Uživatelská příručka RA pro ČSOB



Datum: prosinec 2019 Verze: 3.0

Obsah

1.	Úvod		3
2.	Účel ap	likace	3
3.	Obsluh	a RA	3
3.	1. Zá	kladní myšlenka	3
3.	2. Sp	uštění aplikace a přihlášení operátora RA	3
3.	3. Pr	votní přihlášení operátora	4
3.	4. Už	źivatelské rozhraní	5
3.	5. Zp	vracování žádosti o prvotní certifikát	6
	3.5.1.	Krok 1 – Žádost o certifikát	6
	3.5.2.	Krok 2 – Kontrola žádosti	10
	3.5.3.	Krok 3 – Doplnit údaje	11
	3.5.4.	Krok 4 – Rekapitulace	13
	3.5.5.	Krok 5 – Tisk protokolu o podání žádosti	14
	3.5.6.	Krok 6 - Odeslat žádost	14
	3.5.7.	Krok 7 – Čekání na odpověď Certifikační autority	15
	3.5.8.	Krok 8 - Předání certifikátu	17
	3.5.9.	Krok 9 - Tisk dokumentů	19
	3.5.10.	Krok 10 - Zavřít žádost	19
3.	6. Žá	dost o následný certifikát	20
	3.6.1.	Krok 1 – Žádost o certifikát	20
	3.6.2.	Krok 5 – Tisk protokolu o podání žádosti	23
	3.6.3.	Krok 6 - Odeslat žádost	23
	3.6.4.	Krok 7 – Čekání na odpověď Certifikační autority	23
	3.6.5.	Krok 8 - Předání certifikátu	23
	3.6.6.	Krok 9 - Tisk dokumentů	23
	3.6.7.	Krok 10 - Zavřít žádost	24
3.	7. M	ožnosti MENU	24
	3.7.1.	Aplikace	25
	3.7.2.	Nastavení aplikace	26
	3.7.3.	Certifikát klienta	32
	3.7.4.	Nápověda	35
4.	Práce s	operátorskou čtečkou karet	35
4.	1. Čt	ečka čipových karet ORGA 920 M	35
4.	2. Čt	ečka čipových karet INGENICO iHC200	36
5.	Řešení	chybových stavů	39

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.

		Přihlási	t operátora	Vytvořit sou	bor pro technickou podporu	Kód RA: LO
	DRITY Apl	ikace re	gistrační a	utority I.C	The superior of the second se	inded at the begin that the r implementation of parts of provided services of the cost of ravided services
O aplikaci ICARA						
o upintuei zoritot		Název aplikace	icara			
		Verze aplikace	4.7.0.0			
		Kód RA	LO			
	Přih	lášený operátor	není přihlášen			
	Pla	tnost certifikátu	?			
Užitečné odkazy www.ica.cz	RA info	Certifika	ační politiky	Se	znam veřejných certifik	átů
		icara	This product inc okračovat přihlášením o	ciudes software develo covetores operátora?	Aplikace využívá knihovr oped by the OpenSSL Project bio software written by Eric Y -2017 All Right Res nformace na interne	nu OpenSSL. for use in the OpenSSL Toolkit (www.opens Young (eay@cryptsoft.com) erved Vaše dotazy zodpovíme na ac tu <u>www.ica.cz</u>
		A	Ne Ne	Zrušit		

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.

Parametry	
Číslo RA	LO
Umístnění RA (např. Praha).	Praha
Spouštět v maximalizovaném okně	✓ Ano
Soubor pro technickou podporu	Poštovní klient
Tisk	
Výchozí jazyk protokolů	Česky (Czech)
Výchozí tiskárna	Výchozí tiskárna Windows 🔽
Tisknout přímo	🗹 Ano (při tisku dokumentů nezobrazovat okno s nastavením tisku)
Náhled protokolu asociovanou aplikací	Ano (Ne - aplikace wordpad)
Okraje	Vlevo (mm) 16 Nahoře (mm) 10

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.

