Smlouva o poskytování služeb I.CA

uzavřená podle ustanovení § 1746 odst. 2 zákona č. 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů (dále jen „Občanský zákoník“)

Smluvní strany

První certifikační autorita, a.s.

Se sídlem: Praha 9, Podvinný mlýn 2178/6, PSČ 190 00
Zastoupená: [redacted] předsedou představenstva
[redacted]nem představenstva
IČ: 264 39 395
DIČ: CZ26439395
Bankovní spojení: Československá obchodní banka, a.s.
Číslo účtu: 168457418/0300
zapsaná v obchodním rejstříku, vedeném Městským soudem v Praze, spisová značka B, vložka 7136.

(dále též „**I.CA**“ nebo „**Poskytovatel**“)

a

Česká republika – Národní úřad pro kybernetickou a informační bezpečnost
Se sídlem Brno, Mučednická 1125/31, PSČ 616 00
IČ: 05800226
Zastoupená: Ing. Karlem Řehkou, ředitelem
Bankovní spojení: Česká národní banka, pobočka Brno
Číslo účtu: 3031881/0710

(dále též „**Objednatel**“, **„zákazník“ nebo „žadatel“**)

(dále jednotlivě také jako **„Smluvní strana“** a společně také jako „**Smluvní** s**trany**“)

Preambule

Smluvní strany uzavírají v souladu s níže uvedeným dnem, měsícem a rokem tuto Smlouvu o poskytování služeb I.CA (dále jen "smlouva").

1. Článek
Úvodní ustanovení

1.1. Poskytovatel prohlašuje, že je kvalifikovaným poskytovatelem služeb vytvářejících důvěru podle Nařízení Evropského parlamentu a Rady č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES („eIDAS“) a zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů,

pro oblast vydávání kvalifikovaných certifikátů pro elektronické podpisy, kvalifikovaných elektronických časových razítek, kvalifikovaných certifikátů pro elektronické pečetě, kvalifikovaných certifikátů pro autentizaci internetových stránek a kvalifikované služby ověřování platnosti kvalifikovaných elektronických podpisů a pečetí.

2. Článek
Předmět smlouvy

2.1. Předmětem této smlouvy je poskytování služeb I.CA pro zákazníka v podobě vydávání tzv. SSL (Secure Socket Layer) certifikátů pro společnost zákazníka (dále jen "SSL certifikáty").

2.2. Definované SSL certifikáty podle podmínek této smlouvy jsou uvedených typů:

2.2.1. tzv. SSL Domain validated certifikát (dále jen "SSL DV") obsahující v příslušných položkách doménová jména.
SSL DV certifikáty budou vydávány v souladu s Certifikační politikou vydávání SSL certifikátů (dále jen "CPSSL"), která je uvedena v příloze č. 1 a která je vždy dostupná v aktuálním znění na www.ica.cz.

2.2.2. tzv. SSL Organization validated certifikát (dále jen "SSL OV") obsahující navíc informace o organizaci, které je certifikát vydáván.
SSL OV certifikáty budou vydávány v souladu s Certifikační politikou vydávání SSL certifikátů (dále jen "CPSSL"), která je uvedena v příloze č. 1 a která je vždy dostupná v aktuálním znění na www.ica.cz.

2.2.3. Kvalifikované certifikáty pro autentizaci internetových stránek vydávané právnickým osobám (dále jen QCweb, někdy označované také jako QWAC[1]; tyto certifikáty jsou založeny na profilu a podmínkách pro SSL Extended validation certifikáty) obsahující navíc údaje o vlastníkovi/organizaci a dále ověřitelné údaje.
QCweb certifikáty budou vydávány v souladu s Certifikační politikou vydávání kvalifikovaných certifikátů pro autentizaci internetových stránek právnickým osobám (dále jen "CPQCweb"), která je uvedena v příloze č. 2 a která je vždy dostupná v aktuálním znění na www.ica.cz.

2.2.4. Kvalifikované certifikáty pro autentizaci internetových stránek vydávané právnickým osobám s atributy pro PSD2 (dále jen „QCweb PSD2“).
QCweb PSD2 certifikáty budou vydávány v souladu s Certifikační politikou vydávání kvalifikovaných certifikátů pro autentizaci internetových stránek právnickým osobám (dále jen "CPQCweb"), která je uvedena v příloze č. 2 a která je vždy dostupná v aktuálním znění na www.ica.cz.

