuji a odesílám žádost“. Od okamžiku odeslání žádosti je veškerá práce s žádostí zálohována na pevný disk, takže v případě havárie aplikace, výpadku el. energie apod. bude při příštím spuštění ICARA obnoven přesně stejný stav jako před výpadkem.



3.5.7. Krok 7 – Čekání na odpověď Certifikační autority

Aplikace ICARA se v tomto kroku pravidelně dotazuje serveru I.CA na úspěšné vyřízení žádosti. Doba čekání bývá 5-10 minut. Během této doby je operátor stručně informován o stavu zpracování textovým popisem.



Funkce „**Stornovat žádost**“ umožňuje operátorovi RA, stornovat zpracování žádosti. Funkčností nelze stornovat žádost již vydaného certifikátu. Funkce stornování žádosti je dostupná v závislosti na konfiguraci aplikace.

Funkce „**Obnovit**“ umožní obnovit zpracovávání žádosti. Pokud bude zpracování trvat déle, měl by operátor nejdříve využít této možnosti a pokusit se tak dokončit proces odeslání. Teprve pak by se měl operátor obrátit na operátory I.CA. Kontaktní informace jsou k dispozici ve žlutém rámečku.

Při požadované službě TWINS, je aplikací průběžně zobrazován stav obou žádostí.
Jakmile je certifikát získán, žádost automaticky přejde do následujícího kroku.

Pokud bude žádost o certifikát Certifikační autoritou **zamítnuta**, aplikace operátorovi sdělí důvod zamítnutí. V takovém případě není umožněno s žádostí dále pracovat (další kroky zůstanou znepřístupněny), operátor vysvětlí důvod klientovi a žádost zavře. Možné příčiny zamítnutí jsou:

„Žádost o certifikát byla zamítnuta, protože nevyhovuje Certifikační Politice“ - nesprávné kódování, chybná délka položek, chybné naplnění položek žádosti, apod.

Příčina: Žádost nesplňuje podmínky I.CA.

Postup operátora: Odmítne žádost, klient musí přijít znovu se správnou žádostí.

„Žádost o certifikát byla odmítnuta operátorem I.CA.“

Příčina: Pracovník I.CA při ruční kontrole žádosti zjistil nějaký nedostatek, důvod odmítnutí je stručně uveden pod chybovým textem (v červeném rámečku).

Postup operátora: Podle důvodu odmítnutí. Většinou je problém v nesrovnalostech údajů vkládaných na RA. V takovém případě klikne na tlačítko Opravit údaje, žádost se načte znovu a operátor vyplní údaje správně. Pokud je příčina odmítnutí samotná žádost donesená klientem, odmítne ji.

„Žádost o certifikát nebyla zpracována z 'jiných' technických důvodů - např. duplicitní klíče.“

Příčina: Veřejný klíč obsažený v žádosti byl již v minulosti použit. Typicky se tato chyba objevuje, pokud je jedna žádost poslána na I.CA vícekrát.
Postup operátora: Odmítne žádost, klient musí přijít znovu s novou žádostí.

„Žádost o certifikát byla odmítnuta, protože obsahovala neúplné nebo nesprávné údaje.“

„Žádost o certifikát byla odmítnuta, protože selhalo ověření elektronického podpisu operátora RA.“

„Žádost o certifikát byla odmítnuta z rozhodnutí fakturačního systému I.CA.“

Příčina: Vydání certifikátu bylo zamítnuto, protože položky uvedené v žádosti neodpovídají kritériím nastavení plátce, žádost má nepovolenou délku klíče, atd.

Postup operátora: Pro zjištění konkrétního důvodu zamítnutí kontaktujte podporu I.CA (hotlinera@ica.cz)

„Při zpracování žádosti vznikla vnitřní chyba systému I.CA.“

Příčina: Chyba ICARA nebo systémů I.CA

Postup operátora: kontaktuje technickou podporu I.CA (hotlinera@ica.cz).

„Při komunikaci se serverem I.CA došlo k závažné chybě.“

Příčina: Výpadek internetového spojení a/nebo serverů I.CA.

Postup operátora: Po obnovení spojení na servery I.CA se pokusí certifikát „stáhnout“ z databáze I.CA dodatečně. Dohledání certifikátu provede podle čísla žádosti, u které nastala chyba. Tisky protokolů je nutné dořešit přes menu „Certifikát klienta“.

V případě nejasností kontaktuje technickou podporu I.CA (hotlinera@ica.cz).

„Žádost o certifikát byla zamítnuta, protože se nepodařilo přidělit identifikátor MPSV.“

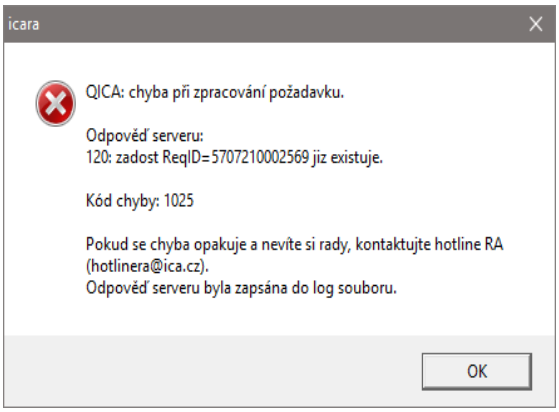
Příčina: V žádosti o kvalifikovaný certifikát byl specifikován požadavek na přidělení identifikátoru Ministerstva práce a sociálních věcí. Tento identifikátor se však nepodařilo přidělit. Chyba je většinou na straně serverů MPSV.

Postup operátora: Zavře žádost a pokusí se ji načíst (vygenerovat) a vyřídit znovu. Pokud se i napodruhé ID MPSV nepřidělí, kontaktuje technickou podporu I.CA (hotlinera@ica.cz).

„Žádost se nepodařilo odeslat. Odesílaná žádost o certifikát je již v databázi.“

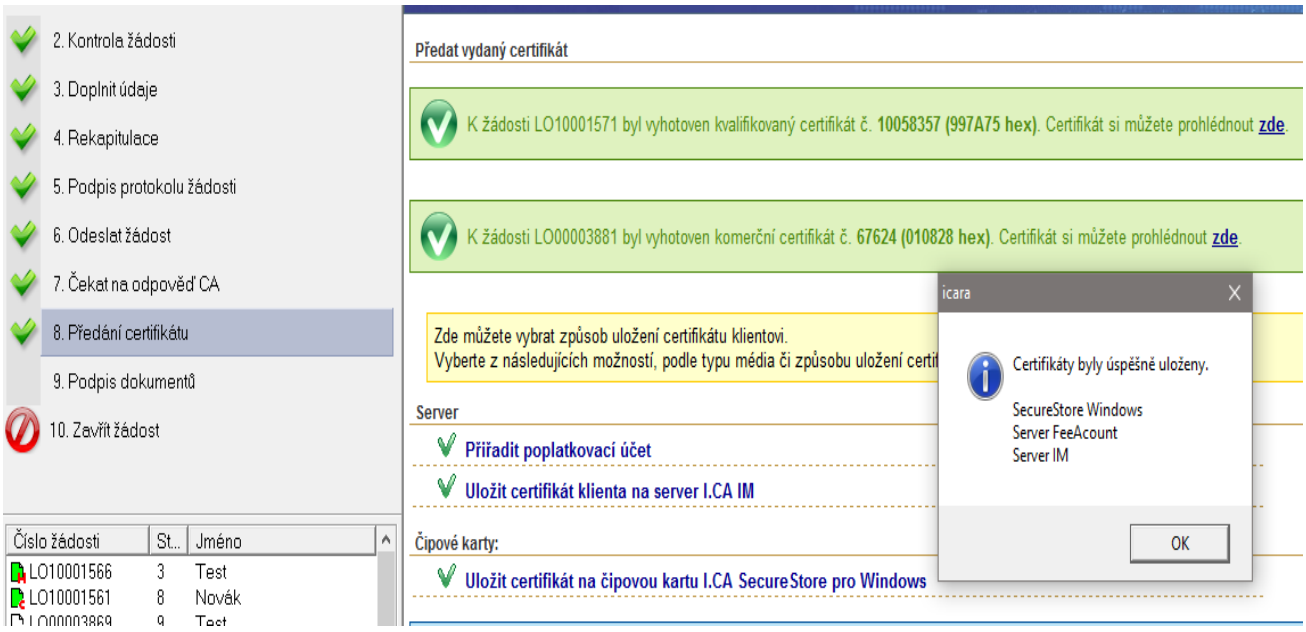
Příčina: Obvyklou příčinou tohoto stavu je, že stejný kód RA používá ve stejné chvíli i jiná pobočka / operátor. Tomuto operátorovi bylo přiděleno stejné číslo žádosti a tato žádost byla již odeslána ke zpracování.

Postup operátora: Vygenerovat novou žádost (pokud byla generována na RA), případně žádost znovu načíst. Tím dojde k přidělení nového čísla žádosti.



