Dodatek č. 4
Smlouvy o provozu mobilních registračních autorit MPSV pro vydávání kvalifikovaných certifikátů a o poskytování služeb I.CA

První certifikační autorita, a.s.
Se sídlem: Praha 9, Podvinný mlýn 2178/6, PSČ 190 00,
zastoupená: [redacted] předsedou představenstva
[redacted] členem představenstva
IČ: 264 39 395
DIČ: CZ264 39 395
Bankovní spojení: účet číslo 168457418/0300 vedený u ČSOB, a.s
Zapsaná v obchodním rejstříku, vedeném Městským soudem v Praze, spisová značka B 7136.

(dále jen „I.CA")

a

Česká republika - Ministerstvo práce a sociálních věcí
se sídlem: Praha 2, Na Poříčním právu 1, PSČ 128 01
zastoupená: [redacted] ředitelem odboru informačních a komunikačních technologií
IČ: 00551023
Bankovní spojení: Česká národní banka, č. účtu 2229001/0710

(dále jen „MPSV")

uzavírají níže uvedeného dne, měsíce a roku tento dodatek č. 4 (dále též dodatek) Smlouvy o provozu mobilních registračních autorit MPSV pro vydávání kvalifikovaných certifikátů a o poskytování služeb I.CA.

Preambule

Smluvní strany vycházejí ze Smlouvy o provozu mobilních registračních autorit MPSV pro vydávání kvalifikovaných certifikátů a o poskytování služeb I.CA uzavřené dne 20.6.2007, z jejího Dodatku č. 1 uzavřeného dne 8.10.2009, kterým bylo rozšířeno vydávání certifikátů o komerční certifikáty, Dodatku č. 2 uzavřeného dne 23.2.2011, kterým bylo rozšířeno vydávání kvalifikovaných a komerčních certifikátů pro potřeby České správy sociálního zabezpečení v souladu s podmínkami veřejné zakázky vypsané v roce 2007 MPSV pod evidenčním číslem 60005947 a Dodatku č. 3 uzavřeného dne 23.3.2011, kterým byla v návaznosti na zřízení Úřadu práce ČR uskutečněna změna naplnění položek „O" a „OU" v kvalifikovaných a komerčních certifikátech vydávaných pro zaměstnance Úřadu práce ČR.

Předmětem tohoto dodatku č. 4 (dále jen „dodatku") je doplnění možnosti vydávaných kvalifikovaných certifikátů o kvalifikované systémové certifikáty a komerčních certifikátů o

komerční serverové certifikáty včetně možnosti plně elektronického vydání a možnost změny e-mailové adresy při vydání následného certifikátu.

I.
Účel dodatku smlouvy

1. Účelem dodatku smlouvy je doplnění možnosti vydávaných kvalifikovaných certifikátů o kvalifikované systémové certifikáty a komerčních certifikátů o komerční serverové certifikáty elektronickou cestou a možnost změny e-mailové adresy při vydání následného certifikátu

II.
Předmět dodatku smlouvy

1. Provozování služeb registrační autority se řídí platnými ustanoveními Certifikační politiky I.CA pro kvalifikované systémové certifikáty (CPQSC) a platnou Provozní směrnicí pro pracovníky Registračních autorit I.CA pro vydávání kvalifikovaných certifikátů a kvalifikovaných systémových certifikátů (PSQRA), které tvoří přílohu č. 5 tohoto dodatku; a dále se řídí platnými ustanoveními Certifikační politiky I.CA pro komerční a komerční serverové certifikáty (CPKC) a platnou Provozní směrnicí pro pracovníky Registračních autorit I.CA pro vydávání komerčních a komerčních serverových certifikátů (PSKRA), které tvoří přílohu č. 6 tohoto dodatku.
2. Žádosti o kvalifikované systémové certifikáty, vydávané podle tohoto dodatku, musí splňovat podmínky stanovené zákonem č. 227/2000 Sb., o elektronickém podpisu, ve znění pozdějších předpisů (dále jen „zákon o elektronickém podpisu") a CPQSC. Pro vydání kvalifikovaného systémového certifikátu je třeba předložit dokumenty uvedené v přílohách č.1 a č.2 tohoto dodatku, tj. Plnou moc a Potvrzení o zaměstnaneckém poměru.
3. Žádosti o komerční certifikáty pro servery, vydávané podle tohoto dodatku, musí splňovat podmínky stanovené CPKC. Pro vydání komerčního serverového certifikátu je třeba předložit dokumenty uvedené v přílohách č.1, č.3 a č.4 tohoto dodatku, tj. Plnou moc, Potvrzení o zaměstnaneckém poměru a Čestné prohlášení o vlastnictví serveru.
4. Vydávání kvalifikovaných systémových certifikátů a komerčních serverových certifikátů bude upraveno tak, aby veškeré dokumenty nutné pro vydání certifikátů existovaly pouze v elektronické formě. Konkrétní popis je uveden v příloze č.7 tohoto dodatku.
5. Změna e-mailové adresy při vydání následného certifikátu bude umožněna u všech typů certifikátů, tj. kvalifikovaného a kvalifikovaného systémového, komerčního a komerčního serverového. Generátor následných certifikátů bude upraven tak, aby žadatel o následný certifikát měl možnost vyplnit novou e-mailovou adresu či ponechat původní. Konkrétní popis je uveden v příloze č.8 tohoto dodatku.