Aplik	ace Nastavení aplikace Certifikát klienta Nápovéda					
1	। स 🔠 😂 😓 🏠 😓 🤞 🔇	> 😽	Odhlásit	Aleš Pospíchal	Vytvořit soubor pro technickou podpo	ru Kód RA: LO
	1. Žádost o certifikát Žádost č. LO10001421		Aplikace	registračn	í autority I.CA	LCA) was founded at the begin see gained in Implementation n a field of commercial provid stration of digital certificates h quality of provided services.
Ý	2. Kontrola žádosti	0 aplikaci ICARA			,engini	
	3. Doplnit údaje	Název aplikace	icara			
	4. Rekapitulace	verze apiikace Kód RA Přihlášený operátor	LO Aleš Pospíchal			
	5. Podpis protokolu žádosti	Platnost certifikátu	zbývá 286 dnů			
	6. Odeslat žádost					
	7. Čekat na odpověď CA	Užitečné odkazy www.ica.cz RA info Cert	ifikační politiky	Seznam veřejných	n certifikátů <u>Seznam zneplat</u>	něných certifikátů
	8. Předání certifikátu					
	9. Podpis dokumentû		А	plikace využívá knihovnu	J OpenSSL.	
Ø	10. Zavřít žádost	This product include	s software developed b cryptographic so	y the OpenSSL Project fo ftware written by Eric Yo	or use in the OpenSSL Toolkit (www.opens: oung (eay@cryptsoft.com)	il.org) and
Čísk Císk C	o žádosti St Jméno D10001415 5 Test D10001416 9 Test D10001421 3 Pospíchel	Copyright První certifikač	ní autorita, a.s. 2000 Další i	-2017 All Right Rese	rved Vaše dotazy zodpovíme na adi u <u>www.ica.cz</u>	ese <u>hotline RA</u> .

"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.

Aplikace Nastavení aplikace Certifikát klienta Nápověda				
😰 स. स. 🗘 😓 🎊 🤌 😕 🧀	*	Odhlásit Aleš Pospíchal	Vytvořit soubor pro technickou podporu	Kód RA: LO
1. Žádost o certifikát Žádost č. LO10001443	CERTIFICATION AUTHORITY A	plikace registrační	autority	was founded at the begin ained in implementation eld of commercial provid on of eligital certificates i lity of provided services.
 2. Kontrola žádosti 3. Doplnit údaje 4. Rekapitulace 5. Tisk protokolu 6. Odeslat žádost 7. Čekat na odpověď CA 8. Předání certifikátu 9. Tisk dokumentů 10. Zavřít žádost 	Výběr žádosti o certifikát Vytvořeni žádosti o certifikát Generátory žádosti: Klient ELB (bezpapírov TWINS pro zaměstnance Č Neklient ČSOB Klient ELB (papírová doku Další volby Elexims (bezpapírově)	ré) 🐿 :SOB mentace, jednání v zastoupen) A	
Číslo žádosti St Jméno ^ LO10001443 9 Test ^ R 811000401 9 Novák ^ R 811000416 8 Novák ^ R 110001441 10 TEST ^ LO10001448 9 folytimututututututututututututututututututu	Flexins (papirově) Flexins (papirově) Načtení existující žádosti o certi Server Načíst žádost ze serveru I.	fikát CA	B	

"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.

– Vytvoření žádosti o certifikát – Generátory žádostí:	
🕼 Klient ELB - Windows (bezpapírově) 🐿	
Vložení Identifikačního čísla klienta - získání personálních dat žadatele o certifikát	×
Výběr typu identifikace:	
Identifikační číslo:	
Zadané hodnoty dále slouží pro vyhledání poplatkových účtů. OK Storno	

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.

Uvolnit místo na karté Operace "generování" byla po kartě odstraněním nepotřební	zastavena z důvodu ch obiektů.	u vyčištění čipové karty	y, je potřeba uvolnit mís	> to na
Během mazání objektů budete Název kontejneru Objekt 09/12/2019 12:54:26 Objekt 09/12/2019 12:58:19 Objekt 09/12/2019 12:58:49 P1 P11 P21	vyzvání k zadání PI	N. Sériové číslo	Platnost certifikātu	
Ponechat privátní klíče			OK Zruš	it

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.

Chyba při získání dat o klientovi. Vyberte z následujících možností: Znovu zadat identifikační číslo Přerušit zpracování žádosti	Chyba		×
Znovu zadat identifikační číslo	Chyba při :	získání dat o klientovi. Vyberte z následujících n	nožností:
Přerušit zprzopyžní žádosti		Znovu zadat identifikační číslo	
		Přerušit zpracování žádosti	
Pokračovat s manuálním zadáním dat		Pokračovat s manuálním zadáním dat	

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

Vložení ldentifikačního čísla klienta – získání poplatkových účtů	×
Výběr typu identifikace:	
Identifikační údaje: IČID: OLI: I + I IPPID:	
Vložené ldentifikační číslo slouží pro vyhledání poplatkových účtů OK Storno	

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.

Přin	ačtení seznamu poplatkových účtů nastala chyba
	Znovu zadat identifikační číslo
	Pokračovat a vydat certifikát bez poplatku

Volba "Klient Flexims"

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.