3.5.8. Krok 8 - Předání certifikátu

Po úspěšném získání certifikátu z CA budou certifikáty automaticky uloženy na čipovou kartu klienta, na server Identity Manager (IM) a dojde k uložení poplatkového účtu na server ČSOB. O úspěšném předání certifikátů bude aplikace operátora informovat. Po kliknutí na tlačítko „OK“ aplikace automaticky přeskočí do dalšího kroku. Pokud se certifikáty automaticky neuloží, má ještě operátor možnost uložit certifikáty dodatečně prostřednictvím nabízených odkazů na této stránce.



Volba „Uložit certifikát na čipovou kartu I.CA SecureStore“

Funkce uloží certifikát na čipovou kartu zvoleného typu. Uložení proběhne úspěšně jen za těchto podmínek:

- V klientské čtečce je vložena karta, na které je privátní klíč odpovídající k žádosti resp. certifikátu
- Na kartě je dostatek paměti pro uložení certifikátu.
- Na kartě jsou přítomny ve speciálním úložišti pro kořenové certifikáty komerční i kvalifikované kořenové certifikáty I.CA

Pokud na kartě není dostatek místa pro nový certifikát, zobrazí se chybová zpráva. V takovém případě je potřeba paměť uvolnit odstraněním vypršených nebo nepoužívaných certifikátů. Operátor nemá možnost toto provést prostřednictvím aplikace ICARA. K tomuto účelu slouží specializované aplikace pro správu čipových karet (pro karty Starcos 3 je to SW I.CA Securestore Card Manager).

Pozor! Při „čištění” karty nesmažte privátní klíč k certifikátu, který chcete na kartu uložit!

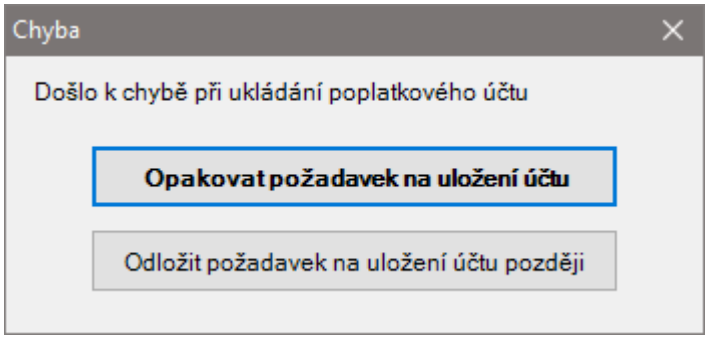
Volba „Uložit certifikát klienta na server I.CA IM“

Vydaný certifikát je doplněn o další identifikační údaje klienta a pomocí HTTPS spojení odeslán na vzdálený server.

Volba „Přiřadit poplatkovací účet“

Na server ČSOB se odešle informace, na který bankovní účet klienta se má právě vyhotovený certifikát poplatkovat. Součástí odesílané informace je sériové číslo vystaveného certifikátu, identifikační údaje klienta (například OLI) a zvolený poplatkovací účet.

Pokud by nastala při přiřazení poplatkovacího účtu chyba, znamená to, že se nepodařilo na server ČSOB uložit výše uvedené informace. Pravděpodobně se jedná o dočasný výpadek služby.
Operátorovi se zobrazí tato hláška, kde může opakovat odeslání ještě jednou nyní, případně tuto akci odložit na později. Neuložení poplatkovacího účtu nebrání v dokončení dalších kroků žádosti, samotné opakování akce pro přiřazení poplatkovacího účtu je možné dokončit později i po odchodu klienta z pobočky.



V případě ne-klientských certifikátů bude zpřístupněna pouze volba „Uložit certifikát na čipovou kartu“. Na server IM se ne-klientské certifikáty neukládají.

3.5.9. Krok 9 - Tisk dokumentů

V tomto kroku operátor zobrazí a podepisuje zbývající protokoly svým certifikátem a vystaveným certifikátem klienta. U vydávání s papírovou dokumentací, operátor protokoly vytiskne. Operátor může zvolit jiný jazyk tisku protokolu, pokud si jej žadatel přeje. Také může změnit počet vytištěných kopií, ale implicitně je nastaven počet kopií dokumentů podle požadavku I.CA. Jednotlivé protokoly budou zobrazovány pod sebou.
Jakmile jsou podepsány (případně vytisknuty) všechny protokoly, krok je označen jako splněný.

Seznam protokolů (u papírové dokumentace):

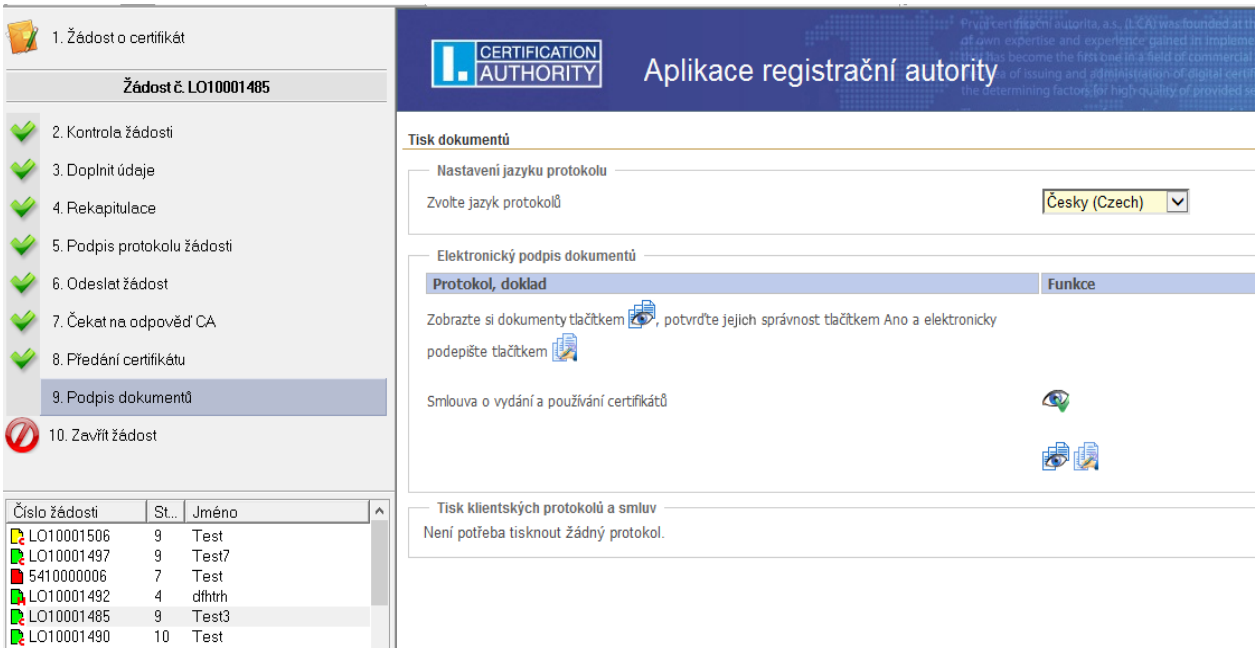
Protokol o podání žádosti na vydání certifikátu (tiskne se vždy v 5 kroku)

Smlouva o vydání a používání certifikátů (tiskne se vždy až na výjimky)

Příloha č. 1 (pokud certifikát obsahuje ID MPSV, tiskne se pouze 1x, dokument zůstává s dokumentací na pobočce)

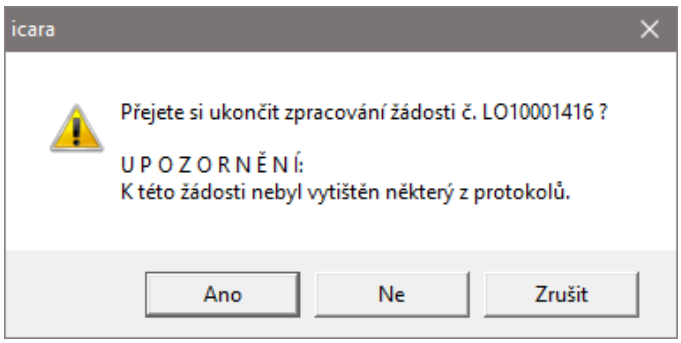
Daňový doklad (týká se ne-klientských certifikátů)

U bezpapírové pobočky je zaslán klientovi e-mail s přístupem na elektronické úložiště dokumentů.