III.
Práva a povinnosti MPSV

1) MPSV se zavazuje při provozu Registrační autority dodržovat platnou CPQSC a PSQRA, které jsou uvedeny v příloze č.5 tohoto dodatku, a platnou CPKC a PSKRA, které jsou uvedeny v příloze č.6 tohoto dodatku. Za škody vzniklé v souvislosti s jejím nedodržením, zejména s vyzrazením a zneužitím soukromého klíče žadatele o certifikát, nese plnou a výlučnou odpovědnost MPSV.

2) Veškeré změny CPQSC a CPKC, uvedené v bodě 1. Článku II. tohoto dodatku, zaslané I.CA na e-mailovou adresu [redacted] jsou vůči MPSV účinné okamžikem potvrzení ze strany MPSV, které učiní do 3 pracovních dnů od předání. Pokud MPSV nebude se změnou CPQSC a CPKC souhlasit, oznámí tuto skutečnost ve lhůtě 3 pracovních dnů od předání I.CA a je oprávněna smlouvu vypovědět. Výpovědní doba v tomto případě činí 15 dnů a začíná běžet dnem následujícím po dni, ve kterém bylo I.CA oznámeno, že MPSV se změnou CPQSC a CPKC nesouhlasí.

IV.
Práva a povinnosti I.CA

1) I.CA nebude akceptovat žádosti zaměstnanců MPSV podané z Registrační autority směrem k I.CA, které nebudou splňovat naplnění položek žádosti o kvalifikovaný systémový certifikát a žádosti o komerční certifikát pro servery podle podmínek tohoto dodatku.
2) I.CA se zavazuje realizovat elektronizaci vydávání kvalifikovaných systémových a komerčních serverových certifikátů nejpozději do 2 měsíců od podpisu tohoto dodatku.
3) I.CA se zavazuje realizovat změnu e-mailové adresy při vydání následného certifikátu nejpozději do 1 měsíce od podpisu tohoto dodatku.

V.
Cenové podmínky

1) Cena za vydání jednoho prvotního kvalifikovaného systémového certifikátu na dobu platnosti 1 roku splňujícího naplnění položek elektronické žádosti o vydání kvalifikovaného certifikátu pro MPSV činí:

530,- Kč bez DPH + DPH v aktuální zákonné výši, jež k datu podpisu tohoto dodatku činí 21%; cena s DPH k datu podpisu tohoto dodatku tak činí **641,30** Kč.

2) Cena za vydání jednoho následného kvalifikovaného systémového certifikátu splňujícího naplnění položek elektronické žádosti o vydání kvalifikovaného certifikátu s platností 1 rok pro MPSV činí:

530,- Kč bez DPH + DPH v aktuální zákonné výši, jež k datu podpisu tohoto dodatku činí 21%; cena s DPH k datu podpisu tohoto dodatku tak činí **641,30** Kč.

3) Cena za vydání jednoho prvotního komerčního certifikátu pro server na dobu platnosti 1 roku splňujícího naplnění položek elektronické žádosti o vydání komerčního certifikátu pro MPSV činí:

570,- Kč bez DPH + DPH v aktuální zákonné výši, jež k datu podpisu této Smlouvy činí 21%; cena s DPH k datu podpisu tohoto dodatku tak činí **689,70** Kč.