Zadejte osobní číslo zaměstnance	×	ľ
Osobní číslo zaměstnance	OK	
	Storno	
		J

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.

		rogistrační autority	t one in a field of commercial provide not sophi	
Žádost č. LO10001421			igministration of digital certificates the Crech in the Greek in the Crech in the C	
2. Kontrola žádosti	Kontrola žádosti o certifikát			
3. Doplnit údaje	a) Automatická kontrola Kontrola žádosti byla úspo	išně dokončena.		
4. Rekapitulace	D) Zobrazit položky žádosti			
	Žádost o certifikát			
5. Tisk protokolu	Číslo žádosti	L010001421 (7607910001421)		
C. Oxforelat Xédant	Typ certifikátu	Žádost o TWINS kvalifikovaný certifikát pro zaměstnar	nce	
	Doložky žádosti			
7. Čekat na odpověď CA	Polozky zadosti Zkratka	Názov položky	Názov položky	Hodnota
	Childred	commonName	Obacné iména	Ing. Aleč Despichal Cos
8. Předání certifikátu	con an	contributivative generationQualifier	Gonorační rozličaní	Ing. Ales Pospicital CSC.
	generationQualiter	serialtiumber	Cárlavá čísla	IDCC7 12241224
9. Tisk dokumentů	senaivumber	le calitativame	Seriove cisio	DCC2-12341234
	C. C	IDCallCyName above OrDen in settleme	MISLO	Praha 10
10. Zavřít žádost	51	stateOrProvincename	ODIASE	Prana
		countryname	Stat	CZ
	0	organizationName	Nazev nrmy	Prvni certifikacni autorita
	00	organizationalUnitName	Nazev casti firmy	Helpdesk
	ticle	title	Pozice ve firme	Pracovnik neipdesku
	street	streetAddress	Ulice	Podvinny mlyn 21/8/6
	postalCode	postalCode	PSC	10400
	GN	givenName	Krestni jmeno	Ales
	SN	sumame	Přijmení	Pospichal
	Žádost o certifikát			
	Číslo žádost	LO00003674 (7607900003674)		
∋žádosti St… Jméno	Typ certifikáti	Žádost o TWINS komerční certifikát pro zaměstnan	ce	
010001415 5 Test				
010001416 9 Test	Položky žádosti			
010001421 3 Posnichal	Zkratka	Název položky	Název položky	Hodnota
	CN	commonName	Obecné iméno	Ing. Aleš Pospíchal Csc.
	generationOualifier	generationOualifier	Generační rozlišení	MI.
	serialNumber	serialNumber	Sériové číslo	IDCC7-12341234
	1	localityName	Místo	Praha 10
	ST	stateOrProvinceName	Oblast	Praha
	C	countryName	Stát	C7
	0	organizationName	Název firmy	První certifikační autorita
	01	organizational InitName	Název části firmv	Heindesk
	title	title	Pozice ve firmě	Pracovník belodesku
	streat	streetAddress	llice	Podvinný mýn 2179/6
	postalCode	nostalCode	DSČ	10400
	CN	pustacoue	r Ju Všestej iméne	10400
		giverindine	Niesun Jineno	Ales
	ON CN		D ^M ara - (Decesteland

Grafické rozlišení typů žádosti o certifikát

- 📔 žádost o službu TWINS
- 퇹 vydané certifikáty služby TWINS
- žádost o kvalifikovaný certifikát
- 🔁 vydaný kvalifikovaný certifikát
- 🗋 žádost o komerční certifikát
- 🗳 vydaný komerční certifikát
- Р 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).

Informace o žadateli - Žádost o službu TWINS pro zaměstnance		
	Hodnota z žádosti	Vstup operátora
Titul (před jménem) ?	Ing.	Ing.
Jméno ?	Aleš	Aleš
Příjmení ?	Pospíchal	Pospíchal
Titul (za jménem) ?	Csc.	Csc.
Ulice ?	Praha 10	Podvinný mlýn
Č. popisné/orientační		2178/6
Město		Praha 10
PSČ ?		10400
Stát	CZ	Česká republika 🗸
Rodné číslo ?		U cizinců je možné místo RČ zadat datum narození
Pohlaví ?		
Doklad totožnosti ?		Občanský průkaz 🗸
Číslo primárního dokladu totožnosti ?		
Sekundární doklad ?		
Ostatní doklady ?		
E-mail ?	pospichal@ica.cz	pospichal@ica.cz
Fakturační údaje / Informace o právnické osobě		
Po kliknutí na odkaz upravíte fakturační údaje.		
Informace o certifikátu		
		19341934
Hesio pro zneplatneni a		
pädělit IK MPSV 2		
Ostatní údaje		
Jazyková verze protokolů		Česky (Czech)
		Zaslat certifikát v ZIP formátu
Ověřit údaje Opravit plátce		

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!