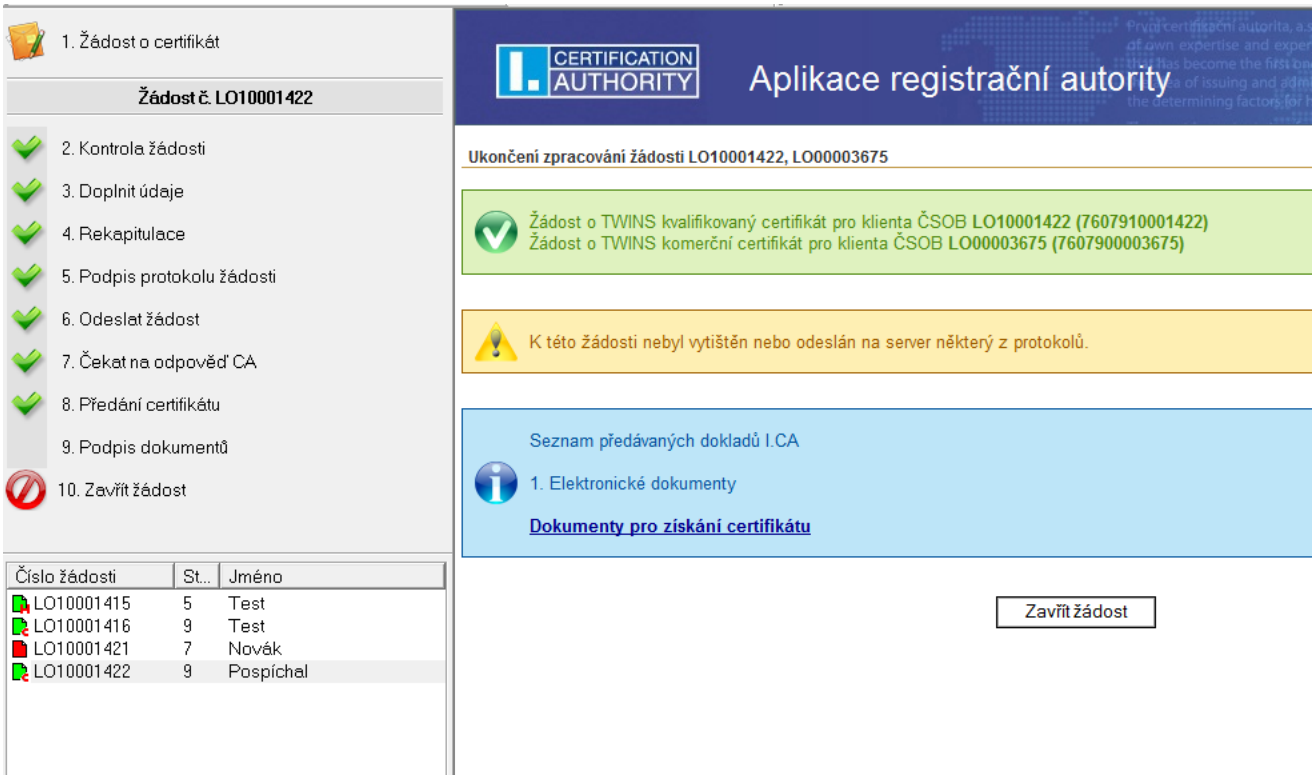


3.5.10. Krok 10 - Zavřít žádost

V tomto kroku je možné celou žádost uzavřít. Žádost je uzavřena kliknutím na tlačítko „Zavřít žádost“. Pokud nebyl operátorem certifikát předán nebo nebyl vytisknut nějaký protokol, aplikace jej na to upozorní.



Na stránce je pro kontrolu operátora dále zobrazen potřebný seznam předávaných dokladů I.CA. V případě jakýchkoliv jiných nejasností je na stránce uveden odkaz, kterým bude operátor přesměrován na stránky I.CA týkajících se dokumentace k vydávání kvalifikovaného certifikátu a produktu TWINS.



3.6. Žádost o následný certifikát

Při obnově certifikátu prochází žádost při svém zpracování pouze pěti povinnými kroky, posledním krokem lze rovněž žádost uzavřít, jsou to:

1. Žádost o certifikát
5. Tisk protokolu o podání žádosti
6. Odeslání žádosti na Certifikační autoritu (CA)
7. Čekání na odpověď CA
8. Předání certifikátu
10. Zavření žádosti.

Ostatní kroky jsou buď zautomatizovány, nebo přeskakovány.

3.6.1. Krok 1 – Žádost o certifikát

Krok 1 při obnově certifikátu vyžaduje načíst certifikát, který bude chtít klient obnovit. Při obnově certifikátu lze načítat pouze certifikáty, které jsou uloženy na čipové kartě.
Po stisku tlačítka pro krok 1 na panelu „Vyřízení žádosti“ dojde k zobrazení známých dostupných možností pro získání žádosti.

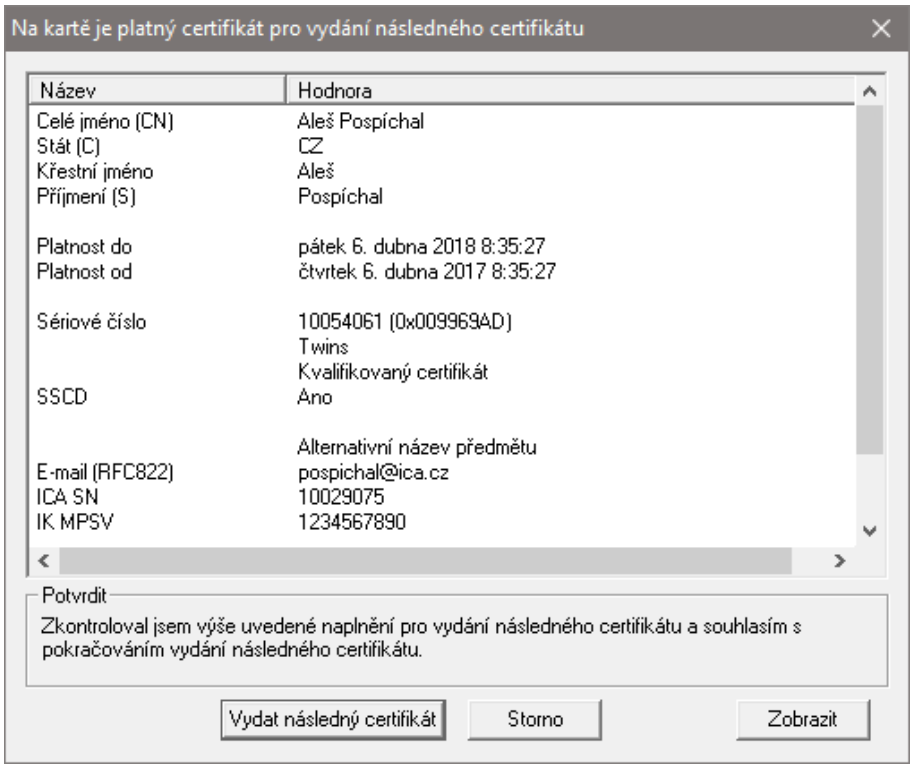
Volba „Vytvořit žádost pro klienta ELB“

Před samotnou volbou operátor vyzve klienta, aby vložil čipovou kartu do klientské čtečky.

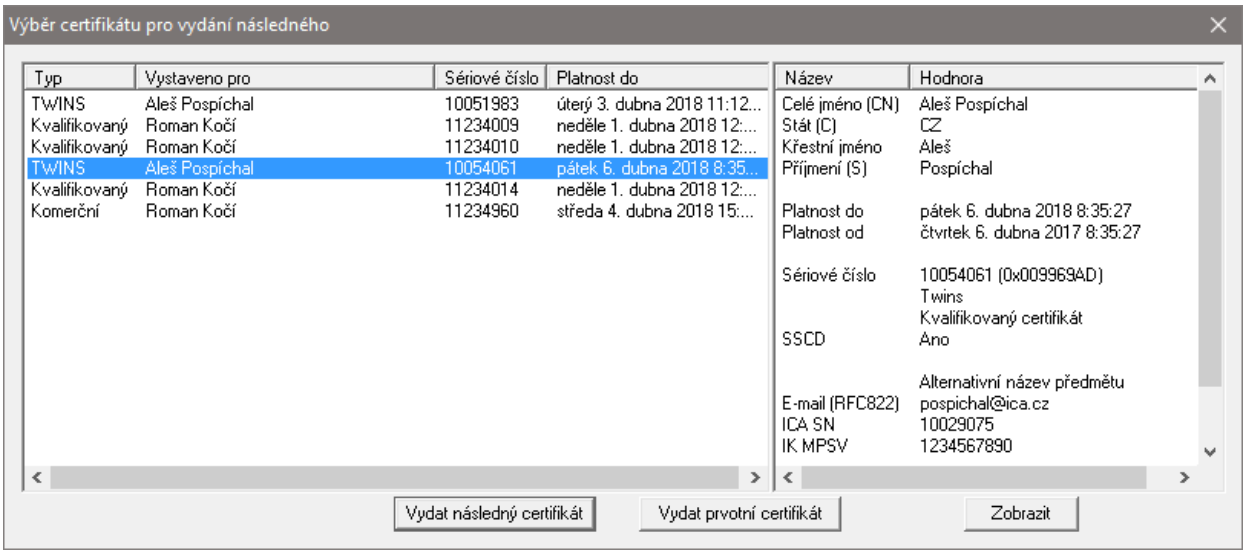
Zobrazená funkce umožní načíst platné certifikáty, které se nacházejí na čipové kartě, a které bude možné obnovit.