2.3. Uvedené SSL certifikáty podle podmínek této smlouvy budou vydávány na základě elektronické žádosti o SSL certifikáty, která musí být zaslána na e-mailovou adresu ssl@ica.cz a která musí dále splňovat níže popsané a definované požadavky dle CPSSL respektive dle CPQCweb. Elektronická žádost musí být odeslána v příloze e-mailové zprávy, kterou prokazatelně odešle oprávněná osoba (dále též „schvalovatel“) na straně

[1] QWAC - Qualified Web Authentication Certificate

zákazníka a která bude k tomuto úkonu zplnomocněna plnou mocí, jejíž vzor je uveden v příloze č. 3 této smlouvy (dále jen "Plná moc pro SSL a QCweb certifikáty").

2.4. Vydávání certifikátů SSL bude probíhat on-line po ověření žádosti a žadatele a pouze prostřednictvím pracoviště registrační autority I.CA v sídle společnosti I.CA.

3. Článek
Technické požadavky a postup získání SSL certifikátů

3.1. Technické požadavky, konkrétní postupy, odkazy na generátory a jednotlivé povolené naplnění položek v SSL DV, SSL OV a QCweb certifikátech jsou dále detailně uvedeny v příloze č. 4 v dokumentu "Informace a postup získání SSL certifikátu", jenž je součástí této smlouvy.

4. Článek
Práva a povinnosti zákazníka vyplývající z této smlouvy

4.1. Zákazník je povinen vytvářet žádosti o SSL certifikáty v souladu s platnou CPSSL nebo v souladu s platnou CPQCweb a podle postupů uvedených v dokumentu "Informace a postup získání SSL certifikátu".

4.2. Zákazník prohlašuje, že bude používat SSL a QCweb certifikáty pouze k účelu, ke kterým byly vydány.

5. Článek
Práva a povinnosti I.CA vyplývající z této smlouvy

5.1. Pokud zaslaná žádost nebude v souladu CPSSL či v souladu s CPQCweb a nebo požadavky uvedenými v příloze č. 4, vyhrazuje si I.CA právo takovou žádost nepřijmout a nevydat příslušný SSL certifikát.

5.2. I.CA dále neodpovídá za škody způsobené spoléhajícím se třetím stranám v případech, kdy zákazník nesplnil povinnosti požadované CPSSL či CPQCweb (např. poskytnutí nesprávných údajů apod.), dle kterých mohlo dojít k vydání SSL certifikátů.

6. Článek
Cenové podmínky

6.1. Cena za vydání jednoho prvotního DV nebo OV SSL certifikátu na dobu platnosti 1 roku s uvedením **jedné domény** a splňujícího naplnění položek elektronické žádosti o vydání SSL certifikátu dle CPSSL pro zákazníka činí:

967,- Kč bez DPH

6.2. Cena za vydání jednoho prvotního DV nebo OV SSL certifikátu na dobu platnosti 1 roku s maximálním uvedením **pěti domén** a splňujícího naplnění položek elektronické žádosti o vydání SSL certifikátu dle CPSSL pro zákazníka činí:

4.050,- Kč bez DPH

6.3. Cena za vydání jednoho prvotního DV nebo OV SSL certifikátu na dobu platnosti 1 roku s maximálním uvedením **deseti domén** a splňujícího naplnění položek elektronické žádosti o vydání SSL certifikátu dle CPSSL pro zákazníka činí:

7.355,- Kč bez DPH

6.4. Cena za vydání jednoho prvotního QCweb certifikátu na dobu platnosti 1 roku s uvedením **jedné domény** a splňujícího naplnění položek elektronické žádosti o vydání QCweb certifikátu dle CPQCweb pro zákazníka činí:

1.934,- Kč bez DPH

6.5. Cena za vydání jednoho prvotního QCweb certifikátu na dobu platnosti 1 roku s maximálním uvedením **pěti domén** a splňujícího naplnění položek elektronické žádosti o vydání QCweb certifikátu dle CPQCweb pro zákazníka činí:

8.100,- Kč bez DPH

6.6. Cena za vydání jednoho prvotního QCweb certifikátu na dobu platnosti 1 roku s maximálním uvedením **deseti domén** a splňujícího naplnění položek elektronické žádosti o vydání QCweb certifikátu dle CPQCweb pro zákazníka činí:

14.710,- Kč bez DPH

6.7. Cena za vydání jednoho prvotního QCweb PSD2 certifikátu na dobu platnosti 1 roku s uvedením **jedné domény** a splňujícího naplnění položek elektronické žádosti o vydání QCweb certifikátu dle CPQCweb pro zákazníka činí:

3.000,- Kč bez DPH

6.8. Cena za vydání jednoho prvotního QCweb PSD2 certifikátu na dobu platnosti 1 roku s maximálním uvedením **pěti domén** a splňujícího naplnění položek elektronické žádosti o vydání QCweb certifikátu dle CPQCweb pro zákazníka činí:

9.000,- Kč bez DPH

6.9. Cena za vydání jednoho prvotního QCweb PSD2 certifikátu na dobu platnosti 1 roku s maximálním uvedením **deseti domén** a splňujícího naplnění položek elektronické žádosti o vydání QCweb certifikátu dle CPQCweb pro zákazníka činí:

16.000,- Kč bez DPH

6.10. Vyúčtování ceny za vydání všech prvotních SSL a QCweb certifikátů bude podle této smlouvy prováděno hromadně, vždy jednou měsíčně zpětně za poslední uplynulý kalendářní měsíc, v němž I.CA SSL a QCweb certifikáty vydala.

6.11. I.CA je povinna vystavit řádný daňový doklad podle podmínek této smlouvy do 15. dne kalendářního měsíce, za který je účtována cena za vydání všech SSL a QCweb certifikátů.

6.12. Zákazník je povinen uhradit cenu za všechny vydané SSL a QCweb certifikáty I.CA, převodem na účet I.CA do 30 dnů, a to na základě daňového dokladu, vystaveného I.CA a odeslaného na e-mailovou adresu posta@nukib.cz, případně do datové schránky: zzfnkp3.

Daňový doklad musí mít náležitosti daňových a účetních dokladů, stanovených platnými právními předpisy. Zákazník je oprávněn daňový doklad, který nebude splňovat náležitosti podle platných právních předpisů a jehož věcný obsah nebude v souladu s počtem a druhem vydaných SSL certifikátů, vrátit I.CA.

I.CA je povinna nedostatky daňového dokladu odstranit a vystavit nový daňový doklad. Na základě vadně vystaveného daňového dokladu ve smyslu tohoto odstavce se zákazník neocitá v prodlení. Doba splatnosti počíná běžet znovu od opětovného doručení doplněného či opraveného, resp. nově vystaveného daňového dokladu.

6.13. V případě prodlení zákazníka s uhrazením daňového dokladu, vystaveného I.CA, je I.CA oprávněna účtovat zákazníkovi úrok z prodlení ve výši stanovené platnými právními předpisy.

6.14. Při nezaplacení ceny za vydané SSL a QCweb certifikáty v době splatnosti, si I.CA vyhrazuje právo nepřijímat od zákazníka další žádosti na vydávání SSL a QCweb certifikátů podle této smlouvy, a to do doby vyrovnání všech finančních závazků ze strany zákazníka.

7. Článek
Další ustanovení týkající se QCweb a QCweb PSD2 certifikátů a oprávněné osoby zákazníka žádat o tyto certifikáty

7.1. Žádosti o QCweb a QCweb PSD2 certifikáty a jejich dodatečné schvalování, pokud to bude nutné, bude ověřováno jedním z následujících způsobů:

7.1.1. Přímé fyzické ověření schvalovatele podle osobních dokladů - při

a) osobním předání žádosti nebo
b) osobním potvrzení o schválení žádosti.

7.1.2. Předání dodatečných dokumentů na dálku, které musí obsahovat kvalifikovaný elektronický podpis dle eIDAS na PDF dokumentech a na emailové zprávě obsahující:

a) dokument žádosti o certifikát a související dokumenty nebo
b) odpověď na požadavek o potvrzení o schválení dokumentu o žádosti

7.2. Oprávnění schvalovatele musí být periodicky potvrzováno jednou ročně vždy na začátku kalendářního roku (dále jen „periodicita“) a to uvedeným způsobem:

7.2.1. Pracovník I.CA vyzve zákazníka k potvrzení periodicity zasláním výzvy na email zplnomocněné osoby dle Plné moci pro potvrzovatele periodicity viz. příloha č. 5, která bude k tomuto kroku zplnomocněna. Nesmí se jednat o jednoho ze schvalovatelů, kteří budou uvedeni v aktuálně platné Plné moci pro SSL certifikáty viz. příloha č. 3 a její následné verze.