Dále jen pro ne-klientské certifikáty:

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"

Dopinit údaje - vybrat plátce za certifikát - Žádost o TWINS kvalifikovaný certifikát pro zaměstnance LO10001421 (7607910001421) & Žádost o TWINS komerční certifikát pro zaměstnance LO00003674 (7607900003674)

Metodické pokyny		
Zvolte plátce za certifikát ?		
Identifikátor plátce		Cena vč. DPH
● 999 - ICA a.s obecné		-
Další povolení plátci za certifikát		
Identifikátor plátce		Cena vč. DPH
O 26919 - Česká republika - Česká správa sociálního zabezpečení - PP		-
🔿 10172 - Československá obchodní banka, a.s CZ - Flexims		-
🔾 26905 - Československá obchodní banka, a.s. CZ - HCA		-
🔿 13472 - Československá obchodní banka, a.s. CZ - STARCOS		-
O 26894 - ICA - HCA		-
O 26906 - ICA - HCA - operátorské		-
O 26848 - Michal - Test		-
O 26897 - Mihula - HCA		-
O 26057 - Mihula1		-
○ 9897 - Ministerstvo zahraničních věcí České republiky - CDBP		-
O 12522 - Pay P Univerzál - bez kontrol		-
O 26771 - Samoplátce CZ		495,00 Kč
O 26850 - Samoplátce ČR - EUR, doklady bez DPH		27,10€
○ 26773 - Samoplátce SK		26,88 €

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.

	1. Žádost o certifikát		a ragistrační autority	
	Žádost č. LO10001421		the determining factors for high quality of provided services	
V	2. Kontrola žádosti	Rekapitulace - Žádost o TWINS kvalifikovaný certifikát	t pro zaměstnance LO10001421 (7607910001421) & Žádost o TWINS komerční certifikát pro zaměstnan	ice LO00003674 (7607900003674)
*	3. Doplnit údaje	Údaje zadané na RA		
	4 Rokanitulaco	Název položky	Vstup operátora	Hodnota žádosti
	4. Herophalace	Titul před jménem	Ing.	Ing.
	5. Tisk protokolu	Jméno	Aleš	Aleš
		Příjmení	Novák	Pospíchal
	6. Odeslat žádost	Titul za jménem	Csc.	Csc.
		Adresa	Podvinný mlýn 2178/6, 10400 Praha 10	
	7. Čekat na odpověď CA	Stát (C)	CZ	CZ
		E-mailová adresa	novak@ica.cz	pospichal@ica.cz
	8. Předání certifikátu	Pohlaví	Muž	
		Rodné číslo (datum narození)	111111111	
	9. Tisk dokumentů	Primární doklad totožnosti	OP	
	10 7 *** **-!*	Číslo primárního dokladu	11	
V	TU. Zavni zadusi	Sekundární doklad totožnosti	1111	
		Název organizace (O)	První certifikační autorita, a.s.	
		Platnost certifikátu	365 dnů	
		Zveřejnit certifikát	Ano,Ano	
		Certifikát Comfort	Ne	
		Zaslat certifikát v ZIP	Ne	
		Heslo pro zneplatnění	12341234	
		Identifikátor MPSV	Ano, klient žádá	
		Platbu provede	Platba projekty, Faktura	
		Identifikátor plátce	999 - ICA a.s obecné	
		Jazyk komunikace s klientem	český	
Čísla Di LC Di LC Di LC	žádosti St Jméno 10001415 5 Test 10001416 9 Test 10001421 3 Pospíchal	Pokračovat Opravit údaje		Skrýt položky žádosti

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.

🧊 l	न 🗐 🔷 😓 🏠 🔌 🛃 🧇	* *	Odhlásit Aleš Pospíchal	Vytvořit soubor pro technickou podporu	Kód RA: LO
1	1. Žádost o certifikát Žádost č. LO10001421	CERTIFICATION AUTHORITY A	plikace registrační a	autority	was founded at the beg aned in implementatio at of commercial provide the control of the not original control of the control of the information of the control of the control of the information of the control of the control of the control of the information of the control of the control of the control of the information of the control of the control of the control of the information of the control of the control of the control of the control of the information of the control of the information of the control of
V 2	2. Kontrola žádosti	Čekejte prosím, Vaše žádost o certifikát	se vyřizuje	and south of a second HIMP Hereiter	
쓪 3	3. Doplnit údaje	Žádost o TWINS kvalifikovaný certifik	át pro zaměstnance LO10001421		
🧼 d	4. Rekapitulace	Žádost byla odeslána r Žádost byla přijata I.C.	na I.CA a čeká na provedení kontrol. A a čeká se na schválení způsobu platby z	a certifikát.	
9 🔶	5. Tisk protokolu	Platba za certifikát byl Platba za certifikát byl	a schválena, žádost čeká na přidělení IK M a schválena, žádost čeká na potvrzení ope	PSV erátorem I.CA	
V 6	5. Odeslat žádost	Žádost byla schválena	operátorem I.CA, čeká se na vyhotovení	certifikátu	
ī	7. Čekat na odpověď CA	Žádost o TWINE komorční cortifikát s	ro zaměstnanco 1000002674		
	3. Předání certifikátu	Žádost o tvino konercin cer chikac p	a I.CA a čeká na provedení kontrol.	1.01.71	
	3. Tisk dokumentû	Zadost byla prijata I.C. Platba za certifikát byla	A a ceka se na schvalení způsobu platby z a schválena, žádost čeká na potvrzení ope	a certifikat. erátorem I.CA	
1	0. Zavřít žádost	Žádost byla schválena Certifikát byl vyhotove	operátorem I.CA, čeká se na vyhotovení n.	certifikátu	
		Dokud není vystaven certifikát, je mo	žné zpracování žádosti stornovat.		
		Obnovit			Stornovat žádost
		V případě delší odezvy volejte operát Linka technické podpory tel.: +420 2 Před Vaším dotazem si připravte čís	ory I.CA tel.: +420 577 103 168, +420 84 081 933, 932 Io žádosti o certifikát.	603 900 687 (po-pá 7:00-19:00 hod)	
Číslo ž LO1 LO1 LO1	iádosti StJméno 0001415 5 Test 0001416 9 Test 0001421 7 Novák				