4) Cena za vydání jednoho následného komerčního certifikátu pro server splňujícího naplnění položek elektronické žádosti o vydání komerčního certifikátu s platností 1 rok pro MPSV činí:

570,- Kč bez DPH + DPH v aktuální zákonné výši, jež k datu podpisu této Smlouvy činí 21%; cena s DPH k datu podpisu tohoto dodatku tak činí **689,70** Kč.

5) Cena za realizaci elektronizace vydávání kvalifikovaných systémových a komerčních serverových certifikátů činí 753.650,- Kč bez DPH, tj. 911.916,50 Kč s DPH ve výši 21%.
6) Cena za realizaci změny e-mailové adresy při vydání následného certifikátu činí 328.700,- Kč bez DPH, tj. 397.727,- Kč s DPH ve výši 21%.
7) Ceny uvedené v odst. 5) a 6) tohoto dodatku budou splatné po vystavení předávacího protokolu podepsaného oprávněnými zástupci obou smluvních stran osvědčujícího úspěšnou realizaci.

VI.
Závěrečná ustanovení

1. Tento dodatek smlouvy nabývá platnosti a účinnosti dnem podpisu oběma smluvními stranami. Dodatek smlouvy se uzavírá na dobu neurčitou.
2. Dodatek smlouvy je vyhotoven ve čtyřech vyhotoveních v českém jazyce s platností originálu, z nichž dvě vyhotovení obdrží I.CA a dvě vyhotovení obdrží MPSV.
3. Seznam příloh, které tvoří nedílnou součást tohoto dodatku smlouvy:

1.Příloha č.1 – Plná moc
2.Příloha č.2 – Potvrzení o zaměstnaneckém poměru pro kvalifikované systémové certifikáty
3.Příloha č.3 – Potvrzení o zaměstnaneckém poměru pro komerční serverové certifikáty
4.Příloha č.4 – Čestné prohlášení o vlastnictví serveru
5.Příloha č.5 – CPQSC a PSQRA
6.Příloha č.6 – CPKC a PSKRA
7.Příloha č.7 – popis elektronizace vydávání kvalifikovaných systémových a komerčních serverových certifikátů
8.Příloha č.8 – popis změny e-mailové adresy při obnově.

V Praze dne .....

[redacted]

předseda představenstva

[redacted]

člen představenstva

CERTIFICATION AUTHORITY
První certifikační autorita, a.s.
Podvinný mlýn 2178/6, 190 00 Praha 9
IČ: 26439395
880

V Praze dne 05.-12-2013

[redacted]

ředitel odboru informačních a komunikačních technologií

MINISTERSTVO PRÁCE A SOCIÁLNÍCH VĚCÍ ČESKÉ REPUBLIKY Na Poříčním právu

[redacted]

Příloha č. 1

Plná moc

Zmocnitel

Název:	**Česká republika – Ministerstvo práce a sociálních věcí**
Adresa:	**Na Poříčním právu 1, 12801 Praha 2**
IČ:	**00551023**

Zmocněnec

Jméno a příjmení: za útvar: Adresa trvalého bydliště:	Datum narození: ..... Rodné číslo:	Podpis zmocněnce:

Zmocnitel tímto uděluje plnou moc výše uvedenému zmocněnci k vyřizování žádostí o kvalifikovaný a komerční zaměstnanecký certifikát a kvalifikovaný systémový a komerční serverový certifikát na registrační autoritě I.CA v rozsahu:

- samostatné jednání - podpis formuláře „Potvrzení o zaměstnaneckém poměru" zaměstnancům ZMOCNITELE

V Praze dne: .....

.....
Oprávněná osoba

Tuto plnou moc přijímám

V Praze dne: .....

.....
zmocněnec

Příloha č. 2

Potvrzení o zaměstnaneckém poměru

Tímto potvrzujeme, že pan/paní

.....,

R.Č. ..... bytem .....

Č. OP .....

je k dnešnímu dni naším zaměstnancem.

Název: Česká republika – Ministerstvo práce a sociálních věcí
Adresa: Na Poříčním právu 1, 12801 Praha 2
IČ: 00551023

Souhlasíme s tím, aby mu/jí byl společností První certifikační autorita, a.s. vydán kvalifikovaný systémový certifikát s uvedením názvu našeho úřadu.

V položce „Zařízení" žádosti o kvalifikovaný systémový certifikát bude uvedeno:

Zařízení = ...

V položce „O" žádosti o kvalifikovaný systémový certifikát bude uvedeno:

O = ...

V položce „OU" žádosti o kvalifikovaný systémový certifikát bude uvedeno:

OU =.....

