Dodatek č. 2

k rámcové smlouvě ze dne 14. 03. 2017

První certifikační autorita, a.s.
zapsaná v obchodním rejstříku u Městského soudu v Praze, oddíl B, vložka 7136

se sídlem:	Praha 9 - Libeň, Podvinný mlýn 2178/6, PSČ 190 00
zastoupená:	Ing. Petrem Budišem, Ph.D., MBA, předsedou představenstva a Ing. Romanem Kučerou, členem představenstva
IČO:	26439395
DIČ:	CZ26439395

(v textu též **„poskytovatel" či „I.CA"**)

a

Ústřední vojenská nemocnice – Vojenská fakultní nemocnice Praha
příspěvková organizace zřízená Ministerstvem obrany ČR

se sídlem:	U Vojenské nemocnice 1200, 169 02 Praha 6
zastoupená:	prof. MUDr. Miroslavem Zavoralem, Ph. D., ředitelem
IČO:	61383082
DIČ:	CZ61383082

(v textu též **„objednatel", „zákazník" nebo „žadatel"**)

Preambule

1. Smluvní strany uzavřely dne 14.03.2017 na základě výsledku výběrového řízení k veřejné zakázce malého rozsahu s názvem „Uzavření rámcové smlouvy služeb certifikační autority a provozu registračního místa" Rámcovou smlouvu, ev. č. objednatele 0281/2017-SML, jejímž předmětem je poskytování služeb certifikační autority (dále jen „Smlouva").
2. V návaznosti na požadavek technické specifikace předmětu plnění uvedený v bodu c) v příloze č. 1 Smlouvy „Možnost vydání ostatních druhů certifikátů" obě strany podpisem tohoto Dodatku upřesňují Smlouvu o technické podmínky procesu vydávání a kontrol položek kvalifikovaných certifikátů pro autentizaci internetových stránek. Ostatní náležitosti Smlouvy nedotčené tímto Dodatkem zůstávají beze změny.
3. Smluvní strany prohlašují, že změna závazku ze Smlouvy nikterak nemění celkovou povahu veřejné zakázky, hodnota předmětné změny (1 934,- Kč bez DPH) je nižší než finanční limit pro nadlimitní veřejnou zakázku a než 10 % původní hodnoty závazku ze Smlouvy ve smyslu ustanovení § 222 odst. 4 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů. Smluvní strany na základě výše uvedeného prohlašují, že změnou smluvních ujednání uvedených

v tomto Dodatku č. 2 nedochází k podstatné změně závazku ze Smlouvy ve smyslu ust. § 222 odst. 3 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů.

I. Změna smlouvy

1. Příloha č. 2 Smlouvy se doplňuje o další odstavec v následujícím znění: „Cena za vydání jednoho kvalifikovaného certifikátu pro autentizaci internetových stránek na dobu platnosti 1 roku s uvedením jedné domény činí 1 934,- Kč bez DPH."
2. Do seznamu příloh v odstavci č. 8, části IX. se doplňuje „- Příloha č. 4 - Technické podmínky procesu vydávání a kontrol položek kvalifikovaných certifikátů pro autentizaci internetových stránek".
3. Doplňuje se nová příloha č. 4.

II. Závěrečná ustanovení

1. Tento dodatek č. 2 nabývá platnosti dnem jeho podpisu oběma smluvními stranami a účinnosti jeho uveřejněním v registru smluv.
2. Smluvní strany se dohodly na tom, že Dodatek č.2 zašle správci registru smluv k uveřejnění 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, objednatel, a to nejpozději do 10 pracovních dnů od uzavření tohoto Dodatku č.2. Poskytovatel se zavazuje poskytnout objednateli za tímto účelem nezbytnou součinnost. Obě smluvní strany prohlašují, že žádná část Dodatku č. 2 neobsahuje jejich obchodní tajemství.
3. Dodatek č. 2 se vyhotovuje ve dvou stejnopisech, po jednom pro každou smluvní stranu.

V Praze dne: dle el. podpisu

za poskytovatele:

Petr Budiš
Digitálně podepsal Petr Budiš
Datum: 2021.08.25 13:01:17 +02'00'

.....

Ing. Petr Budiš, Ph.D., MBA
předseda představenstva společnosti
První certifikační autorita, a.s.

Ing. Roman Kučera
Digitálně podepsal Ing. Roman Kučera
Datum: 2021.08.25 13:00:26 +02'00'

.....

Ing. Roman Kučera
člen představenstva společnosti
První certifikační autorita, a.s.