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."

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

<u>Postup operátora</u>: 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."

<u>Příčina:</u> Veřejný klíč obsažený v žádosti byl již v minulosti použit. Typicky se tato chyba objevuje, pokud je jedna žádost poslána na I.CA vícekrát. <u>Postup operátora:</u> 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."

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

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

"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.

<u>Postup operátora:</u> 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."

<u>Příčina:</u> 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."

<u>Příčina:</u> 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.

<u>Postup operátora:</u> 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.

V	2. Kontrola žádosti	Předat vydaný certifikát	
V	3. Doplnit údaje		
V	4. Rekapitulace	K žádosti LO10001571 byl vyhotoven kvalifikovaný certifikát č. 10058357 (997A75 hex). Certifikát si můžete prohlédnout <u>zde</u> .
V	5. Podpis protokolu žádosti		
Ý	6. Odeslat žádost	K žádosti LO00003881 byl vyhotoven komerční certifikát č. 67624 (010828	8 hex). Certifikát si můžete prohlédnout <u>zde</u> .
V	7. Čekat na odpověď CA	ic	cara X
V	8. Předání certifikátu	Zde můžete vybrat způsob uložení certifikátu klientovi. Vybert z přelodníčích měžectí, cedle trav média ži začesku vležení certifi	
	9. Podpis dokumentû	vyberte z nasiedujících moznosti, podle typu media či způsobů dložení čerti	Certifikaty byly úspěšně uloženy.
		Server	SecureStore Windows
Ø	10. Zavřítžádost	✓ Přířadit poplatkovací účet	Server FeeAcount Server IM
		♥ Uložit certifikát klienta na server I.CA IM	
Číslo	o žádosti St Jméno 🔨	Čipové karty:	ОК
	D10001566 3 Test D10001561 8 Novák	♥ Uložit certifikát na čipovou kartu I.CA SecureStore pro Windows	
ID IO	100003869 9 Teet		

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.

	1. Žádost o certifikát		ikačni autorita, a.s., (I. CA) was founded at th bertise and experience gained in impleme come the first one in a field of commercial
	Žádost č. LO10001485		issuing and administration of digital certif ining factors for high quality of provided se
V	2. Kontrola žádosti	Tisk dokumentů	
4	3. Doplnit údaje	Nastavení jazyku protokolu	
V	4. Rekapitulace	Zvolte jazyk protokolů	Česky (Czech) 🔽
Ý	5. Podpis protokolu žádosti	Elektronický podpis dokumentů	
\checkmark	6. Odeslat žádost	Protokol, doklad	Funkce
Ý	7. Čekat na odpověď CA	Zobrazte si dokumenty tlačítkem 🐼, potvrďte jejich správnost tlačítkem Ano a elektronicky	
V	8. Předání certifikátu	podepište tlačitkem 💹	
	9. Podpis dokumentů	Smlouva o vydání a používání certifikátů	
Ø	10. Zavřít žádost		
			()
Číslo) žádosti St., Jméno 🔨	Tisk klientských protokolů a smluv	
	010001506 9 Test	Není potřeba tisknout žádný protokol.	
	010001497 9 Test7		
5 4	10000006 / Lest		
	010001432 4 unioff		
	010001490 10 Test		

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.

🕎 1. Žádost o certifikát	
Žádost č. LO10001422	
父 2. Kontrola žádosti	Ukončení zpracování žádosti LO10001422, LO00003675
💙 3. Doplnit údaje	
🞸 4. Rekapitulace	Žádost o TWINS kvalifikovaný certifikát pro klienta ČSOB LO10001422 (7607910001422) Žádost o TWINS komerční certifikát pro klienta ČSOB LO00003675 (7607900003675)
5. Podpis protokolu žádosti	
6. Odeslat žádost	
7. Čekat na odpověď CA	K teto žadosti nebyl vytisten nebo odeslan na server nektery z protokolu.
8. Předání certifikátu	
9. Podpis dokumentů	Seznam předávaných dokladů I.CA
🕢 10. Zavřít žádost	1. Elektronické dokumenty
<u> </u>	Dokumenty pro získání certifikátu
Číslo žádosti St Jméno	
LO10001415 5 Test LO10001416 9 Test	Zavřítžádost
LO10001421 7 Novák	
LO10001422 9 Pospíchal	

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.