V položce „T" žádosti o kvalifikovaný systémový certifikát bude uvedeno:

T = ...

V .....dne .....

.....
jméno a funkce
oprávněné osoby k jednání za
Českou republiku – Ministerstvo práce
a sociálních věcí

.....
podpis zaměstnance

Příloha č. 3

Potvrzení o zaměstnaneckém poměru

Tímto potvrzujeme, že pan/paní

.....,

R.Č. ..... bytem .....

Č. OP .....

je k dnešnímu dni naším zaměstnancem.

Název:	Česká republika – Ministerstvo práce a sociálních věcí
Adresa:	Na Poříčním právu 1, 12801 Praha 2
IČ:	00551023

Souhlasíme s tím, aby mu/jí byl společností První certifikační autorita, a.s. vydán komerční serverový certifikát s uvedením názvu našeho úřadu.

V položce „Název" žádosti o komerční serverový certifikát bude uvedeno:

Název = ...

V položce „O" žádosti o komerční serverový certifikát bude uvedeno:

O = ...

V položce „OU" žádosti o komerční serverový certifikát bude uvedeno:

OU =.....

V .....dne .....

.....	.....
jméno a funkce oprávněné osoby k jednání za Českou republiku – Ministerstvo práce a sociálních věcí	podpis zaměstnance

Příloha č. 4

Čestné prohlášení o vlastnictví serveru

Název:	**Česká republika – Ministerstvo práce a sociálních věcí**
Adresa:	**Na Poříčním právu 1, 12801 Praha 2**
IČ:	**00551023**

Já, níže podepsaný, jménem České republiky – Ministerstva práce a sociálních věcí,

čestně prohlašuji,

že server .....

je ve vlastnictví České republiky – Ministerstva práce a sociálních věcí.

Toto čestné prohlášení slouží pro vydání komerčního serverového certifikátu I.CA.

V Praze dne .....

.....
Podpis oprávněné osoby
Česká republika – Ministerstvo práce a sociálních věcí

Příloha č. 5

CPQSC

(Certifikační politika I.CA pro kvalifikované systémové certifikáty)

aktuální verze – viz:

www.ica.cz

PSQRA

(Provozní směrnice pro pracovníky registračních autorit I.CA pro vydávání kvalifikovaných certifikátů)

aktuální verze – viz:

https://rainfo.ica.cz

Příloha č.6

CPKC

(Certifikační politika I.CA pro komerční certifikáty)

aktuální verze – viz:

www.ica.cz

PSKRA

(Provozní směrnice pro pracovníky registračních autorit I.CA pro vydávání komerčních certifikátů)

aktuální verze – viz:

https://rainfo.ica.cz

Příloha č.7

Elektronizace vydávání kvalifikovaných systémových a komerčních serverových certifikátů

Úvod pro problematiky – právní hledisko

Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů (dále jen „ZoEP“) stanoví v § 6 odst. 1) písm. f) a odst. 4):

„f) před uzavřením smlouvy o poskytování kvalifikovaných certifikačních služeb s osobou, která žádá o poskytování služeb podle tohoto zákona, informovat tuto osobu **písemně** o přesných podmínkách pro využívání kvalifikovaných certifikačních služeb, včetně případných omezení pro jejich použití, o podmínkách reklamací a řešení vzniklých sporů a o tom, zda je, či není akreditován Ministerstvem vnitra (dále jen "ministerstvo") podle § 10; tyto informace lze předat elektronicky.“.

„(4) Kvalifikovaný poskytovatel certifikačních služeb poskytuje služby podle tohoto zákona na základě smlouvy. **Smlouva musí být písemná**.“.

Konkrétně v případě I.CA jde o dokumenty podepsané žadatelem o certifikát a operátorem Registrační autority zmocněným zastupovat I.CA:

- Protokol o podání žádosti o certifikát
- Smlouva o vydání a používání certifikátu (dále jen „dokumenty“).

O písemné formě hovoří občanský zákoník:
§ 40 zákona č. 40/1964 Sb., občanský zákoník:

(4) Písemná forma je zachována, je-li právní úkon učiněn telegraficky, dálnopisem nebo elektronickými prostředky, jež umožňují zachycení obsahu právního úkonu a určení osoby, která právní úkon učinila.

