

č. 120120001/07

Dodatek č. 1

k Ujednání o zřízení a provozu mobilních registračních autorit ČSSZ pro vydávání kvalifikovaných a komerčních certifikátů a o poskytování služeb I.CA a zapůjčení potřebného HW a SW vybavení ze dne 6. 1. 2012

(dále jen „Dodatek“)

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: CZ26439395
Bankovní spojení: Československá obchodní banka, a.s.
Číslo účtu: [redacted]
zapsaná v obchodním rejstříku, vedeném Městským soudem v Praze, spisová značka B,
vložka 7136.

(dále též „I.CA“)

a

Česká republika - Česká správa sociálního zabezpečení

Se sídlem: Praha 5, Křížová 25, PSČ 225 08
Zastoupená: JUDr. Jiřím Biskupem, ústředním ředitelem
IČ: 00006963
DIČ: neplátce
Bankovní spojení: Česká národní banka
Číslo účtu: [redacted]

(dále též „ČSSZ“)

(dále jednotlivě také jako „Strana“ a společně také jako „Strany“)

uzavírají níže uvedeného dne, měsíce a roku tento Dodatek k Ujednání o zřízení a provozu mobilních registračních autorit ČSSZ pro vydávání kvalifikovaných a komerčních certifikátů a o poskytování služeb I.CA a zapůjčení potřebného HW a SW vybavení uzavřeného mezi Stranami dne 6. 1. 2012 (dále jen „Ujednání“).

Preamble

Obě Strany podpisem tohoto Dodatku upřesňují Ujednání o technické podmínky procesu vydávání a kontrol položek podtypu komerčních certifikátů, tzv. **SSL** (Secure Socket Layer) **certifikátů** tak, jak je níže v tomto Dodatku uvedeno.

I.

1. Strany se dohodly na tom, že za dosavadní článek VII. Ujednání se vkládá nový článek VIII. s názvem **Podmínky vydávání SSL certifikátů**, který zní takto:

„VIII.

Podmínky vydávání SSL certifikátů

- 1) SSL (Secure Socket Layer) certifikáty (dále jen „SSL certifikáty“) budou vydávány v souladu s Certifikační politikou pro SSL certifikáty (dále jen "CP SSL"), která je uvedena v příloze č. 8 tohoto ujednání, a která je vždy dostupná v aktuálním znění na www.ica.cz.
- 2) SSL certifikáty jsou dvojího typu:
 - a) tzv. Domain validated SSL certifikát (dále jen "DV") obsahující v příslušných položkách plně kvalifikovaná doménová jména.
 - b) tzv. Organization validated SSL certifikát (dále jen "OV") obsahující navíc informace o organizaci, které je certifikát vydáván.
- 3) Uvedené SSL certifikáty podle podmínek tohoto ujednání budou vydávány na základě elektronické žádosti o SSL certifikáty, která musí být předem zaslána na e-mailovou adresu [REDACTED] a která musí dále splňovat níže popsané a definované požadavky dle CP SSL. Elektronická žádost musí být prokazatelně odeslána ve formě přílohy e-mailové zprávy zmocněnou osobou na straně ČSSZ uvedenou v Potvrzení o zaměstnaneckém poměru – plné moci, jež tvoří přílohu č. 9 tohoto ujednání z e-mailové adresy stejné domény, pro kterou bude SSL certifikát vystaven.
- 4) Seznam osob, jež mohou být zmocněny k podání žádosti o SSL certifikát či k zneplatnění tohoto certifikátu:

P. č.	Titul, jméno a příjmení	Datum narození	RČ	Číslo OP	e-mailová adresa
1.	[REDACTED]				
2.					

- 5) Vydávání SSL certifikátů bude probíhat on-line po ověření žádosti a žadatele a výhradně prostřednictvím pracoviště registrační autority I.CA v sídle společnosti I.CA.
- 6) Technické požadavky, konkrétní postupy a jednotlivá povolená naplnění položek v DV a OV certifikátech jsou detailně uvedeny v příloze č. 10 tohoto ujednání. Informace a postup získání SSL certifikátu, jenž je součástí tohoto ujednání.
- 7) ČSSZ je povinna vytvářet žádosti o SSL certifikáty v souladu s platnou CP SSL a podle postupů uvedených v příloze č. 10 tohoto ujednání.

- 8) Pokud zasláná žádost nebude v souladu s CP SSL anebo požadavky uvedenými v příloze č. 10 tohoto ujednání, vyhrazuje si I.CA právo takovou žádost nepřijmout a nevydat příslušný SSL certifikát.
- 9) I.CA dále neodpovídá za škody způsobené spoléhajícím se třetím stranám v případech, kdy ČSSZ nesplnila povinnosti požadované CP SSL (např. poskytnutí nesprávných údajů apod.), dle kterých mohlo dojít k vydání SSL certifikátu.
- 10) Cena za vydání jednoho prvotního SSL certifikátu (DV nebo OV) na dobu platnosti 1 roku s uvedením jedné domény a splňujícího naplnění položek elektronické žádosti o vydání SSL certifikátu dle CP SSL pro ČSSZ činí:

967,- Kč bez DPH, tj. 1 170,07 Kč s DPH.