é je platný certifikát pr	o vydání následného certifikátu	×
v	Hodnora	^
méno (CN)	Aleš Pospíchal	
C)		
ni imeno		
eni (5)	Pospichal	
ost do	nátek 6. dubna 2018 8:35:27	
ost od	čtvrtek 6. dubna 2017 8:35:27	
/é číslo	10054061 (0x009969AD)	
	Twins	
	Kvalifikovaný certifikát	
l	Ano	
	Alternativni nazev predmetu	
I (NFLOZZ) N	pospicnal@ica.cz 10029075	
	1234567890	
54	1234307030	× .
	>	
dit		
troloval jsem výše uvede	ené naplnění pro vydání následného certifikátu a souhlasím s	
ačováním vydání násled	ného certifikátu.	
Vudata	páslednú certifikát Storpo Zobrazit	1
vyddri		
		 ž je platný certifikát pro vydání následného certifikátu v Hodnora méno (CN) Aleš Pospíchal CZ ní jméno Aleš ení (S) Pospíchal ost do pátek 6. dubna 2018 8:35:27 zé číslo 10054061 (0x009969AD) Twins Kvalifikovaný certifikát Alternativní název předmětu pospichal@ica.cz N 10029075 vSV 1234567890 Vydat následného certifikátu Vydat následný certifikát Storno Zobrazit

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.

Vj	/běr certifikátu	ı pro vydání následného						×
	Тур	Vystaveno pro	Sériové číslo	Platnost do	Název	Hodnora		^
	TWINS	Aleš Pospíchal	10051983	úterý 3. dubna 2018 11:12	Celé jméno (CN)	Aleš Pospíchal		
	Kvalifikovaný	Roman Kočí	11234009	neděle 1. dubna 2018 12:	Stát (C)	cz		
	Kvalifikovaný	Roman Kočí	11234010	neděle 1. dubna 2018 12:	Křestní jméno	Aleš		
	TWINS	Aleš Pospíchal	10054061	pátek 6. dubna 2018 8:35	Příjmení (S)	Pospíchal		
	Kvalifikovaný	Roman Kočí	11234014	neděle 1. dubna 2018 12:				
	Komerční	Roman Kočí	11234960	středa 4. dubna 2018 15:	Platnost do	pátek 6. dubna 2018 8:35:27		
					Platnost od	čtvrtek 6. dubna 2017 8:35:27		
					Sériové číslo	10054061 (0x009969AD)		
						Twins		
						Kvalifikovaný certifikát		
					SSCD	Ano		
						Alternativní název předmětu		
					E-mail (RFC822)	pospichal@ica.cz		
					ICA SN	10029075		
					IK MPSV	1234567890		Υ
	<			>	<		>	
		Vyd	dat následný ceri	ifikát Vydat prvotní c	ertifikát	Zobrazit		

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.

۷	/ložení ldentifikačního čísla klienta – získání poplatkových účtů	×
	Výběr typu identifikace:	
	● IČID ○ IPPID	
	ldentifikační číslo:	
	Vložené Identifikační číslo slouží pro vyhledání poplatkových účtů	
	OK Storno	

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.

icara	×
Certifikáty byly SecureStore Wir	úspěšně uloženy. ndows
	ОК

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".

🧊 1. Žádost o certifikát	
Žádost č. LO10001423	
🞸 2. Kontrola žádosti	Ukončení zpracování žádosti LO10001423, LO00003676
父 3. Doplnit údaje	
🞸 4. Rekapitulace	Žádost o následný TWINS kvalifikovaný certifikát LO10001423 (7607910001423) Žádost o následný TWINS komerční certifikát LO00003676 (7607900003676)
5. Tisk protokolu	
6. Odeslat žádost	
💙 7. Čekat na odpověď CA	Zpracovani zadosti o certifikat bylo dokonceno.
🞸 8. Předání certifikátu	
9. Tisk dokumentů	Seznam předávaných dokladů I.CA
🕖 10. Zavřít žádost	Dokumenty pro získání certifikátu
	Zavīt žádost
Číslo žádosti St Jméno ■ L010001422 9 Pospíchal ■ L010001415 5 Test ■ L010001416 9 Test ■ L010001421 7 Novák ■ L010001423 8 Aleš Pospíchal	

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 Nastavení aplikace Certifikát klienta Nápověda