Aplikace nabídne zobrazení platných možných certifikátů k obnově v závislosti na jejich počtu:

V případě **jednoho** platného certifikátu k obnově se zobrazí informace o certifikátu, viz. obrázek. Pokud nedošlo ke změnám položek, které jsou uvedeny v certifikátu, může operátor přejít k samotné obnově certifikátu stisknutím tlačítka „Obnovit“. Prostřednictvím tlačítka „Zobrazit“ lze zobrazit samotný certifikát. V opačném případě, pokud položky a informace o klientovy nebudou souhlasit s položkami uvedenými na certifikátu, operátor zamítne obnovu certifikátu stisknutím tlačítka „Storno“. V takovém případě bude operátor aplikací přesměrován na vydávání nového prvotního certifikátu. Po přesměrování se zobrazí dialogové okno pro zadání IPPIDu a data narození a pokračuje standardním způsobem ve vydávání nového prvotního certifikátu.

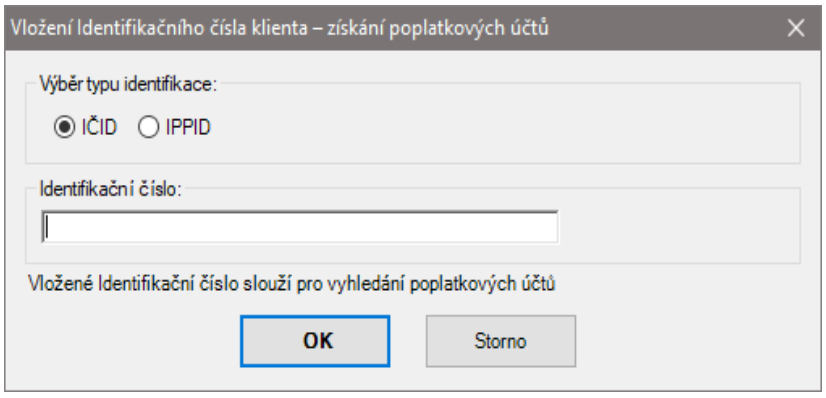


V Případě, kdy bude na kartě **více** platných certifikátů k obnově, se nejprve zobrazí jejich seznam viz. obrázek. Seznam přehledně zobrazí certifikáty postupně dle typu, jména, sériového čísla a platnosti daného certifikátu. Operátor na základě informací od klienta vybere certifikát, který chce klient obnovit. Pokud nedošlo ke změně položek ve vybraném certifikátu k obnově, může operátor kliknout na tlačítko „Obnovit“. Pokud klient nebude chtít obnovit ani jeden z uvedených certifikátů a bude chtít vydat nový prvotní certifikát, klikne operátor na tlačítko „Storno“. Aplikace ho automaticky opět přesměruje na vydávání prvotního certifikátu.

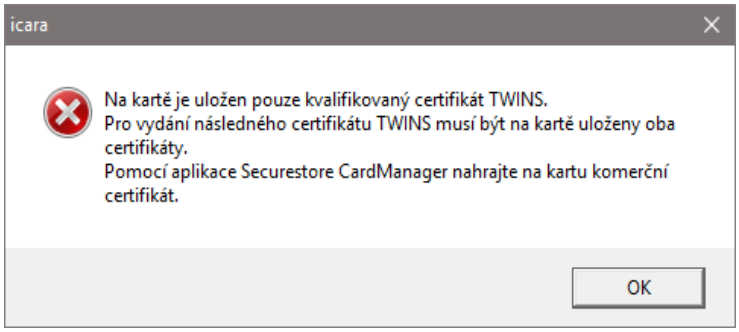


Pozn.: Při načítání certifikátů aplikace zobrazí i ne-klientské certifikáty, které jsou na čipové kartě a které půjde také obnovit.

Po stisknutí tlačítka „**Vydat následný certifikát**“ se zobrazí okno pro zadání identifikačních údajů pro získání seznamu účtů, na který se bude vydávaný certifikát poplatkovat. Dále bude aplikace automaticky generovat žádost o obnovení certifikátu. Zároveň bude generovat nové privátní klíče. Po vytvoření klíčů je klient vyzván, aby 2x zadal PIN pro uložení klíčů na čipovou kartu. Po zadání, přejde proces obnovy do dalšího kroku.



Pokud obnovovaný certifikát TWINS obsahuje pouze jednu veřejnou část certifikátu, a to buď kvalifikovanou nebo komerční, aplikace operátora na tuto skutečnost upozorní, viz. obrázek. V takovém případě je nutné chybějící veřejnou část z produktu TWINS dohrát na čipovou kartu, aby tak produkt TWINS byl kompletní a byl připraven k obnově.



Aplikace načte pouze certifikáty, které mají ke svým privátním klíčům i jejich veřejné části. Pokud tedy bude mít klient na čipové kartě více privátních klíčů bez jejich veřejných certifikátů (klient je může využívat pro dešifrování starších e-mailových zpráv), aplikace je nenačte.

Automatická kontrola kroků 2, 3, 4

Kroky 2, 3 a 4 jsou při obnově certifikátu automaticky přeskakovány. Aplikace tak označí tyto kroky za splněné a přejde rovnou ke kroku číslo 5. Pro ověření informací lze do jednotlivých přeskočených kroků zpětně nahlédnout.

3.6.2. Krok 5 – Tisk protokolu o podání žádosti

Při obnově certifikátu se protokol o podání žádosti netiskne, krok je automaticky přeskočen.

3.6.3. Krok 6 - Odeslat žádost

V tomto kroku operátor odesílá žádost o obnovu ke zpracování do I.CA. Žádost operátor odešle stisknutím tlačítka „Potvrzuji a odesílám žádost“. Od okamžiku odeslání žádosti je veškerá práce s žádostí zálohována na pevný disk, takže v případě havárie aplikace, výpadku el. energie apod. bude při příštím spuštění ICARA obnoven přesně stejný stav jako před výpadkem.

3.6.4. Krok 7 – Čekání na odpověď Certifikační autority

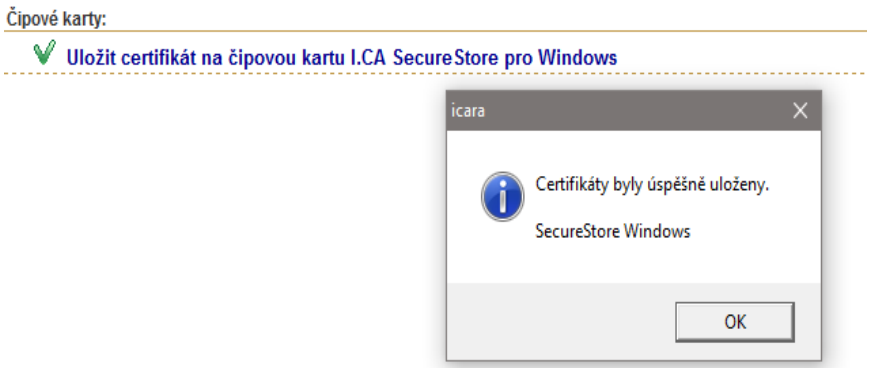
Aplikace ICARA se v tomto kroku pravidelně dotazuje serveru I.CA na úspěšné vyřízení žádosti. Doba čekání bývá 5-10 minut. Během této doby je operátor stručně informován o stavu zpracování textovým popisem.

Funkčnosti a možnosti při obnově certifikátu se v tomto kroku nijak neliší od vydávání prvotního certifikátu.

3.6.5. Krok 8 - Předání certifikátu

Po úspěšném získání certifikátu z CA budou certifikáty automaticky uloženy na čipovou kartu klienta a dojde k uložení poplatkového účtu na server ČSOB. Obnovené certifikáty se na server IM neukládají.

Pokud se certifikáty na kartu automaticky neuloží, např. z důvodů naplnění karty, je operátor, po odstranění nepotřebných certifikátů z karty, uloží prostřednictvím odkazu „Uložit certifikát na čipovou kartu I.CA SecureStore“. Po uložení a předání certifikátu aplikace automaticky přejde k dalšímu kroku.