Nový občanský zákoník (č. 89/2012 Sb.) účinný od 1. 1. 2014 definuje totéž v § 562:

(1) Písemná forma je zachována i při právním jednání učiněném elektronickými nebo jinými technickými prostředky umožňujícími zachycení jeho obsahu a určení jednající osoby.

(2) Má se za to, že záznamy údajů o právních jednáních v elektronickém systému jsou spolehlivé, provádějí-li se systematicky a posloupně a jsou-li chráněny proti změnám. Byl-li záznam pořízen při provozu závodu a dovolá-li se jej druhá strana k svému prospěchu, má se za to, že záznam je spolehlivý.

Z veřejně dostupných zdrojů (http://www.itpravo.cz/index.shtml?x=62154) vyplývá:

„Písemná forma právního úkonu předpokládá existenci dvou náležitostí: písemnosti a podpisu. Písemnost spočívá v tom, že obsah právního úkonu je zachycen v textu listiny. Písemný projev musí být zároveň podepsán; činí-li právní úkon více osob, nemusí být jejich podpisy na téže listině, ledaže právní předpis stanoví jinak. Písemná forma je podle § 40 odst. 4 ObčZ (č. 40/1964 Sb.) zachována, je-li právní úkon učiněn telegraficky, dálnopisem nebo elektronickými prostředky, jež umožňují zachycení obsahu právního úkonu a určení osoby, která právní úkon učinila.“
A dále (http://www.epravo.cz/top/clanky/listinna-a-elektronicka-podoba-pisemneho-pravniho-ukonu-84178.html) :
„Závěrem lze konstatovat, že právní úkon opatřený zaručeným elektronickým podpisem je třeba z hlediska podpisu vnímat jako perfektní, a to přesto, že z teoretického a faktického hlediska vykazuje odlišné znaky od vlastnoručního podpisu.“

Z výše uvedeného lze dovodit, že forma písemného úkonu – podpisu dokumentů - může být nahrazena elektronickou formou při zachování veškerých právních účinků.

Proto lze elektronickou formou podepsat pouze dokumenty potřebné pro vydání certifikátu tehdy, pokud je k podpisu použit elektronický podpis založený na kvalifikovaném certifikátu vydaným akreditovaným poskytovatelem certifikačních služeb, který je platný před okamžikem podpisu dokumentů.

Závěrem lze tedy konstatovat, že nic nebrání plné elektronizaci procesu vydání kvalifikovaných systémových a komerčních serverových certifikátů v prostředí resortu MPSV.

Návrh technického řešení

Nutné předpoklady:

- Žadatel o kvalifikovaný systémový či komerční serverový certifikát musí vlastnit kvalifikovaný osobní certifikát (jako součást TWINS) platný v době podání žádosti o kvalifikovaný systémový či komerční serverový certifikát na registrační autoritě.
- Tento certifikát musí mít uložen na čipové kartě Starcos 3.0 ve formě klasické čipové karty.
- Operátor registrační autority musí vlastnit kvalifikovaný certifikát (jako součást TWINS), kterým bude podepisovat dokumenty nutné pro vydání certifikátu. TWINS bude mít uložen na operátorské čipové kartě (operátorský autentizační certifikát /jako součást TWINS/ bude sloužit stejně jako nyní pro autentizaci operátora k ICARA.
- Pro přístup k Portálu ICA musí žadatel vlastnit komerční certifikát (jako součást TWINS). Ten musí vlastnit ještě před zahájením procesu vydávání certifikátu.
- Pracoviště RA bude dovybaveno externí čtečkou.

Postup:

- Žadatel o kvalifikovaný systémový či komerční serverový certifikát (dále jen „certifikát“) se dostaví na Mobilní registrační autoritu MPSV oprávněnou vydávat certifikáty pro resort MPSV.
- Na RA se dostaví s vygenerovanou žádostí o certifikát, resp s ID, pod kterým je žádost uložena na serveru I.CA, a potřebnými dokumenty vyhotovenými buď v papírové či v elektronické podobě ve formátu PDF, JPEG nebo PNG (uloženými např. na přenosném USB nosiči). Výjimkou jsou osobní doklady (OP, řidičský průkaz apod.), jež žadatel musí mít fyzicky s sebou.
- Potřebné dokumenty:
    - Pro kvalifikovaný systémový certifikát
        - OP + např. ŘP žadatele
        - Plná moc právnické osoby k zastupování MPSV
        - Potvrzení o zaměstnaneckém poměru
    - Pro komerční serverový certifikát
        - OP žádající osoby
        - Plná moc právnické osoby k zastupování MPSV
        - Prohlášení o vlastnictví serveru
        - Potvrzení o zaměstnaneckém poměru
- Potřebné dokumenty mohou být přineseny na USB nosiči, zaslány na pracoviště RA mailem nebo na místě naskenovány pracovníkem RA. Skenování a získání dokumentů z emailu není dodávanou funkčností. ICARA soubory získá z file systému.
- Operátor RA přijme a zkontroluje žádost o certifikát.
- Operátor RA načte a zobrazí si dokumenty z žadatelova USB nosiče nebo provede naskenování papírových dokladů do jednoho z povolených formátů. Dokumenty podepíše svým kvalifikovaným certifikátem uloženým na čipové kartě. ICARA bude akceptovat elektronické dokumenty ve formátech PDF, JPEG nebo PNG. Povolené velikosti jsou uvedeny níže.
- ICARA bude kontrolovat, že operátor zobrazil veškeré potřebné dokumenty a jsou připravené k odeslání do úložiště.
- Na ICARA bude vygenerován Protokol a podání žádosti o certifikát.

- Žadateli zobrazí na monitoru text Protokolu o podání žádosti o certifikát. Pokud žadatel souhlasí, použije svůj kvalifikovaný osobní certifikát (součást TWINS) uložený na čipové kartě a podepíše Protokol. Protokol podepíše následně i operátor. K podpisu se využije systém distribuovaného podpisu.
- Dokumenty v elektronické podobě se vloží do datového úložiště ICA. K potřebným dokumentům se nebude vydávat časové razítko.
- Protokol o podání žádosti o certifikát se vloží do datového úložiště ICA. Zde se provede kontrola podpisů PDF a ověří typ certifikátu a platnost (přes OSCP). Bez ověření a uložení nebude možné dál v procesu pokračovat.
- Operátor pokračuje ve zpracování.
- ICARA vygeneruje Smlouvu o vydání a používání certifikátu.
- Operátor vydá certifikát a podle volby žadatele mu jej uloží na přenosné médium.
- Žadateli se na monitoru zobrazí text Smlouvy o vydání a používání certifikátu. Pokud žadatel souhlasí, použije svůj kvalifikovaný osobní certifikát uložený na čipové kartě a podepíše ji. Smlouvu podepíše následně i operátor. K podpisu se využije distribuovaný podpis.
- Smlouva se vloží do datového úložiště ICA.
- Pokud má žadatel přenosné médium, tak se mu na něj uloží podepsané:
    - Protokol o podání žádosti o certifikát
    - Smlouva o vydání a používání certifikátu
- Úložiště ICA automaticky vygeneruje e-mailovou zprávu s linkem, na kterém je možné se přihlásit do Portálu a zde získat uložené dokumenty:
    - žadatel bude mít možnost získat dokumenty
        - Protokol o podání žádosti o certifikát
        - Smlouva o vydání a používání certifikátu
    - administrátor MPSV bude mít možnost prohlédnout a získat stejné dokumenty, tj. Protokol o podání žádosti o certifikát a Smlouvu o vydání a používání certifikátu náležející žadatelům/zaměstnancům MPSV
- Při stažení souboru bude vyžadováno zadat text z captcha
- Výsledkem postupu tedy je:
    - Na straně žadatele/držitele certifikátu:
        - Vydaný certifikát
        - Dokumenty v elektronické podobě, jež si může uložit na svém PC
    - Na straně operátora/I.CA:
        - Veškeré dokumenty uložené k danému číslu žádosti v elektronické podobě.
        - Protokol o podání žádosti o certifikát a Smlouva o vydání a používání certifikátu podepsané oběma stranami a opatřené časovým razítkem.
        - Tyto dokumenty budou následně před vypršením platnosti elektronické značky, kterým je časové razítko podepsáno, přepodepsány (PAdES-LTV v případě dokumentů vytvořených I.CA.

Dokumenty budou do úložiště přijímány v povolených formátech a kontrolovaných velikostech. Pokud žadatel přinese dokumenty v jiném formátu nebo větší než povolená kontrolovaná velikost, operátor RA provede jejich konverzi nebo nově naskenuje při doporučeném nastavení skeneru.