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) <u>Panel nástrojů</u>



- a) <u>Otevřít žádost</u> táž funkce jako Krok 1 v panelu vyřízení žádostí
- b) <u>Uložit žádost, Uložit žádosti</u> 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) <u>Test spojení na servery CA</u> zjistí, zda jsou dostupné servery certifikační autority
- g) Tisk aktuální stránky vytiskne aktuální stránku, ve které se nachází aplikace
- h) <u>Nápověda</u> vstup do nápovědy, jsou zde uloženy informace zobrazované pod otazníky v Kroku 3 - Doplnění údajů
- i) <u>Konec</u> ukončení aplikace

2) <u>Stavový řádek</u>

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

Žádost o následný certifikát služby TWINS	MPSV	NUM
---	------	-----

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.

Číslo žádosti	Stav	Jméno
R 9H10000497	8	Nový
2 9H10000498	8	Novák
9H10000500	9	Kratochvíl

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).

		Odhlásit	Aleš Pospíchal	Vytvořit soubor pro technickou podporu	Kód RA: LO
--	--	----------	----------------	--	------------

<u>Konec</u>

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

3.7.2. Nastavení aplikace

Operátor

nastavem aplikace KA
)perátor
Odhlásit operátora - Aleš Pospíchal
Nový certifikát operátora
Vydání následného certifikátu operátora
Aktualizovat seznam operátorů
Zobrazit seznam operátorů
Informace o čipové kartě operátora
ldržba a ladění aplikace
Vytvořit soubor pro technickou podporu
Seznam používaných certifikátů
Seznam používaných certifikátů Zobrazit číselník chyb

1) <u>Přihlásit operátora, Odhlásit operátora</u> - 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) <u>Aktualizovat seznam operátorů</u> 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)** <u>Zobrazit seznam operátorů</u> 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

Testevet desturnest serveri I CA

- 7) <u>Vytvořit soubor pro technickou podporu</u> 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) <u>Seznam používaných certifikátů</u> zobrazí seznam používaných certifikátů. Tato funkce se využívá při telefonické pomoci hotlineRA operátorovi.
- 9) <u>Zobrazit číselník chyb</u> zobrazí seznam chybových kódů aplikace
- 10) <u>Provést test spojení na servery CA</u> zjistí, zda jsou dostupné servery certifikační autority. Tato funkce se využívá při telefonické pomoci hotlineRA operátorovi.

Stav spojení
V
\mathbf{V}
\mathbf{V}
V
V
V
V
Testovat dostupnost

Sestavy a statistiky

 Sestavy - statistiky Přehled počtů a typů vydaných certifikátů se zobrazuje vždy za jeden kalendář Před prvním zobrazením statistik můžete být vyzván(a) k výběru svého operátor 	ní měsíc. rského certifikátu.
Zvolte období	Duben 🗸 2017 🗸

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

Parametry	
1	Číslo RA LO
2	Umístnění RA (např. Praha). Praha
3 4	Spouštět v maximalizovaném okně 🗹 Ano
_	Soubor pro technickou podporu Poštovní klient 🗸

- <u>Číslo RA</u> je nutno doplnit dvouznakový kód RA, ke kterému je v databázi I.CA přidělen konkrétní certifikát operátora
- 2) <u>Umístění RA</u> doplní se místo, kde je RA umístěna. Toto místo se zobrazí na protokolech a smlouvách vytištěných k vydaným certifikátům

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

4) <u>Soubor pro technickou podporu</u> – 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

Tisk		
1	Výchozí jazyk protokolů	Česky (Czech)
2	Výchozí tiskárna	Výchozí tiskárna Windows 🗸
3	Tisknout přímo	🗌 Ano (při tisku dokumentů nezobrazovat okno s nastavením tisku)
4	Náhled protokolu asociovanou aplikací	Ano (Ne - aplikace wordpad)
	Olaria	Vlevo (mm) 16 Nahoře (mm) 10
	Okraje	Vpravo (mm) 16 Dole (mm) 16

- <u>Výchozí jazyk protokolů</u> lze nastavit, v jakém jazyku se budou tisknout jednotlivé protokoly a smlouvy k vydaným certifikátům. Jazyk protokolů pak lze změnit pro konkrétní certifikát.
- 2) <u>Výchozí tiskárna</u> zde je možno vybrat a nastavit výchozí tiskárnu pro aplikaci RA. Uplatnění najde především u mobilních RA.
- 3) <u>Tisknout přímo</u> při tisku se nezobrazuje dialog tiskárny.
- 4) <u>Náhled protokolu asociovanou aplikací</u> 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

Další funkce	
Nastavit připojení k internetu	
Použít nastavení Internet Exploreru	✓ Ano
Proxy server	
Autentizace proxy serveru	Uživatel Hesio
Autentizace firewall	Uživatel Heslo

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

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

<u>Autentizace firewall</u> - 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.