7.2.2. I.CA bude považovat periodicitu za potvrzenou přijetím emailu s odpovědí na výzvu o potvrzení periodicity, kterou zašle odpovědný pracovní I.CA, ve kterém bude v příloze dokument typu PDF, který bude elektronicky podepsán kvalifikovaným elektronickým podpisem dle eIDAS jedním ze statutárních zástupců zákazníka nebo jedním ze zplnomocněných osob dle Plné moci pro potvrzovatele periodicity.

7.2.3. Pokud nebude pravidelně potvrzována periodicita, nesmí I.CA dle požadavků na QCweb certifikáty vydávat nové, resp. navazující QCweb a QCweb PSD2 certifikáty a smluvní vztah může být se zákazníkem z těchto důvodů ukončen.

7.3. Pokud dojde k situaci, kdy oprávnění některého ze schvalovatelů uvedených v Plné moci pro SSL certifikáty je odvoláno, musí zákazník o této skutečnosti **ihned** uvědomit I.CA, zasláním emailu na kontaktní osobu na straně I.CA, který bude elektronicky podepsán kvalifikovaným elektronickým podpisem dle eIDAS jedním ze statutárních zástupců zákazníka nebo zplnomocněnou osobou dle Plné moci pro potvrzování periodicity.

7.4. Ke každému vydanému QCweb a QCweb PSD2 certifikátu je možné zasílat na email schvalovatele elektronicky dokumentaci k vydanému certifikátu ve formě Protokolu o podání žádosti o vydání kvalifikovaného certifikátu pro autentizaci webových stránek certifikátu I.CA a Protokol (Podmínky) o vydání a používání kvalifikovaného certifikátu pro autentizaci internetových stránek .

7.5. Zákazník požaduje zasílat dokumentaci definovanou v bodě 7.4. ke každému vydanému QCweb a QCweb PSD2 certifikátu na email schvalovatele - ANO.

7.6. Upozornění na závažné následky vyplývající ze zneužití QCweb a QCweb PSD2:

7.6.1. QCweb a QCweb PSD2 certifikát (a k němu příslušný soukromý klíč) slouží jako forma digitální identity žadatele/zákazníka. Ztráta nebo zneužití této identity, může mít za následek velké škody pro žadatele/zákazníka. Žadatel/zákazník je proto zodpovědný za všechna použití svého QCweb a QCweb PSD2 certifikátu (a k němu příslušného soukromého klíče). Žadatel/zákazník potvrzuje, že má právo používat všechna doménová jména, která požaduje uvést v QCweb a QCweb PSD2 certifikátech.

7.6.2. Žadatel/zákazník podpisem smlouvy potvrzuje, že se seznámil s podmínkami smlouvy a podmínkami používání QCweb a QCweb PSD2 a zavazuje se je dodržovat.

8. Článek
Další ujednání

8.1. I.CA se zavazuje, že pokud v souvislosti s realizací této smlouvy při plnění svých povinností přijde do styku s osobními údaji ve smyslu nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice

95/46/ES (obecné nařízení o ochraně osobních údajů) (dále jen „GDPR“), učiní veškerá opatření, aby nedošlo k neoprávněnému nebo nahodilému přístupu k těmto osobním údajům, neoprávněným přenosům, k neoprávněnému zpracování, či jinému zneužití osobních údajů. I.CA se zavazuje, že podnikne všechny nezbytné kroky k zabezpečení osobních údajů. I.CA zejména zajistí, aby přístup osobním údajům měli pouze zaměstnanci I.CA, jejichž přístup je nezbytný ke splnění předmětu této smlouvy a že tyto činnosti budou vykonávat pouze osoby bezúhonné a zavázané povinností mlčenlivosti.

9. Článek
Závěrečná ustanovení

9.1. Tato Smlouva a vztahy z ní vyplývající se řídí českým právním řádem. Veškeré spory vyplývající z této Smlouvy se smluvní strany budou snažit řešit smírnou cestou. Teprve nepovede-li takové smírčí jednání k vyřešení sporu, bude soudní spor veden u příslušného obecného soudu ČR.