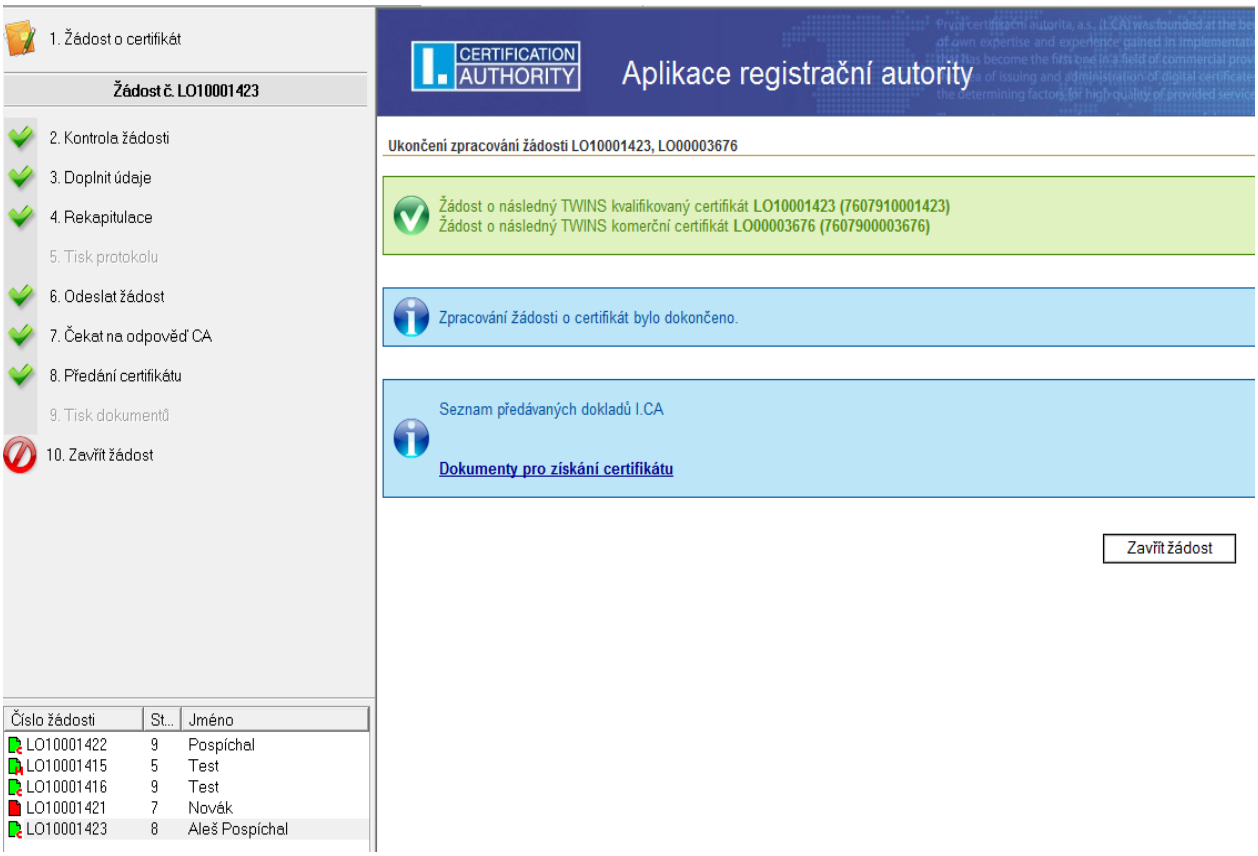


3.6.6. Krok 9 - Tisk dokumentů

Při obnově není nutné tisknout znovu smlouvu o vydání a používání certifikátu a jiné zbývající dokumenty. Proto je tento krok deaktivován a přeskakován. Dodatečné informace o obnoveném certifikátu budou klientovy zaslány na uvedený email.

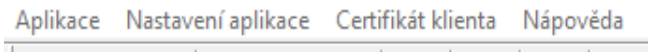
3.6.7. Krok 10 - Zavřít žádost

Žádost o obnovu operátor uzavře kliknutím na tlačítko „Zavřít žádost“.



3.7. Možnosti MENU

V této části příručky jsou stručně popsány funkce aplikace, které může operátor využívat z menu. Menu je rozděleno na 4 části:



Aplikace - umožní změnit vizuální nastavení aplikace skrýváním nebo zobrazením oken. Také je zde možno aplikaci zavřít.

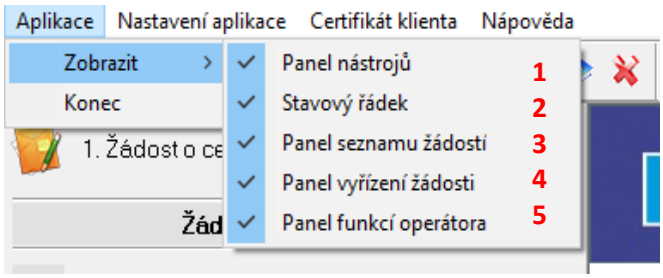
Nastavení aplikace - umožní změny nastavení aplikace, správu operátorů majících oprávnění pracovat s RA, nastavení tisku a připojení k internetu.

Certifikát klienta - pomocné menu operátora, které umožňuje načítat certifikáty klientů a poskytovat další služby I.CA (zneplatňování certifikátů, předávání kořenových certifikátů, předávání certifikačních politik apod.)

Nápověda - v této části jsou odkazy na nápovědu, příručku a další informační kanály pro operátory (odkaz „O aplikaci“)

3.7.1. Aplikace

Zobrazit
Můžete zvolit, která část okna aplikace bude zobrazena nebo skryta.



1) Panel nástrojů

a) b) c) d) e) f) g) h) i)

a) Otevřít žádost - táž funkce jako Krok 1 v panelu vyřízení žádostí

b) Uložit žádost, Uložit žádosti - umožní uložení rozpracovaného stavu žádosti (žádostí) ještě před Krokem 6, kdy jsou žádosti ukládány automaticky

c) Obnovit stránku - funkce totožná s funkcí Internet Exploreru

d) Zpět - funkce totožná s funkcí Internet Exploreru

e) Domů, O aplikaci - odkaz na úvodní stránku aplikace RA

f) Test spojení na servery CA – zjistí, zda jsou dostupné servery certifikační autority

g) Tisk aktuální stránky - vytiskne aktuální stránku, ve které se nachází aplikace

h) Nápověda - vstup do nápovědy, jsou zde uloženy informace zobrazované pod otazníky v Kroku 3 - Doplnění údajů

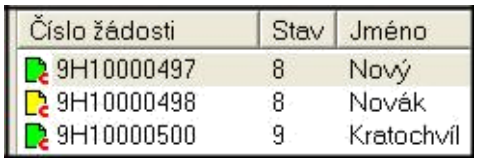
i) Konec - ukončení aplikace

2) Stavový řádek

Zobrazuje typ žádosti, která je právě vyřizována. Stavový řádek leží ve spodní části okna aplikace.

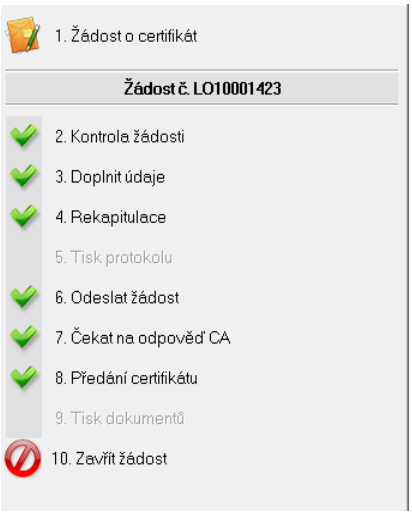
3) Panel seznamu žádostí

V tomto oknu jsou zobrazeny rozpracované žádosti, kterým již bylo přiděleno jedinečné číslo. Dále je zobrazen stav vyřízení žádosti (resp. krok, ve kterém se žádost nachází) a CN certifikátu pro jednodušší identifikaci.



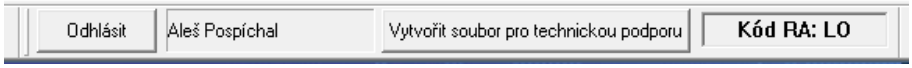
4) **Panel vyřízení žádostí**

Zobrazuje jednotlivé kroky, ve kterých se nachází konkrétní žádosti. Pokud je krok splněn, je označen značkou. Po splnění všech požadovaných kroků (1-9) lze žádost zavřít.



5) **Panel funkcí operátora**

Umožňuje přihlášení a odhlášení operátora dle zobrazeného seznamu. Dále umožňuje vytvořit soubor pro technickou podporu a zobrazuje nastavené číslo pobočky RA (kód RA).



Konec

Kliknutím zavře aplikaci. Pokud máte rozpracované žádosti, budete na tuto skutečnost upozorněni.

3.7.2. Nastavení aplikace

Operátor

1) **Přihlásit operátora, Odhlásit operátora** - slouží k přihlášení nebo odhlášení již zavedeného operátora do RA. Totožnou funkci má Panel funkcí operátora v hlavním okně aplikace.

2) **Nový certifikát operátora**

Operátor RA se autorizuje při komunikaci s I.CA svým operátorským certifikátem. Tento certifikát má uložen privátní klíč na čipové kartě operátora (typ Starcos) a držiteli certifikátu bylo schváleno a přiděleno v databázi I.CA oprávnění operovat na RA (tzv. „právo OPRA“). Certifikát operátora musí být importován do aplikace ICARA při zavádění operátora do seznamu operátorů, kteří mohou na dané pobočce RA pracovat. To znamená, že aplikace ICARA tento certifikát zná a může sledovat dobu jeho platnosti, zjednodušovat jeho obnovování apod.

Certifikát operátora si registruje do systému Windows sama aplikace ICARA, není potřeba ho ručně registrovat. Při zrušení nebo poškození registrace v systému si ji aplikace ICARA sama obnoví při novém přihlášení operátora.