Typ dokumentu	Doporučený formát	Doporučená nastavení skeneru	Průměrná velikost	Povolená velikost
Plná moc právnické osoby k zastupování MPSV	PDF	150 DPI Stupně šedi A4	150KB/stránka	200KB/stránka
Prohlášení o vlastnictví serveru	PDF	150 DPI Stupně šedi A4	150KB/stránka	200KB/stránka
Potvrzení o	PDF	150 DPI Stupně šedi	150KB/stránka	200KB/stránka

zaměstnaneckém poměru		A4		
Občanský průkaz/řidičský průkaz	JPEG	150 DPI Stupně šedi Automatická velikost	75KB/stránku	100KB/stránku

Rozpad ceny

Činnost	**Odhadovaná pracnost (člověkoměsíce)**	**Cena Kč bez DPH**	**Cena Kč s DPH**
Vývojová analýza	2	180.000	217.800
Příprava vývojového prostředí (server, databáze) pro úložiště	0,25	19.250	23.292,50
Návrh struktury databáze úložiště	0,20	15.400	18.634
Funkčnost aplikace úložiště	0,75	57.750	69.877,50
Podpis PAdES	1,25	96.250	116.462,50
Přepodepisování dokumentů - automatické procesy	0,75	57.750	69.877,50
Podpora pro vydávání QSC, KSC na základě podpisu QC v systému I.CA	0,75	57.750	69.877,50
Integrace skenování, označování dokumentů	1,5	115.500	139.755
ICARA – plugin pro práci s úložištěm	0,5	38.500	46.585
ICARA – podpis PDF	0,5	38.500	46.585
Testování	0,5	38.500	46.585
Dokumentace	0,5	38.500	46.585
Celkem	**9,45**	**753.650**	**911.916,50**

Příloha č.8

Změna e-mailové adresy při obnově

Úvod pro problematiky – právní hledisko

Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů (dále jen „ZoEP") nezná pojem „následný"[1] certifikát.

Pravidla vydávání následného certifikátu upravuje v souladu se ZoEP Certifikační politika I.CA, a to pro všechny typy certifikátů.
V předmětném případě jde především o kvalifikované osobní certifikáty zaměstnanců resortu MPSV (tj. ministerstva, Úřadu práce ČR, SUIP a ČSSZ).

Proces vydání následného certifikátu s umístěním e-mailové adresy je popsán v kapitole 3.1.1.16 Certifikační politiky pro vydávání kvalifikovaných certifikátů verze 3.1 (dále jen „CPQC I.CA"), jež je k dispozici na http://www.ica.cz/Certifikacni-politika.

Podle dikce CP je nutné před vydáním prvotního certifikátu ze strany žadatele hodnověrně doložit vlastnictví e-mailové adresy nebo čestné prohlášení o vlastnictví ve formě podpisu pravdivosti údajů ve Smlouvě o vydání a používání certifikátu (článek I. odst. 7. – „Podpisem této smlouvy žadatel potvrzuje správnost a úplnost údajů Žádosti uvedených v Protokolu o podání žádosti na vydání kvalifikovaného certifikátu I.CA, který tvoří nedílnou součást této smlouvy.").
Odst. 5. Čl. I. Smlouvy o vydání a používání certifikátu stanoví, cituji „Před ukončením platnosti prvního i každého následného QC vydaného na základě této smlouvy bude žadatel upozorněn na možnost požádat o vydání následného QC v souladu s CPQC I.CA. Pokud tak učiní, vztahuje se tato smlouva i na všechny vydané následné QC.".

Technicky není možné, aby operátor registrační autority ověřil platnost e-mailové adresy a její příslušnost k žadateli. Je nutné ponechat doložení e-mailové adresy na žadateli, či v případě následného certifikátu na držiteli certifikátu předchozího, kterým žadatel o následný certifikát podepisuje žádost o vydání následného certifikátu.
Správnost údajů v certifikátu uvedených, tedy i stávající či nové/změněné e-mailové adresy, potvrzuje žadatel podpisem Smlouvy o vydání a používání certifikátu.
Vydání následného certifikátu i se změněnou e-mailovou adresou je tedy kryto Smlouvou o vydání a používání certifikátu.

Je tedy možné umožnit žadateli o následný certifikát změnit e-mailovou adresu v následném certifikátu.

Výchozí premisy:

1. E-mailová adresa musí být v souladu s RFC5280 umístěna pouze v položce SAN.rfc822Name certifikátu. Tato položka je naplňována počínaje 11.4.2011; pokud v předchozím certifikátu byla e-mailová adresa uvedena v položce emailAddress, je přesunuta do položky SAN.rfc822Name. Z toho plyne, že změna e-mailové adresy při obnově certifikátu je možná po 12.4.2012, kdy všechny obnovené certifikáty budou mít e-mailovou adresu v položce SAN.rfc822Name.