- 11) Cena za vydání jednoho prvotního SSL certifikátu (DV nebo OV) na dobu platnosti 1 roku s maximálním uvedením pěti domén a splňujícího naplnění položek elektronické žádosti o vydání SSL certifikátu dle CP SSL pro ČSSZ činí:

4 050,- Kč bez DPH, tj. 4 900,50 Kč s DPH.

- 12) Cena za vydání jednoho prvotního SSL certifikátu (DV nebo OV) na dobu platnosti 1 roku s maximálním uvedením deseti domén a splňujícího naplnění položek elektronické žádosti o vydání SSL certifikátu dle CP SSL pro ČSSZ činí:

7 355,- Kč bez DPH, tj. 8 899,55 Kč s DPH.“.

2. Strany se dále dohodly na tom, že dosavadní článek VIII. Ujednání s názvem **Závěrečná ustanovení** se nově označuje jako článek IX. s názvem **Závěrečná ustanovení**, a nově zní takto:

„IX. Závěrečná ustanovení

Nedílnou součástí tohoto ujednání jsou:

- a) Příloha č. 1 - Technické, procesní a bezpečnostní požadavky
 - b) Příloha č. 2 - Plná moc (vzor)
 - c) Příloha č. 3 - CPQC, CPQSC a PSQRA
 - d) Příloha č. 4 - CPKC a PSKRA
 - e) Příloha č. 5 - Rozsah a forma součinnosti při provozování Registrační autority
 - f) Příloha č. 6 - Prohlášení pověřené osoby (vzor)
 - g) Příloha č. 7 - Přehled umístění Registračních autorit ČSSZ (RA ČSSZ)
 - h) Příloha č. 8 - Certifikační politika pro SSL certifikáty
 - i) Příloha č. 9 - Potvrzení o zaměstnaneckém poměru – plná moc
 - j) Příloha č. 10 - Informace a postup získání SSL certifikátu.“.
3. Strany se dohodly na tom, že dosavadní přílohy č. 1 až č. 7 Ujednání se doplňují o nové přílohy, a to o přílohu č. 8 s názvem Certifikační politika pro SSL certifikáty, přílohu č. 9 s názvem Potvrzení o zaměstnaneckém poměru – plná moc a přílohu č. 10 s názvem Informace a postup získání SSL certifikátu.

II.

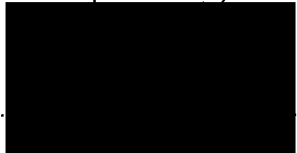
1. Ostatní ujednání Ujednání zůstávají tímto Dodatkem nedotčena.
2. Tento Dodatek nabývá platnosti a účinnosti dnem jeho podpisu Stranami.
3. Tento Dodatek je vyhotoven v pěti (5) vyhotoveních v českém jazyce s platností originálu, z nichž dvě (2) vyhotovení obdrží I.CA a tři (3) vyhotovení obdrží ČSSZ.
4. Nedílnou součástí tohoto Dodatku jsou nové přílohy č. 8, č. 9 a č. 10 Ujednání, tedy:
 - Příloha č. 8 – Certifikační politika pro SSL certifikáty,
 - Příloha č. 9 - Potvrzení o zaměstnaneckém poměru – plná moc,
 - Příloha č. 10 - Informace a postup získání SSL certifikátu.
5. Strany se s tímto Dodatkem důkladně seznámily a prohlašují, že jeho textu porozuměly a na důkaz své svobodné a určité vůle připojují níže své podpisy.

V Praze dne 22/2/2016

První certifikační autorita, a.s.



předseda představenstva



člen představenstva



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

V Praze dne 24.2.2016

**Česká republika -
Česká správa sociálního zabezpečení**



JUDr. Jiří Biskup
ústřední ředitel

Certifikační politika pro SSL certifikáty (CP SSL)

CP SSL

(Certifikační politika I.CA pro SSL certifikáty)

aktuální verze – viz.

WWW.ICA.CZ

Potvrzení o zaměstnaneckém poměru – plná moc

Tímto potvrzujeme, že pan/paní

.....,

R.Č. bytem

Č. OP

je k dnešnímu dni naším zaměstnancem.