Volba menu „Nový certifikát operátora“ slouží pro vytvoření žádosti o TWINS certifikát, který má být použit jako certifikát operátora. Před generováním žádosti je zapotřebí přihlásit existujícího operátora. Protože certifikát je z hlediska I.CA certifikát jako každý jiný a musí být vydán v souladu s CP I.CA, je potřeba uvést osobní údaje operátora (rodné číslo a číslo občanského průkazu). Po stisku tlačítka „Pokračovat“ je zapotřebí vyměnit čipové karty v operátorské čtečce. Ze čtečky se na výzvu aplikace vyjme karta přihlášeného operátora a vloží karta operátora, pro kterého se generuje certifikát. Na tuto druhou kartu bude uložen soukromý klíč k novému certifikátu. Karty vyměňujte vždy, až po upozornění programu!

Po odsouhlasení se zobrazí formulář pro vložení osobních údajů operátora. Tyto údaje budou použity pro položky nového certifikátu. Zadávají se s diakritikou. Po stisku „Kontrola žádosti“ je zobrazena rekapitulace údajů a na další stisk tlačítka „Vytvořit žádost“ se žádost vygeneruje a načte pro zpracování do ICARA. Po automatickém načtení vygenerované žádosti do ICARA program zobrazí výzvu pro vložení původní čipové karty operátora, který je přihlášen (jménem kterého se bude žádost vyřizovat).

Další zpracování žádosti o certifikát operátora probíhá podobně jako zpracování běžné žádosti, až na krok 3 (doplnění údajů), který je vypuštěn. Po načtení žádosti do ICARA je žádost v kroku 5 - tisk protokolu o podání žádosti. Tento protokol tedy vystavuje existující operátor novému operátorovi. Po odeslání žádost a získání vydaného certifikátu se žádost dostává do kroku 8 – Předání certifikátu, který je třeba přeskočit do bodu 9 - Tisk dokumentů.

Poté, co bude tomuto novému certifikátu schváleno a přiděleno oprávnění operovat na RA (právo „OPRA“), bude možné nového operátora přihlásit do aplikace a vyřizovat jeho jménem běžné žádosti. **Pro přidělení tohoto oprávnění je potřeba kontaktovat helpdesk ČSOB!**

3) **Vydání následného certifikátu operátora**

Obnovuje se vždy certifikát toho operátora, který je právě přihlášen. Na formuláři je potřeba určit úložiště privátního klíče certifikátu (SecureStore CSP) a heslo pro zneplatnění obnoveného certifikátu. Po vyplnění údajů operátor stiskne „Pokračovat“, program vygeneruje nový privátní klíč na čipovou kartu a současně žádost o certifikát a tuto žádost načte do ICARA.

Zpracování žádostí je zkráceno - kroky č. 3, 4 a 5 jsou trvale neaktivní. Po načtení je žádost v kroku 6 (odeslání žádosti). Po odeslání na CA a získání vyhotoveného certifikátu se v kroku 8 „Předání obnoveného certifikátu“ nabídne pouze uložení na čipovou kartu. **Nový certifikát není třeba ukládat**, žádost je teď možné zavřít. Automaticky dojde k přepsání certifikátu v profilu operátora a při příštím přihlášení bude již použit obnovený certifikát. Do té doby platí starý certifikát. **Pozor! Obnovený certifikát automaticky zdědí oprávnění operovat na RA (právo “OPRA”) až po cca 1hodině.** Do té doby musí operátor pracovat se starým certifikátem.

Přepsáním certifikátu v profilu operátora postup obnovy operátorského certifikátu končí.

4) **Aktualizovat seznam operátorů** - aktualizuje seznam operátorů z databáze I.CA. Používá se v případech, kdy byl operátor na I.CA ručně přidán ke konkrétní RA a je nutno jej okamžitě přihlásit.

5) **Zobrazit seznam operátorů** - zobrazí seznam aktuálně zavedených operátorů ke konkrétní RA. Tato stránka umožňuje i další funkce správy operátorů, jako je přidání a odebírání operátorů.

6) **Informace o čipové kartě operátora**

   Tato volba primárně slouží pro správu karty typu GPK4000 a je dostupná, i když není přihlášený žádný operátor. Tento typ karet se již nepoužívá.
   Pro správu operátorské karty se využívá aplikace SecureStore.

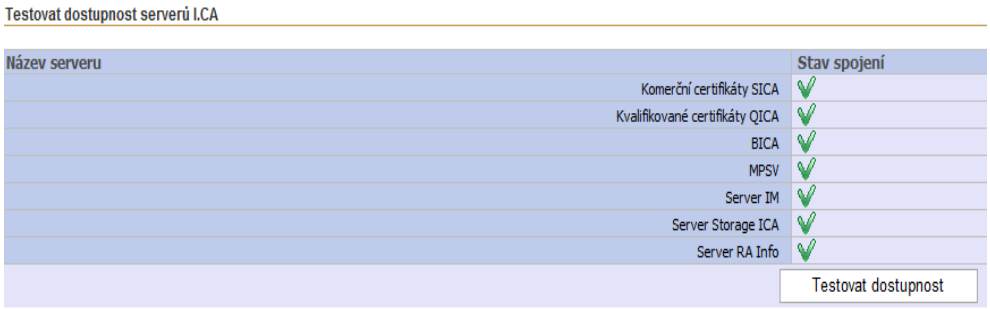
Údržba a ladění aplikace

7) **Vytvořit soubor pro technickou podporu** - vytvoří soubor potřebný pro identifikaci problému, vloží jej jako přílohu do e-mail zprávy a umožní operátorovi doplnit poznámku a mail odeslat na technickou podporu I.CA.

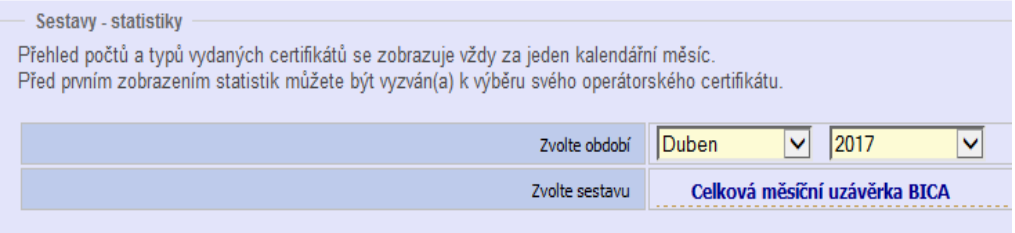
8) **Seznam používaných certifikátů** - zobrazí seznam používaných certifikátů. Tato funkce se využívá při telefonické pomoci hotlineRA operátorovi.

9) **Zobrazit číselník chyb** – zobrazí seznam chybových kódů aplikace

10) **Provést test spojení na servery CA** – zjistí, zda jsou dostupné servery certifikační autority. Tato funkce se využívá při telefonické pomoci hotlineRA operátorovi.



Sestavy a statistiky



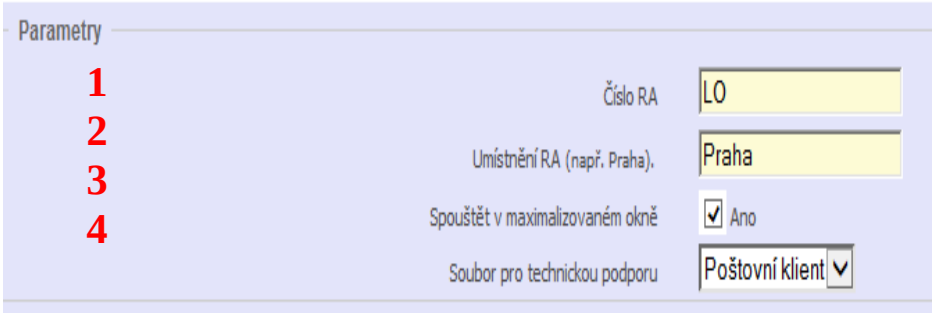
Přehled počtů a typů vydaných certifikátů se zobrazuje vždy za jeden kalendářní měsíc. Před prvním zobrazením statistik budete vyzván(a) k výběru svého operátorského certifikátu. Kliknutím na odkaz „Celková měsíční uzávěrka“ se dostanete na stránku s potřebnou informací.

Ve statistikách se typy certifikátů označují zkratkami:

SC – komerční certifikát
QC – kvalifikovaný certifikát
SS – komerční serverový certifikát
SP – komerční podpisový certifikát k serverovému
QS – kvalifikovaný systémový certifikát
QT – žádost o kvalifikovaný systémový certifikát vyžadující podpisový certifikát
QP – žádost o kvalifikovaný podpisový certifikát pro obnovu
QD – TWINS (kvalifikovaný a komerční certifikát)

Sloupec REQ_ID obsahuje čísla žádostí (ve tvaru pro databázi), na základě kterých byly certifikáty vydány.
Kliknutím na pořadové číslo si lze nechat zobrazit detaily o konkrétním certifikátu.