– Další funkce –	
Nastavit připojení k internetu	
Povolené typy žádostí	
👽 Kvalifikovaný certifikát	🐼 Komerční certifikát
👽 Kvalifikovaný certifikát SR	Technologický (komerční serverový) certifikát
👽 Kvalifikovaný systémový certifikát	💽 Komerční podpisový certifikát pro vydání následného certifikátu
Systémový certifikát	Comerční systémový certifikát služby OCSP
👽 Kvalifikovaný podpisový certifikát pro vydání následného certifikátu	Komerční SSL Domain-validated certifikát
TWINS, Kvalifikovaný certifikát	Komerőní SSL Subject-validated certifikát

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

Menu: Certifikát klienta
Práce s existujícím certifikátem
1 Načíst existující certifikát ze serveru I.CA
2 Zneplatnit certifikát

 <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

Práce s existujícím o	ertifikátem - získat certifikát ze serveru			
Načíst z I.CApod	le jednoho z následujících údajů 🦳 👘			
		Typ certifikátu	Komerční 🗸	
а	Sér	riové číslo certifikátu		*)
b		Číslo žádosti		Např. PH00000017
С	Číslo ž	ádosti (tvar pro DB)		Např. 8007200000017
Načíst		Vyčistit formu	ılář	

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) Číslo žádosti ve tvaru pro DB

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

Práce s existujícím certifikátem č. 35571 (8AF3 hex)
 a) Zobrazit položky certifikátu
 b) Zobrazit certifikát v systémovém dialogu
 c) Uložit na médium
 d) Tisk dodatečných protokolů a smluv

- a) <u>Zobrazení položek certifikátu</u> zobrazení položek předmětu certifikátu, sériového čísla a platnosti
- b) <u>Zobrazit certifikát v systémovém dialogu</u> volba zobrazí certifikát v prostředí Windows
- c) <u>Uložení na médium</u> 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)

Zadat aplikační hodnotu klienta	×
⊂Aplikační identita IPPID nebo OLI není zadána. Zadejte aplikační identitu IPPID I Zadejte aplikační identitu OLI	
Zadejte aplikační identitu IPPID nebo OLI, nebo zadejte obě hodnoty.	
OK Storno	

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)

Osobní údaje klie	enta	Х
– Osobní údaje k	lienta - povinné údaje	
Jméno	[
Příjmení		
– Nepovinné úda	ije	
Titul		
Ulice		
Číslo popisné		
Město		
PSČ		
Kód země	CZ	
Email	pospichal@ica.cz	
Název společi	nosti	
	První certifikační autorita, a.s.	
Číslo plátce		
	OK Storno	

 <u>Tisk dodatečných protokolů a smluv</u> – po volbě typu dotiskovaných dokumentů a kliknutím na tlačítko "Pokračovat", je třeba doplnit požadované údaje dle osobních dokladů držitele certifikátu

Tisk protokolu klienta	
Informace o žadateli	
Titul (před jménem)	
Jméno	Aleš
Příjmení	Pospíchal
Titul (za jménem)	
Adresa	Podvinný mlýn 2178/6. Praha 9
Rodné őslo	
Primární doklad totožnosti ?	Občanský průkaz 🗸
Číslo primárního dokladu totožnosti ?	
Sekundární doklad ?	
Ostatní doklady ?	

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.

Tisk klientských protokolů a smluv					
Formulář		Tisknout	Počet kopii		
Protokol o podání žádosti	1	V	2 🗸		
Smlouva o vydání certifikátu	2	V	2 🗸		
Smlouva o používání certifikátu, příloha MPSV	3	V	1 🗸		
Platební doklad	4		1 🗸		
Protokol o přířazení certifikátu I.CA ke službám ELB ČSOB	5		2 🗸		
Pokračovat Přednastavit		Vyčistit			

Jsou k dispozici tisky těchto protokolů:

- 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

Náp	ověda						
	Uživat	elská příručka					
	Nápov	/ěda aplikace					
	O aplikaci						

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.

Užitečné odkazy				
www.ica.cz	RA info	<u>Certifikační politiky</u>	Seznam veřejných certifikátů	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:

			0	R	G	A		9	0	0			
	I	N	G	E	N	Ι	С	0	-	С	Z		

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

С	а	r	d		ΡI	Ν	•				
*	*	*	*	*	*	*					

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	0	s	3	•	0			

Při vložení nepodporované karty je na displeji zobrazena zpráva:

N	J	e	Z	n	a	m	a	K	a	r	t	a		
١	/	у	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 <u>hotlinera@ica.cz</u>, případně zhotovit soubor pro technickou podporu pro urychlení identifikace problému (viz. menu Nastavení aplikace/Vytvořit soubor pro technickou podporu).