Dodatek č. 2 smlouvy o dodávce certifikátů, časových razítek  
a certifikačních služeb pro informační systémy MZV

evidenční číslo smlouvy MZV: SM6113-002

Smluvní strany

První certifikační autorita, a.s.

se sídlem Podvlnný mlýn 2178/6,190 00 Praha 9

zapsaná v obchodním rejstříku, vedeném Městským soudem v Praze, spisová značka B 7136

264 39 395 CZ264 39 395

IČO:

DIČ:

zastoupená:

XXX předsedou představenstva a XXX, členem představenstva

Bankovní spojení: XXX

Číslo účtu: XXX dále jen „I.CA"

a

Česká republika - Ministerstvo zahraničních věcí

se sídlem Loretánské náměstí 101/5,118 00 Praha 1

IČO: 45769851

zastoupená: XXX, ředitelem odboru aplikací a informačních služeb

Bankovní spojení: Česká národní banka Praha 1

Číslo účtu: 17228-001/0710 dále jen „MZV"

uzavřely níže uvedeného dne, měsíce a roku tento dodatek č. 2 ke Smlouvě o dodávce certifikátů,  
časových razítek a certifikačních služeb pro informační systémy MZV č. SM6113-002 (dále jen „Smlouva").

Preambule

Obě strany podpisem tohoto Dodatku upřesňují Smlouvu o technické podmínky procesu vydávání a kontrol položek podtypu komerčních certifikátů, tzv. SSL (Secure Socket Layer) certifikátů (dále jen „SSL certifikáty"). Ostatní náležitosti Smlouvy nedotčené tímto Dodatkem zůstávají beze změny.

1. Vkládá se nový článek Vlil, který zní:

„Vlil,

Podmínky vydávání SSL certifikátů

1. SSL certifikáty budou vydávány v souladu s Certifikační politikóu pro SSL certifikáty (dále jen "CP SSL"), která je uvedena v příloze č. 14, a která je vždy dostupná v aktuálním znění na [www.ica.cz](http://www.ica.cz).
2. SSL certifikáty jsou dvojího typu:
3. tzv. Domain validated SSL certifikát (dále jen "DV") obsahující v příslušných položkách plně kvalifikovaná doménová jména.
4. tzv. Organization validated SSL certifikát (dále jen "OV") obsahující navíc informace o organizaci, které je certifikát vydáván.
5. Uvedené SSL certifikáty podle podmínek tohoto dodatku budou vydávány na základě elektronické žádosti o SSL certifikáty, která musí být předem zaslána na e-mailovou adresu ssl(5)ica.cz. 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 MZV uvedenou v Potvrzení o zaměstnaneckém poměru - plné moci, jež tvoří Přílohu č. 15 tohoto dodatku z e-mailové adresy stejné domény, pro kterou bude SSL certifikát vystaven.
6. 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.
7. Technické požadavky, konkrétní postupy a jednotlivá povolená naplnění položek v DV a OV certifikátech jsou detailně uvedeny v Příloze č. 16 Informace a postup získání SSL certifikátu, jenž je součástí tohoto dodatku.
8. MZV je povinna vytvářet žádosti o SSL certifikáty v souladu s platnou CP SSL a podle postupů uvedených v Příloze č. 16 tohoto dodatku.
9. Pokud zaslaná žádost nebude v souladu s CP SSL anebo požadavky uvedenými v Příloze č. 16, vyhrazuje si
10. CA právo takovou žádost nepřijmout a nevydat příslušný SSL certifikát.
11. I.CA dále neodpovídá za škody způsobené spoléhajícím se třetím stranám v případech, kdy MZV nesplnila povinnosti požadované CP SSL (např. poskytnutí nesprávných údajů apod.), dle kterých mohlo dojít k vydání SSL certifikátu.
12. 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 MZV činí:

967,- Kč bez DPH, tj. 1170,07 Kč s DPH

1. 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 MZV činí:

4 050,- Kč bez DPH, tj. 4900,50 Kč s DPH

1. 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 MZV činí:

7 355,- Kč bez DPH, tj. 8899,55 Kč s DPH.".

1. Do seznamu příloh v odstavci 14 článku XXXV se doplňují přílohy

„Příloha č. 14 - Certiflkační politika pro SSL certifikáty / Příloha č. 15 - Potvrzení o zaměstnaneckém poměru - plná moc Příloha č. 16 - Informace a postup získání SSL certifikátu.".

1. Dosavadní články Vlil až XXXV se přečíslovávají na IX až XXXVI.
2. Doplňují se nové Přílohy č. 14, č. 15 a č. 16.

Tento Dodatek nabývá platnosti a účinnosti dnem jeho podpisu Smluvními stranami.

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 MZV.

V Praze dne



V Praze dne

I



**Ministerstvo zahraničních věcí**

První certifikační autorita, a.s

XXX

XXX

ředitel odboru aplikací a informačních služeb

XXX

První certifikační autorita, a.s. Padvlnný mlýn 2178/6, 190 00 Praha 9 IČ: 26439395 **(**880**)**

Certifikační politika pro SSL certifikáty  
(CP SSL)

CP SSL

(Certifikační politika I.CA pro SSL certifikáty)

**aktuální verze-viz.**[WWW.ICA.CZ](http://WWW.ICA.CZ)

Potvrzení o zaměstnaneckém poměrů - plná moc

Tímto potvrzujeme, že pan/paní

R.Č. bytem

Č. OP

|  |  |
| --- | --- |
|  | je k dnešnímu dni naším zaměstnancem. |
| Název:  Adresa:  IČO: | Česká republika - Ministerstvo zahraničních věcí  Loretánské náměstí 101/5,118 00 Praha 1 45769851 |

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:  Adresa:  IČO: | Česká republika - Ministerstvo zahraničních věcí  Loretánské náměstí 101/5,118 00 Praha 1 45769851 |
| E-mailová adresa žadatele: Účel použití SSL certifikátu: |  |

|  |  |
| --- | --- |
| V Praze dne |  |

|  |  |
| --- | --- |
| jméno a funkce | Podpis zaměstnance |

pověřené osoby k jednání za Ministerstvo zahraničních věcí

/

Informace a postup získání SSL certifikátu

Žadatel zasílá e-mailem soubor žádosti ve formátu PKCS#10 (.req) na e-mailovou adresu ssl(5)ica.cz. Žadatel může pro generování žádosti použít neveřejné generátory (při zachování důvěrnosti) dostupné 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 předmětu e-mailu s žádostí 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,...)
* Subiect-identity-Validated (SV) - obsahuje ověřitelné údaje o vlastníkovi/organizacl a název domény

1. Požadavky na doménu:

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

* žádosti může být pouze jedna doména druhého řádu (ica.cz) a až devět dalších názvů dnsName (subdomén -[www.ica.cz](http://www.ica.cz), necol.ica.cz, neco2.ica.cz).
* položkách žádosti dále nesmí být IP adresa a doména se zástupnými znaky, tzv. wildcard doména, např.

\*. ica.cz

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

* Obecné jméno (CN) (povinné) = DIMS 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).

1. Položky žádosti pro certifikát typu Organization-ldentity-Validated (OV)
2. Stejné 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 Cl.
* 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).

1. 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 vpodepsaném 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, administrativě.

Pokud údaje v WHOIS uvedeny nebudou, může být zaslán e-mail s žádostí o schválení na adresy admin@<doména>, administrator@<doména>, webmaster@<doména>, hostmaster@<doména>, postmaster@<doména>.

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.

1. 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.

1. 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.

7