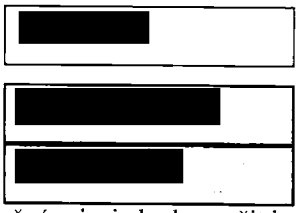
[1] Používá se též pojem „obnova" certifikátu, správnější je však používat pojem „následný" certifikát; pojem „obnova" implikuje u neodborníků možnost prodloužení platnosti původního certifikátu, což je mylná představa. Následný certifikát znamená, že se generuje zcela nový pár klíčů a vydává nový certifikát, pouze se stejným naplněním položek.

2. V této položce může být umístěno více e-mailových adres, změna bude povolena pouze u první e-mailové adresy, kterou používají Windows. Ostatní e-mailové adresy bude možné pouze smazat, nikoli editovat.

Návrh technického řešení

I.CA umožní změnu e-mailové adresy při vydání následných certifikátů takto:

- v on-line generátoru následného certifikátu pod oknem změny hesla přibude okno/okna (v případě více e-mailových adres), kam bude umístěn (překopírován) obsah položky z SAN.rfc822Name původního certifikátu (bude zobrazeno tolik oken, kolik e-mailových adres v položce SAN.rfc822Name je uvedeno
- první okno bude editovatelné a bude obsahovat první e-mailovou adresu z položky SAN.rfc822Name původního certifikátu
- ostatní okna budou needitovatelná (zašedlá) a budou obsahovat další e-mailové adresy z položky SAN.rfc822Name původního certifikátu (pokud byly uvedeny); vedle těchto needitovatelných oken bude zaškrtávací box „Smazat" s možností smazat adresu
- ICA umožní změnu pouze první e-mailové adresy uvedené v SAN.rfc822Name
- pokud žadatel e-mailovou adresu změní, bude tato nová e-mailová adresa umístěna v SAN.rfc822Name následného certifikátu (na prvním místě) a původní e-mailová adresa nebude použita
- pokud žadatel e-mailovou adresu nezmění, bude použita tato první e-mailová adresa umístěná v SAN.rfc822Name původního certifikátu (ostatní, pokud je žadatel neoznačil pro smazání, zůstanou)
- v případě TWINS certifikátů budou použita stejná pravidla při umístění e-mailové adresy do SAN.rfc822Name obou certifikátů.



Pokud si přejete změnit e-mailovou adresu, můžete tak učinit vyplněním tohoto pole. Pokud ji nezměníte, bude použita tato e-mailová adresa uvedená v původním certifikátu

☐ Smazat

☐ Smazat

Totožný princip bude použit i v off-line aplikaci ICANewCert.
V konkrétním případě resortu MPSV to znamená, že vydání nových/prvotních kvalifikovaných certifikátů, navazující na změnu doménové struktury, jež si vyžádá změnu e-mailových adres, nebude nutné řešit, změnu bude možné realizovat plně elektronicky pouhým vydáním následného certifikátu s uvedením nové e-mailové adresy.
Např. současná adresa [redacted] se změní na [redacted]

Protože se jedná o cca 7.500 držitelů kvalifikovaných certifikátů, které by bylo nutné vydat znovu jako prvotní a projít přitom procesem vydání na Veřejné registrační autoritě I.CA či na Mobilní registrační autoritě MPSV či jiné registrační autoritě oprávněné vydávat certifikáty pro resort MPSV, jedná se využitím změny e-mailové adresy v následném certifikátu o výraznou úsporu času, administrativy spojené s vydáním prvotního certifikátu, a v neposlední řadě finančních prostředků.

Rozpad ceny:

Činnost	**Odhadovaná pracnost (člověkoměsíce)**	**Cena Kč bez DPH**	**Cena Kč s DPH**
Vývojová analýza	1	90.000	108.900
Návrh změny CA	1	77.000	93.170
Úprava on-line generátoru následného certifikátu	0,5	38.500	46.585
Komunikace s BICa	0,4	30.800	37.268
Úprava off-line aplikace ICANewCert	0.5	38.500	46.585
Testování	0,5	38.500	46.585
Dokumentace	0,2	15.400	18.634
Celkem	**4,1**	**328.700**	**397.727**