V Praze dne: dle el. podpisu

za objednatele:

[redacted]

prof. MUDr. Miroslav Zavoral, Ph. D.
ředitel Ústřední vojenské nemocnice -
Vojenské fakultní nemocnice Praha

Příloha č. 4

Technické podmínky procesu vydávání a kontrol položek kvalifikovaných certifikátů pro autentizaci internetových stránek

1. Tato příloha upravuje podmínky vydávání kvalifikovaných certifikátů pro autentizaci internetových stránek vydávané právnickým osobám (dále též 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.
2. QWAC certifikáty budou vydávány v souladu s Certifikační politikou vydávání kvalifikovaných certifikátů pro autentizaci internetových stránek právnickým osobám (dále jen "CPQWAC"), která je vždy dostupná v aktuálním znění na [redacted]
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 [redacted] a která musí dále splňovat níže popsané a definované požadavky dle CPQWAC. Elektronická žádost musí být odeslána v příloze e-mailové zprávy, kterou prokazatelně odešle oprávněná osoba (dále též „schvalovatel") na straně zákazníka a která bude k tomuto úkonu zplnomocněna plnou mocí, jejíž vzor je uveden níže (dále jen "Plná moc pro QWAC certifikáty"). **Plné moci nebo tato smlouva musí být úředně ověřena (notářsky nebo přes Czech POINT) nebo elektronicky podepsána kvalifikovaným elektronickým podpisem dle eIDAS od statutárních zástupců zákazníka a všech jeho zmocněnců.**
4. Bude-li žadatelem o certifikát SSL přímo jednatel nebo statutární zástupce zákazníka, který má právo jednat pouze svým jménem, nemusí se Plná moc pro QWAC certifikáty dle odstavce 3. vyplňovat. Jednatel nebo statutární zástupce bude odesílat žádosti o certifikát z e-mailové adresy: .....@..... (Pokud nebude zasílat žádosti statutární zástupce, není nutné e-mail vyplňovat.).
5. 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.
6. Technické požadavky, konkrétní postupy, odkazy na generátory a jednotlivé povolené naplnění položek v QWAC certifikátech jsou dále detailně uvedeny v kapitole "Informace a postup získání SSL certifikátu" níže.

Práva a povinnosti zákazníka ve vztahu ke QWAC certifikátům

1. Zákazník je povinen vytvářet žádosti o SSL certifikáty v souladu s platnou CPQWAC a podle postupů uvedených v dokumentu "Informace a postup získání SSL certifikátu".
2. Zákazník prohlašuje, že bude používat SSL a QWAC certifikáty pouze k účelu, ke kterým byly vydány.

Práva a povinnosti I.CA ve vztahu ke QWAC certifikátům

1. Pokud zaslaná žádost nebude v souladu s CPQWAC anebo požadavky uvedenými v kapitole "Informace a postup získání SSL certifikátu" níže, vyhrazuje si I.CA právo takovou žádost nepřijmout a nevydat příslušný SSL certifikát.

[1] QWAC - Qualified Web Authentication Certificate

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

Další podmínky týkající se QWAC certifikátů a oprávněné osoby zákazníka žádat o tyto certifikáty

1. Žádosti o QWAC certifikáty a jejich dodatečné schvalování, pokud to bude nutné, bude ověřováno jedním z následujících způsobů:

   1.1. Přímé fyzické ověření schvalovatele podle osobních dokladů při

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

   1.2. Předání dodatečných dokumentů na dálku, které musí obsahovat kvalifikovaný elektronický podpis dle eIDAS na PDF dokumentech a na e-mailové zprávě obsahující:

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

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

   2.1. Pracovník I.CA vyzve zákazníka k potvrzení periodicity zasláním e-mailu na jednoho ze statutárních zástupců zákazníka [redacted] nebo zašle tuto výzvu na e-mail zplnomocněné osoby dle Plné moci pro potvrzovatele periodicity viz. vzor níže, která bude k tomuto kroku zplnomocněna. Nesmí se jednat o jednoho ze schvalovatelů, kteří budou uvedeni v aktuálně platné Plné moci pro SSL certifikáty.

   2.2. I.CA bude považovat periodicitu za potvrzenou přijetím e-mailu s odpovědí na výzvu o potvrzení periodicity zaslanou odpovědným pracovníkem 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.

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

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 e-mailu 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.

4. Ke každému vydanému QWAC certifikátu je možné zasílat na e-mail schvalovatele elektronicky dokumentaci k vydanému certifikátu ve formě Protokolu o podání žádosti o vydání kvalifikovaného certifikátu pro autentizaci webových stránek certifikátu I.CA (dále jen „Protokol žádosti“) a Smlouvu o vydání a používání kvalifikovaného certifikátu pro autentizaci internetových stránek (dále jen „Smlouva QWAC“).

5. Zákazník požaduje zasílat dokumentaci definovanou v bodě 4. ke každému vydanému QWAC certifikátu na e-mail schvalovatele: ANO.

6. Upozornění na závažné následky vyplývající ze zneužití QWAC:

6.1. QWAC 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 QWAC certifikátu (a k němu příslušného soukromého klíče). Žadatel/zákazník potvrzuje, že má právo používat všechna doménová jména, která požaduje uvést v QWAC certifikátech.

6.2. Žadatel/zákazník podpisem smlouvy potvrzuje, že se seznámil s podmínkami smlouvy a podmínkami používání QWAC a zavazuje se je dodržovat.