9.2. Pokud jakýkoli závazek dle Smlouvy nebo kterékoli ustanovení Smlouvy je nebo se stane neplatným či nevymahatelným, nebude to mít vliv na platnost a vymahatelnost ostatních závazků a ustanovení dle Smlouvy a smluvní strany se zavazují takovýto neplatný nebo nevymahatelný závazek či ustanovení nahradit novým, platným a vymahatelným závazkem, nebo ustanovením, jehož předmět bude nejlépe odpovídat předmětu a ekonomickému účelu původního závazku či ustanovení.

9.3. V případě, že by se některá ustanovení Smlouvy stala neplatnými v důsledku legislativních změn, nestává se neplatnou celá Smlouva. V takovém případě sjednají smluvní strany nové znění dotčených ustanovení tak, aby vystihovalo co nejpřesněji podstatu původního ujednání a aby co nejlépe odpovídalo duchu Smlouvy.

9.4. Smluvní strany souhlasí s uveřejněním této Smlouvy v registru smluv podle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů a rovněž na profilu objednatele, případně i na dalších místech, kde tak stanoví právní předpis. Uveřejnění této Smlouvy prostřednictvím registru smluv ve lhůtě stanovené zákonem zajistí objednatel.

9.5. Tato Smlouva nabývá platnosti dnem jejího podpisu oběma smluvními stranami.

9.6. Tato Smlouva nabývá účinnosti dnem jejího uveřejnění v informačním systému veřejné správy, který slouží k uveřejňování smluv podle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů.

9.7. Tato Smlouva se uzavírá na dobu neurčitou.

9.8. Místem plnění Smlouvy je sídlo objednatele.

9.9. Smlouvu je možné ukončit:

a) písemnou dohodou smluvních stran;

b) písemnou výpovědí některé ze smluvních stran, zaslanou druhé smluvní straně, a to buď výpovědí s důvodem, kterým je podstatné porušení ustanovení této Smlouvy druhou smluvní stranou, nebo výpovědí bez uvedení důvodu. V obou případech se uplatní výpovědní doba v délce 30 kalendářních dnů počínající běžet prvním dnem

následujícím po dni, kdy bylo písemné vyhotovení výpovědi prokazatelně doručeno druhé smluvní straně.

9.10. Písemnou dohodou smluvních stran je Smlouva ukončena ke dni v této dohodě uvedené a není-li v dohodě takový den uveden, pak ke dni podpisu dohody oběma smluvními stranami.

9.11. Ukončením Smlouvy nejsou smluvní strany zbaveny povinnosti vyrovnat veškeré závazky vzniklé v důsledku platnosti a účinnosti této Smlouvy a učinit veškeré úkony, které nesnesou odkladu a které jsou nutné k zabránění vzniku škody na straně jedné ze smluvních stran.

9.12. Smluvní strany se dohodly, že se ve vztazích mezi I.CA a objednatelem vyplývajících z této Smlouvy neuplatní §1895 – §1900 občanského zákoníku.

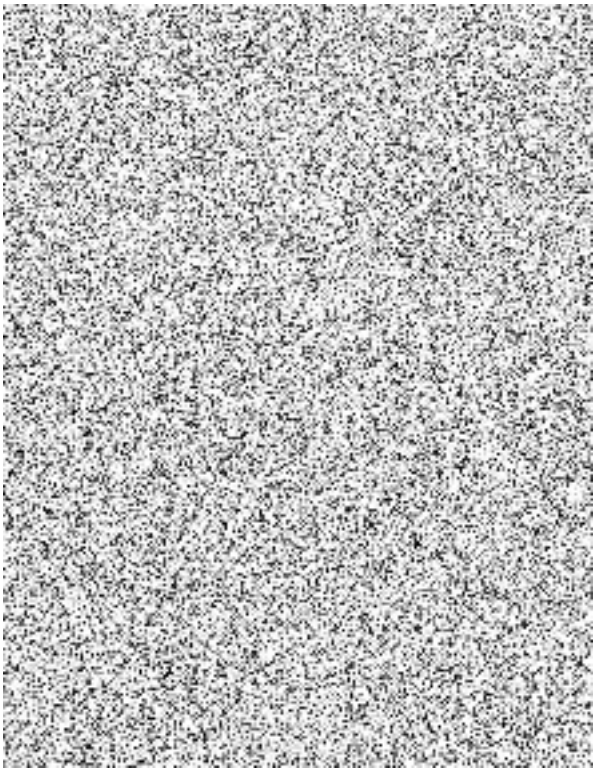
9.13. Tato Smlouva může být změněna dohodou obou smluvních stran. Dohoda o změně Smlouvy nebo o jejím zrušení musí mít písemnou formu označenou jako vzestupně číslované dodatky a musí být podepsána oprávněnými zástupci obou smluvních stran.