Parametry



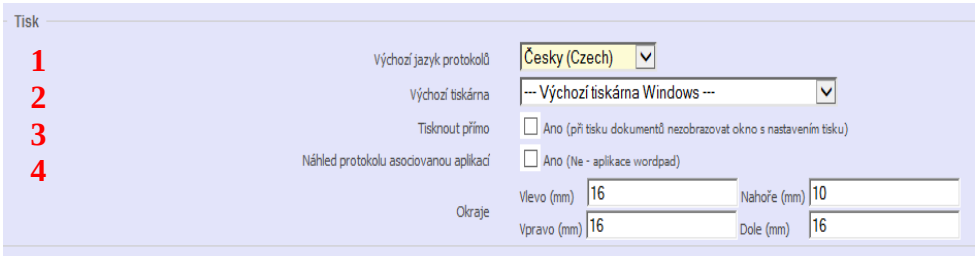
1) **Číslo RA** - je nutno doplnit dvouznakový kód RA, ke kterému je v databázi I.CA přidělen konkrétní certifikát operátora

2) **Umístění RA** - doplní se místo, kde je RA umístěna. Toto místo se zobrazí na protokolech a smlouvách vytištěných k vydaným certifikátům

3) **Spouštět v maximalizovaném okně** - spustí aplikaci v maximální velikosti, kterou umožní monitor.

4) **Soubor pro technickou podporu** – umožňuje si zvolit, jakým způsobem se bude vytvářet soubor pro technickou podporu, zda se pokaždé rovnou otevře nová e-mailová zpráva s přiloženým souborem (je třeba mít na PC operátora nakonfigurovaný některý z podporovaných e-mailových klientů, např. MS Outlook – volba Poštovní klient) nebo zda se soubor uloží na disk ve formě souboru (volba Uložit na disk) nebo zda bude operátor o způsobu vytvoření souboru dotázán při každém stisku tlačítka "Vytvořit soubor pro technickou podporu" (Výběr).

Tisk



1) **Výchozí jazyk protokolů** - lze nastavit, v jakém jazyku se budou tisknout jednotlivé protokoly a smlouvy k vydaným certifikátům. Jazyk protokolů pak lze změnit pro konkrétní certifikát.

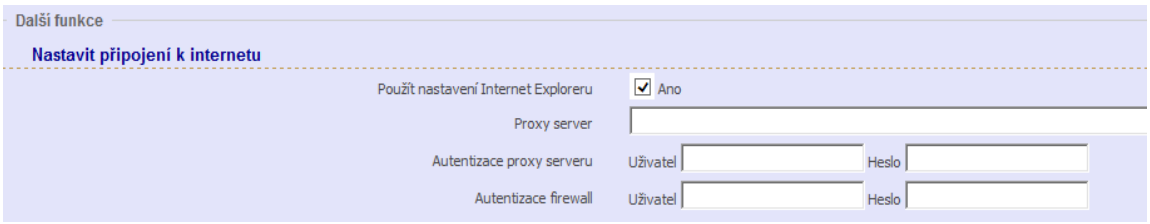
2) **Výchozí tiskárna** - zde je možno vybrat a nastavit výchozí tiskárnu pro aplikaci RA. Uplatnění najde především u mobilních RA.

3) **Tisknout přímo** - při tisku se nezobrazuje dialog tiskárny.

4) **Náhled protokolu asociovanou aplikací** – umožňuje výběr aplikace, ve které se bude zobrazovat náhled vybraných tisknutých dokumentů. Pokud není zaškrtnuto, náhled se bude otevírat v aplikaci MS Wordpad

Další funkce

1) **Nastavit připojení k internetu**
Po rozkliknutí se zobrazí následující formulář:



Použít nastavení Internet Exploreru - využije nastavení Windows pro připojení k internetu

Proxy server/Autentizace proxy serveru - pokud na internet přistupujete z podnikové sítě přes proxy server, je zde možné zadat údaje pro přístup z vnitřní sítě na internet

Autentizace firewall - pokud na internet přistupujete z podnikové sítě přes firewall, je zde možné zadat údaje pro přístup z vnitřní sítě na internet

1) **Povolené typy žádostí**

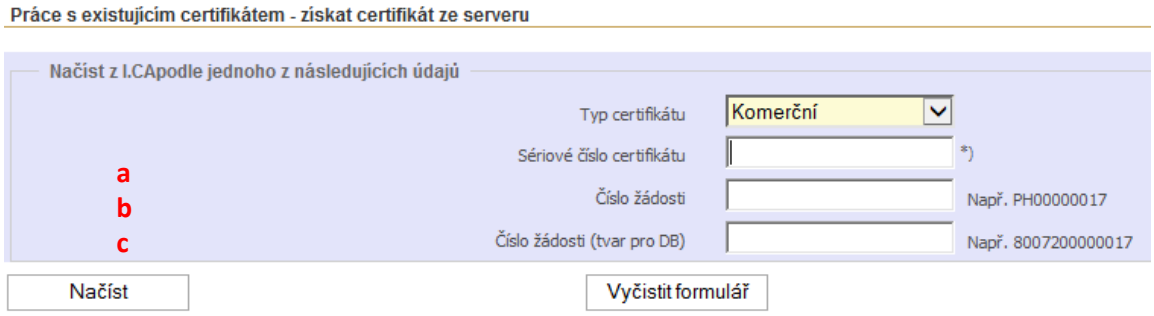
Zobrazuje typy žádostí, které jsou povoleny pro dannou instalaci RA. Např.

Pokud změníte nastavení aplikace (Parametry, Tisk, Připojení k internetu), je nutno aktuální stav prostřednictvím stejnojmenného tlačítka uložit!

3.7.3. Certifikát klienta

Práce s existujícím certifikátem

1) **<u>Získat existující certifikát ze serveru CA</u>** – v případě potřeby je možno z databáze I.CA stáhnout již vydaný certifikát a dále s ním pracovat



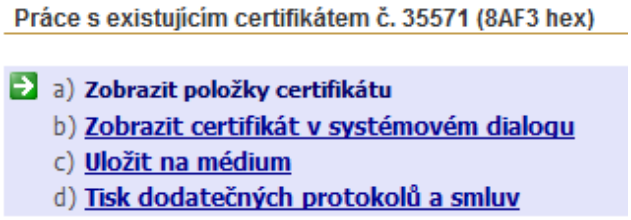
Operátor v prvním kroku volí, zda se jedná o komerční nebo kvalifikovaný certifikát, a následně uvádí jeden (pouze jeden) ze 3 způsobů identifikace certifikátu, a to:

a) <u>Sériové číslo certifikátu</u> - pokud jej uvádí v hexadecimálním tvaru, musí číslo uvést znaky 0x (nula x)

b) <u>Číslo žádosti</u> (na základě které byl certifikát vystaven) v textovém tvaru. Textový tvar žádosti se skládá z dvojpísmenné zkratky pobočky RA a 8 číslic, např. 7B10000258

c) <u>Číslo žádosti ve tvaru pro DB</u>

Pokud byl certifikát úspěšně načten, zobrazí se operátorovi v druhém kroku obrazovka s několika volbami pro práci s tímto certifikátem:

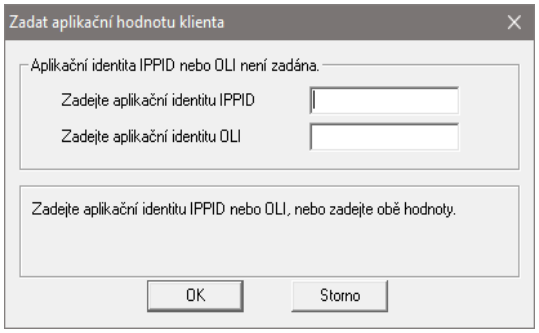


a) Zobrazení položek certifikátu - zobrazení položek předmětu certifikátu, sériového čísla a platnosti

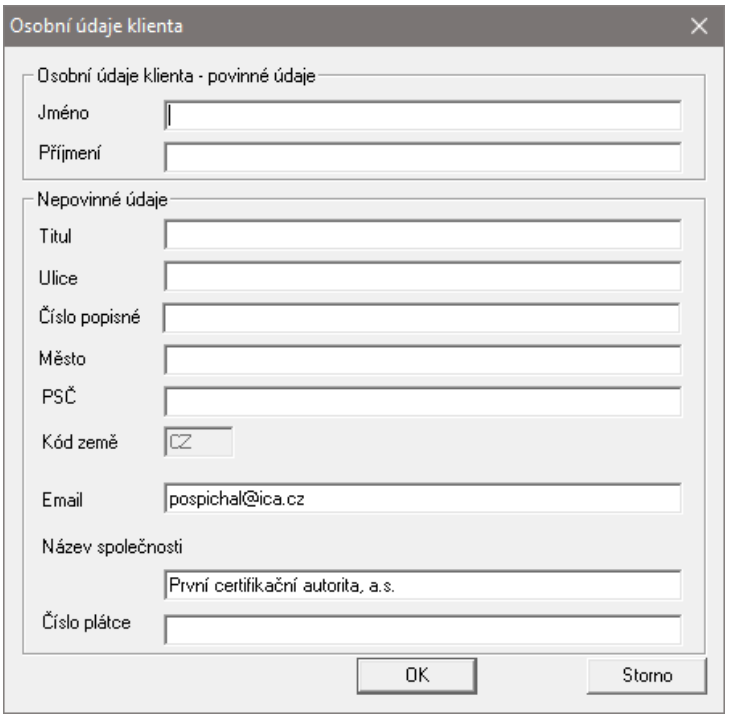
b) Zobrazit certifikát v systémovém dialogu – volba zobrazí certifikát v prostředí Windows

c) Uložení na médium – umožňuje certifikát uložit na zařízení podporované danou instalací RA, obdobně jako v kroku 8 – Předání certifikátu