Plná moc pro QWAC certifikáty

Zmocnitel (společnost /organizace): .....

se sídlem: ..... IČ: .....

Zastoupená:

jméno, příjmení: .....

datum narození: .....

funkce: .....

adresa trvalého bydliště: .....

Zmocněnec[1]:

Jméno a příjmení: *E-mail:* *Adresa trvalého bydliště:*	*Datum narození:* *Rodné číslo:* *Číslo obč. průkazu:* *Číslo sekundárního průkazu:*	*Podpis zmocněnce:*
Jméno a příjmení: *E-mail:* *Adresa trvalého bydliště:*	*Datum narození:* *Rodné číslo:* *Číslo obč. průkazu:* *Číslo sekundárního průkazu:*	*Podpis zmocněnce:*

Zmocnitel tímto uděluje plnou moc všem výše uvedeným zmocněncům (schvalovatelům) k oprávnění k zastoupení při:

- Předkládání a schvalování žádostí o kvalifikované certifikáty pro autentizaci internetových stránek (QWAC) certifikáty.
- Získání digitálního ekvivalentu firemní pečeti, razítka nebo úředního podpisu k vytvoření autenticity firemní webové stránky/stránek.
- Podpisu smlouvy o vydání QWAC certifikátu a podmínek pro používání vydaného QWAC certifikátu.

QWAC a ostatní SSL certifikáty budou vydávány prostřednictvím Registrační autority I.CA umístěné v sídle společnosti I.CA.

Zmocnění dle této plné moci je časově omezené na dobu platnosti rámcové smlouvy a příslušných dodatků.

[1] Zmocněnec nesmí být stejná osoba, která již byla zplnomocněna v Plné moci pro potvrzování periodicity. Doklady zplnomocněných musí být platné minimálně jeden rok.

Plná moc musí být úředně ověřena (notářsky nebo přes Czech POINT) nebo elektronicky podepsána kvalifikovaným elektronickým podpisem dle eIDAS od všech zmocnitelů (musí být uvedeni ve výpisu z obchodního rejstříku) a zmocněnců.

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

.....

jméno a podpis zmocnitele

Informace a postup získání SSL certifikátu

Žadatel zasílá e-mailem soubor žádosti ve formátu PKCS#10 (.req) na e-mailovou adresu [redacted]

- V jejím předmětu musí být uvedeno: *"Žádost o SSL certifikát"*.
- V těle e-mailu 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.

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

Generátor žádosti o QWAC: [redacted]

1. 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

2. Položky žádosti pro certifikát SSL typu QWAC

- 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.

1.1. Rozšíření subjectAlternativeName pro QWAC:

- 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).

3. 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,

- 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, která bude obsahovat náhodný řetězec; kontaktní osoba pošle schválení žádosti obsahující tento řetězec zpět do I.CA,

- 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,

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

Platnost náhodných řetězců je ve všech případech 30 dní.

4. 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,

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

- 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.

5. Obnovení – následný certifikát

Při obnově je vždy nutné zaslat novou žádost o certifikát. Certifikáty se neobnovují, nýbrž se pokaždé vydávají nové 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.

6. Zneplatnění

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

Plná moc pro potvrzovatele periodicity

Zmocnitel (společnost /organizace): .....
se sídlem: ..... IČ: .....

Zastoupená:

jméno, příjmení: .....
datum narození: .....
funkce: .....
adresa trvalého bydliště: .....

Zmocněnec[4]:

Jméno a příjmení:	*Datum narození:*	*Podpis zmocněnce:*
E-mail:	*Rodné číslo:*	
Adresa trvalého bydliště:	*Číslo obč. průkazu:*	
	Číslo sekundárního průkazu:	
Jméno a příjmení:	*Datum narození:*	*Podpis zmocněnce:*
E-mail:	*Rodné číslo:*	
Adresa trvalého bydliště:	*Číslo obč. průkazu:*	
	Číslo sekundárního průkazu:	

Zmocnitel tímto uděluje plnou moc všem výše uvedeným zmocněncům k oprávnění k zastoupení při:

- Potvrzování žádostí zaslaných od První certifikační autority, a.s. k pravidelné roční periodicitě, která potvrzuje navržené schvalovatele v Plné moci pro QWAC certifikáty.
- Oprávnění měnit podle potřeby schvalovatele v Plné moci pro QWAC certifikáty. **ANO/NE[5].**

Zmocnění dle této plné moci je časově omezené na dobu platnosti rámcové smlouvy a příslušných dodatků.

Plná moc musí být úředně ověřena (notářsky nebo přes Czech POINT) nebo elektronicky podepsána kvalifikovaným elektronickým podpisem dle eIDAS od všech zmocnitelů (musí být uvedeni ve výpisu z obchodního rejstříku) a zmocněnců.

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

.....
jméno a podpis zmocnitele

[4]Zmocněnec nesmí být stejná osoba, která již byla zplnomocněna v Plné moci pro SSL certifikáty. Doklady zplnomocněných musí být platné minimálně jeden rok.
[5] Nehodící se škrtněte.