9.14. Tato Smlouva je vyhotovena v elektronické podobě

9.15. Seznam příloh:

Příloha č.1 - Certifikační politika vydávání SSL certifikátů (CPSSL)
Příloha č.2 - Certifikační politika vydávání kvalifikovaných certifikátů pro autentizaci internetových stránek právnickým osobám (CPQCweb)
Příloha č.3 - Plná moc pro SSL a QCweb certifikáty
Příloha č.4 - Informace a postup získání SSL certifikátu
Příloha č.5 - Plná moc pro potvrzovatele periodicity.

Za I.CA:



Za zákazníka:

(podepsáno elektronicky)

……

Ing. Karel Řehka
ředitel

Příloha č. 1

CPSSL

(Certifikační politika vydávání SSL certifikátů)

aktuální verze – viz.

WWW.ICA.CZ

Příloha č. 2

CPQCweb

(Certifikační politika vydávání kvalifikovaných certifikátů pro autentizaci internetových stránek právnickým osobám)

aktuální verze – viz.

WWW.ICA.CZ

Příloha č. 4

Informace a postup získání SSL certifikátu

Žadatel zasílá e-mailem soubor žádosti ve formátu PKCS#10 (.req) na e-mailovou adresu ssl@ica.cz.

- V jejím předmětu musí být uvedeno: *"Žádost o SSL certifikát"*.
- V těle emailu po-té 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 uvedené typy certifikátů:

- *Domain-Validated (DV)* – ověřitelným údajem je doména, položky identifikující subjekt nesmí být v tomto certifikátu uvedeny (položky O, OU, L, St, …)

  generátor žádosti: https://s.ica.cz/cgi-bin/zadosti-kl/sslDV.cgi

- *Organization-identity-Validated (OV)* – obsahuje ověřitelné údaje o vlastníkovi/organizaci a název domény

  generátor žádosti: https://s.ica.cz/cgi-bin/zadosti-kl/sslSV.cgi

- *Kvalifikovaný certifikát pro autentizaci internetových stránek (QCweb)* – obsahuje ověřitelné údaje o vlastníkovi/organizaci, název domény a dále ověřitelné údaje - položky O, OU, L, St, C, IČ, TO …)

  Varianta QCweb PSD2 navíc musí obsahovat informace o poskytovateli platebních služeb. Tj. identifikaci národního vydavatele (v CZ ČNB), číslo licence a přidělené role od národního vydavatele.

  generátor žádosti: https://s.ica.cz/cgi-bin/zadosti/RequestQWEBLCZ.cgi

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 (např. ica.cz) a až devět dalších názvů dnsName (subdomén/serverů - 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 SSL typu Domain-Validated (DV)

- Obecné jméno (CN) **(povinné)** = DNS název serveru, zároveň uveden i do subjectAlternativeName (např. www.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.

3.1. 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 SSL typu Organization-Identity-Validated (OV)

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 CZ.

- StreetAddress (nepovinné) = ulice subjektu.

- PostalCode (nepovinné) = PSČ subjektu.

*4.1. 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).

5. Položky žádosti pro certifikát SSL typu QCweb

- Obecné jméno (CN) **(povinné)** = DNS název serveru, zároveň uveden i do subjectAlternativeName (příklad - www.ica.cz).

- domainComponent **(**DC) (volitelné) = pokud bude uvedeno, musí být obsaženy všechny části DNS názvu z CN (příklad – DC=ica, DC=cz).

- Organization (O) **(povinné)** = název organizace nebo ochranná známka subjektu ověřitelná důvěryhodným způsobem (např. na webu justice.cz).

- Serialnumber (IČ) **(povinné)** = identifikační číslo organizace nebo subjektu ověřitelné důvěryhodným způsobem (např. na webu or.justice.cz).

- Type organization (TO) **(povinné)** = typ organizace (private organization) nebo subjektu ověřitelné důvěryhodným způsobem (např. na webu or.justice.cz).