Název: Česká republika – Česká správa sociálního zabezpečení
Adresa: Křížová 25, 225 08 Praha 5
IČ: 00006963

Souhlasíme s tím, aby mu/jí byl společností První certifikační autorita, a.s. vydán SSL
certifikát s tímto naplněním:

„CN“ pro DV certifikát nebo „O“ pro OV certifikát:

Název organizace: Česká správa sociálního zabezpečení IČ: 00006963

Adresa: Křížová 25, 225 08 Praha 5

E-mailová adresa žadatele:

Účel použití SSL certifikátu:

V Praze dne

.....	
jméno a funkce	podpis zaměstnance
oprávněné osoby k jednání za	
Českou republiku – Českou správu sociálního zabezpečení	

Informace a postup získání SSL certifikátu

Žadatel zasílá e-mailem soubor žádosti ve formátu PKCS#10 (.req) na e-mailovou adresu [redacted]. Žadatel může pro generování žádosti použít neveřejné generátory (při zachování důvěrnosti) uvedené na:

- <https://s.ica.cz/cgi-bin/zadosti-kl/sslDV.cgi> pro DV certifikát
- <https://s.ica.cz/cgi-bin/zadosti-kl/sslSV.cgi> pro OV certifikát
- V jejím předmětu musí být uvedeno: "Žádost o SSL certifikát".
- V těle emailu musí být uvedeno: "Já, níže uvedený, tímto prohlašuji, že všechny údaje uvedené v žádosti o SSL certifikát jsou pravdivé".

Žadatel v e-mailu uvede také kontaktní údaje – telefon, e-mail, poštovní adresu subjektu.

1. Rozlišují se dva typy certifikátů:

- Domain-Validated (DV) – ověřitelným údajem je doména, položky identifikující subjekt nesmí být v tomto certifikátu uvedeny (položky O, OU, L, St, ...)
- Subject-identity-Validated (SV) – obsahuje ověřitelné údaje o vlastníkovi/organizaci a název domény

2. Požadavky na doménu:

Jsou vydávány certifikáty pro všechny typy domén kromě nových gTLD (.company, .bike, .movie, .club apod.).

V žádosti může být pouze jedna doména druhého řádu (ica.cz) a až devět dalších názvů dnsName (subdomén - www.ica.cz, neco1.ica.cz, neco2.ica.cz).

V položkách žádosti dále nesmí být IP adresa a doména se zástupnými znaky, tzv. wildcard doména, např. *.ica.cz

3. Položky žádosti pro certifikát typu Domain-Validated (DV)

- Obecné jméno (CN) (**povinné**) = DNS název serveru, zároveň uveden i do subjectAlternativeName (ica.cz).
- domainComponent (DC) (volitelné) = pokud bude uvedeno, musí být obsaženy všechny části DNS názvu z CN (příklad – DC=ica, DC=cz).
- Country (C) (volitelné) = kód země sídla subjektu, nyní akceptováno pouze CZ.

Rozšíření subjectAlternativeName:

- dnsName (povinné) = alespoň jedna položka, první položka musí být shodná s CN, maximálně jedna doména 2. řádu (příklad dnsName = ica.cz, dnsName = www.ica.cz, dnsName = mail.ica.cz).

4. Položky žádosti pro certifikát typu Organization-Identity-Validated (OV)

5. Stejně položky jako u certifikátu typu DV a navíc:

- Organization (O) (**povinné**) = název organizace nebo ochranná známka subjektu ověřitelná důvěryhodným způsobem (např. na webu or.justice.cz).
- Organization unit (OU) (volitelné) = organizační jednotka
- Country (C) (**povinné**) = kód země, nyní pouze CZ.
- StreetAddress (nepovinné) = ulice subjektu.
- PostalCode (nepovinné) = PSČ subjektu.

Vyplnění jedné z těchto položek je **povinné**, druhá se stává volitelnou:

- Locality (L) = ověřená informace o lokalitě subjektu (Praha 9).
- State (St) = ověřená informace o provincii subjektu (Středočeský kraj).

6. Ověření vlastnictví domény

Ověření proběhne na základě kontaktních údajů uvedených v doménovém registru (dále jen "WHOIS") pro doménu, pro kterou byla přijata žádost o SSL certifikát.

Pokud se bude shodovat e-mailová adresa, ze které byla přijata žádost s adresou uvedenou v podepsaném dodatku, bude ověřena existence domény a její vlastnictví subjektem.

Bude-li e-mailová adresa, ze které žádost přišla, odlišná, bude na první e-mail uvedený z WHOIS, zaslán e-mail pro potvrzení souhlasu s vydáním certifikátu, e-mail bude získán z polí v uvedeném pořadí: registrant (držitel), technical, administrative.

Pokud údaje v WHOIS uvedeny nebudou, může být zaslán e-mail s žádostí o schválení na adresy

Bude-li žádost pro subdoménu, např. Mujweb.seznam.cz a žadatel není vlastníkem domény 2. řádu, tedy seznam.cz, bude potřebné svolení majitele domény – je třeba získat Autorizační dokument domény přímo od vlastníka domény seznam.cz.

7. Obnovení – následný certifikát

Není relevantní. Vždy se budou vydávat pouze prvotní certifikáty. Informace z žádosti je nutné vždy znovu ověřit.

K ověření bude možno použít stejné doklady, pokud jsou aktuální a nejsou starší než 39 měsíců.

8. Zneplatnění

Prováděné stejným způsobem jako u certifikátů vydávaných doposud (web + heslo, e-mail + heslo, podepsaný e-mail, doporučená zásilka + heslo).

Zneplatnění ověřitelné přes seznam CRL, případně online protokolem OCSP.