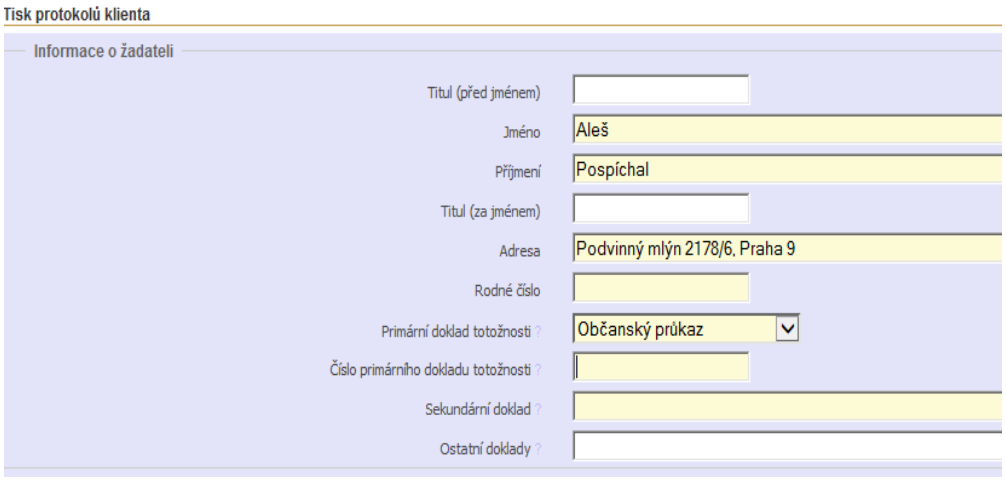
V případě uložení certifikátu na server I.CA IM volbou „Uložit certifikát klienta na server I.CA IM“ bude nejprve zobrazeno dialogové okno pro zadání aplikační identity (IPPID)



a v následujícím kroku budou požadovány osobní údaje o klientovi. Povinné údaje jsou: jméno a příjmení. Ostatní údaje jsou nepovinné. Do položky „číslo plátce“ doplňte číslo plátce, pod kterým byl certifikát vydán. (Platí pro ne-klientské)



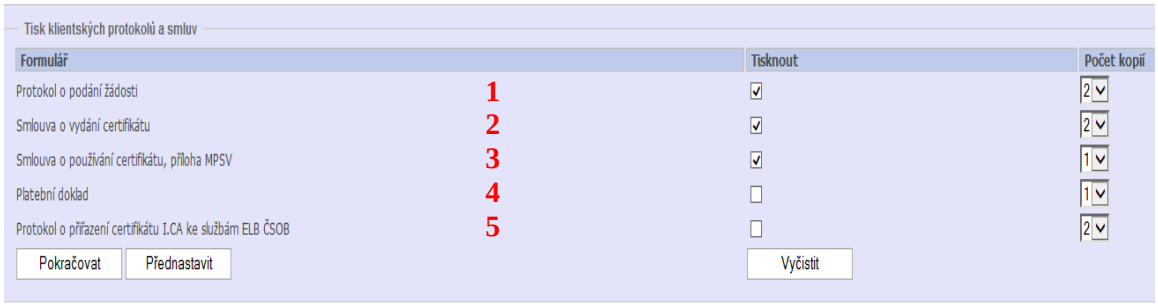
d) Tisk dodatečných protokolů a smluv – po volbě typu dotiskovaných dokumentů a kliknutím na tlačítko „Pokračovat“, je třeba doplnit požadované údaje dle osobních dokladů držitele certifikátu



2) **<u>Zneplatnit certifikát</u>** – certifikát je možno na základě oprávněné žádosti nechat zneplatnit. O zneplatnění certifikátu musí být pořízen protokol a podepsán žadatelem. Pokud žadatel nezná heslo pro zneplatnění certifikátu, musí operátor ověřit totožnost žadatele dle osobních dokladů. V tomto případě je doporučeno kontaktovat pracovníky
I.CA pro konzultaci postupu

Nastavení jazyku protokolů – umožňuje navolit jazyk tištěných protokolů

Tisk klientských protokolů a smluv - pomocí této funkce lze dotisknout potřebné chybějící protokoly a smlouvy k již vydanému certifikátu. Podle vybraných možností budete vyzváni k doplnění údajů o žadateli nebo certifikátu. Z těchto údajů bude vytvořen patřičný protokol či smlouva.

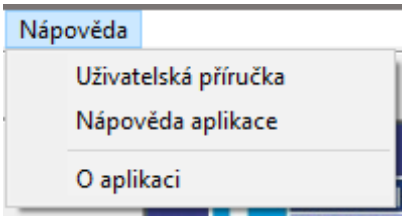


<u>Jsou k dispozici tisky těchto protokolů:</u>

1) Protokol o podání žádosti o certifikát
2) Smlouva o vydání certifikátu
3) Smlouva o používání certifikátu – příloha MPSV
4) Daňový doklad
5) Protokol o přiřazení certifikátu I.CA ke službám ELB ČSOB

Pro každý z protokolů je potřeba vyplnit potřebné údaje. Jednotlivé položky na formulářích mají stejný význam jako při zadávání údajů v kroku 3 při zpracování běžné žádosti. V případě protokolů, které vyžadují zadat certifikát, je výhodné nejprve zvolit certifikát, protože v případě kvalifikovaného certifikátu se údaje uvedené v certifikátu přednastaví do formuláře.

3.7.4. Nápověda



Uživatelská příručka - přímý vstup do této příručky.

Nápověda aplikace - informace o údajích, které mají být zjištěny o žadateli.

O aplikaci - zobrazí identifikační údaje aplikace RA a přihlášeného operátora. Stránka také obsahuje užitečné odkazy na informační podporu operátorů, jako jsou stránky I.CA, stránky určené pro operátory (rainfo), přímé odkazy na certifikační politiky, na seznam veřejných a na seznam zneplatněných certifikátů.

4. Práce s operátorskou čtečkou karet

4.1. Čtečka čipových karet ORGA 920 M

Čtečka nepodporuje správu čipové karty. Pro správu čipové operátorské karty je potřeba použít nainstalovanou klientskou aplikaci SecureStore.

Výchozí stav čtečky po jejím zapnutí je:

				O	R	G	A		9	0	0				
		I	N	G	E	N	I	C	O	-	C	Z			

Čtečka po vložení karty provede kontrolu vložené karty. Pokud je kontrola provedena úspěšně, je na displeji čtečky zobrazena zpráva pro zadání PIN karty:

C	a	r	d		P	I	N	:							
*	*	*	*	*	*	*									

Ověření zadaného PIN proběhne vždy při použití privátního klíče. Pokud je ověření PIN neúspěšné, je na obrazovce PC zobrazen informační dialog a čtečka zobrazí výzvu pro zadání PIN.

Zadaný PIN potvrdíme zelenou klávesou OK.

Správně zadaný PIN je po ověření potvrzen zobrazenou zprávou:

S	t	a	r	c	o	s		3	.	0					

Při vložení nepodporované karty je na displeji zobrazena zpráva:

N	e	z	n	a	m	a		K	a	r	t	a		
V	y	j	m	e	t	e		k	a	r	t	u		

4.2. Čtečka čipových karet INGENICO iHC200

Pro správu čipové operátorské karty je potřeba použít nainstalovanou klientskou aplikaci SecureStore.

Výchozí stav po zapnutí bez vložené operátorské karty je:

Nyní je možné vložit kartu operátora – k tomuto účelu slouží zadní slot ze spodní části čtečky. Po vložení operátorské karty by se měla zobrazit informace Karta vložena a vzápětí by měl být operátor vyzván k zadání PIN. Pokud zůstane zobrazena pouze informace o vložení karty, zkuste kartu znovu zastrčit.

Nyní zadejte PIN ke své operátorské kartě a potvrďte zeleným tlačítkem. Po zadání PIN čtečka napíše Operátor přihlášen, případně oznámí, že byl PIN zadán chybně se zobrazením informace o zbývajících pokusech, a vyzve znovu k zadání PIN. Po úspěšném přihlášení je možné pokračovat přihlášením operátora do aplikace ICARA.

Tato čtečka čipových karet obsahuje také horní slot, který je možné použít pro vložení čipové karty klienta, na kterou se bude generovat žádost o certifikát.

Pokud bude při práci s čipovou kartou klienta požadován PIN, bude zobrazení na čtečce následující. PIN klient zadává také na této čtečce a potvrzuje zeleným tlačítkem.

5. Řešení chybových stavů

Při nestandardním chování aplikace, problémem se žádostí nebo certifikátem, má operátor RA možnost kontaktovat technickou podporu RA na e-mailové adrese hotlinera@ica.cz, případně zhotovit soubor pro technickou podporu pro urychlení identifikace problému (viz. menu Nastavení aplikace/Vytvořit soubor pro technickou podporu).