- Organization unit (OU) (volitelné) = organizační jednotka

- Country (C) **(povinné)** = kód země, ve kterém sídlí organizace nebo subjekt ověřitelné důvěryhodným způsobem (např. na webu or.justice.cz). Nyní pouze CZ.

- State **(povinné)** = kraj země, ve kterém sídlí organizace nebo subjekt ověřitelné důvěryhodným způsobem (např. na webu or.justice.cz). Nyní pouze CZ.

- Locality **(povinné) =** město, ve kterém sídlí organizace nebo subjekt ověřitelné důvěryhodným způsobem (např. na webu or.justice.cz).

- StreetAddress (nepovinné) = ulice subjektu.

- PostalCode (nepovinné) = PSČ subjektu.

5.1. Rozšíření subjectAlternativeName pro QCweb:

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

5.2. Rozšíření subjectAlternativeName pro QCweb PSD2:

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

- directoryName - Description **(povinné)** = autorizované role poskytovatele platebních služeb, minimálně 1 maximálně 4.

- directoryName - DN Qualifier **(povinné)** = jméno registrátora v anglickém jazyce (národní vydavatel).

- directoryName - DMDName **(povinné)** = autorizační číslo poskytovatele platebních služeb dostupné ve veřejném registru.

6. Ověření vlastnictví domény

I.CA ověřuje DNS vlastnictví domény jedním z následujících způsobů:

- na e-mail uvedený u doménového kontaktu dle WHOIS zašle e-mail žádající schválení vydání SSL certifikátu pro DNS jména obsažená v předložené žádosti a který obsahuje náhodný řetězec, doménový kontakt pošle schválení žádosti obsahující tento řetězec zpět do I.CA (#2),
    - Poznámka: (#číslo) označuje číslo podkapitoly popisující příslušný způsob ověřování v BR.

- I.CA zašle na jeden z e-mailů admin, administrator, webmaster, hostmaster nebo postmaster @doména zprávu žádající schválení vydání SSL certifikátu pro DNS jména obsažená v předložené žádosti a která bude obsahovat náhodný řetězec; kontaktní osoba pošle schválení žádosti obsahující tento řetězec zpět do I.CA (#4),

- správce domény vytvoří na serveru pro požadované FQDN adresář /.well-known/pki-validation/, ve kterém vytvoří soubor ica.html a obsahem souboru bude náhodný řetězec, který poskytne I.CA (#6),

- správce domény pro požadované FQDN vytvoří nový DNS záznam typu CNAME nebo TXT, který bude obsahovat náhodný řetězec, který určí I.CA (#7).

Platnost náhodných řetězců je ve všech případech 30 dní.

7. Kontrola CAA záznamů[1]

I.CA provede první kontrolu a:

- pokud byla nalezena množina CAA záznamů, pak vyčká po dobu větší z hodnot (doba TTL CAA záznamu, 8 hodin),

- pokud neexistuje CAA záznam, pak vyčká 8 hodin, a poté provede opakovanou kontrolu.

K dalším krokům ověření žádosti a vydání Certifikátu bude pokračováno pouze pokud je při opakované kontrole zjištěno, že:

- buď žádný CAA záznam neexistuje,
- nebo je nalezena množina CAA záznamů a současně platí:
  - žádný z množiny CAA záznamů neobsahuje neznámou značku a současně není označen jako kritický,
  - a množina CAA záznamů se značkou "issue" je prázdná nebo obsahem některého záznamu z množiny CAA záznamů se značkou "issue" je „ica.cz“.

V opačných případech je žádost odmítnuta.

8. Obnovení – následný certifikát

Při obnově je vždy nutné zaslat novou žádost o certifikát. Certifikáty se neobnovují, nýbrž vydávají se pokaždé pouze prvotní. Informace z žádosti je nutné vždy znovu ověřit.

K ověření bude možno použít stejné doklady, pokud jsou aktuální a nejsou starší než 13 měsíců pro QCweb.

9. Zneplatnění

Zneplatnění je možné provádět obvyklým způsobem (web + heslo pro zneplatnění, e-mail + heslo pro zneplatnění, podepsaný e-mail, doporučená zásilka + heslo pro zneplatnění).

[1] CAA záznamy – specifikují certifikační autority, které mohou pro uvedenou doménu vydávat SSL certifikáty.