

Smlouva o dodávce certifikátů, časových razítek a certifikačních služeb pro informační systémy MZV

ve smyslu ustanovení § 2586 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů („Občanský zákoník“)

ev. č. objednatele: SM7124-041, č.j. 128130/2024-MZV/ORIKT

Uzavřená mezi:

Česká republika - Ministerstvo zahraničních věcí

Sídlo: Praha 1, Loretánské náměstí 101/5, PSČ 118 00
Zastoupená: , ředitelem odboru informačních a komunikačních technologií (ORIKT)
IČO: 45769851
DIČ: CZ45769851
Bankovní spojení: 
Číslo účtu: 
(dále jen „objednatel“ nebo „MZV“) na straně jedné

a

První certifikační autorita, a.s.

zapsána v obchodním rejstříku Městského soudu v Praze, spisová značka - oddíl B., vložka 7136

Sídlo: Praha 9, Libeň, Podvinný mlýn 2178/6, PSČ: 19000
Zastoupená: , předsedou představenstva a , členem představenstva
IČO: 26439395
DIČ: CZ26439395
Bankovní spojení: 
Číslo účtu: 
(dále jen „poskytovatel“ nebo „I.CA“) na straně druhé

(objednatel a poskytovatel dále též jako „smluvní strana“ nebo společně „smluvní strany“)

uzavírají níže uvedeného dne, měsíce a roku tuto Smlouvu o dodávce certifikátů, časových razítek a certifikačních služeb pro informační systémy MZV (dále jen „Smlouva“).

Preamble

1. MZV jako zadavatel veřejné zakázky malého rozsahu zadané mimo rámec zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, s názvem „Dodávka certifikátů, časových razítek a certifikačních služeb pro IS MZV“, rozhodl o přidělení této veřejné zakázky výše uvedenému poskytovateli.
2. Vztahy výslovně neupravené Smlouvou a jejími přílohami se budou řídit příslušnými ustanoveními Občanského zákoníku.

I. Základní pojmy

MZV – Ministerstvo zahraničních věcí České republiky

I.CA – První certifikační autorita, a.s.

RA – klientská registrační autorita I.CA provozovaná na MZV

CPQC – Certifikační politika I.CA pro kvalifikované certifikáty

CPQEP – Certifikační politika I.CA pro elektronickou pečeť

CPKC – Certifikační politika I.CA pro komerční certifikáty

CPQTSA – Certifikační politika I.CA pro kvalifikovaná časová razítka

Produkt TWINS – společné vydání kvalifikovaného certifikátu a komerčního certifikátu na základě zpracování jedné žádosti

PSQRA – Provozní směrnice pro pracovníky Registračních autorit I.CA pro vydávání kvalifikovaných certifikátů a certifikátů pro elektronickou pečeť

PSKRA – Provozní směrnice pro pracovníky registračních autorit I.CA pro vydávání komerčních certifikátů

ICARA – SW pro Registrační autority I.CA.

Dokumenty I.CA – pro potřeby této Smlouvy včetně všech jejích případných dodatků a příloh se rozumí:

- listinná podoba originálu „Protokolu o podání žádosti na vydání kvalifikovaného certifikátu I.CA“
- listinná podoba originálu „Protokolu o podání žádosti na vydání komerčního certifikátu I.CA“
- listinná podoba originálu „Smlouvy o vydání a používání kvalifikovaného certifikátu“
- listinná podoba originálu „Smlouvy o vydání a používání komerčního certifikátu“
- další dokumenty, které jsou operátoři RA při provozování Registrační autority povinni ukládat v souladu s platnou PSQRA
- listinná podoba originálu „Protokolu o podání žádosti na vydání komerčního certifikátu I.CA nebo komerčního technologického (serverového) certifikátu I.CA“
- listinná podoba originálu „Smlouvy o vydání a používání komerčního certifikátu nebo komerčního technologického (serverového) certifikátu I.CA“
- další dokumenty, které jsou operátoři RA při provozování Registrační autority povinni ukládat v souladu s platnou PSKRA.

ZoEP – Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce (dále jen „Zákon o elektronickém podpisu“ či „ZoEP“).

II.

Účel Smlouvy

1. Účelem této Smlouvy je zajistit vydávání kvalifikovaných certifikátů a poskytování produktu TWINS (dále také „zaměstnanecký kvalifikovaný certifikát“), kvalifikovaných certifikátů pro elektronickou pečeť (dále také „certifikát pro ePečeť“), komerčních certifikátů (dále také „zaměstnanecký komerční certifikát“), komerčních technologických certifikátů (dále také „komerční serverový certifikát“), poskytování kvalifikovaných a archivních kvalifikovaných časových razítek, technických HW nosičů certifikátů, testovacího prostředí, školení, konzultací, technické a metodické podpory, provozu a odborné podpory existujících RA MZV, specializovaných služeb pro provoz IS ePasy a dalších služeb souvisejících s poskytováním certifikačních služeb pro potřeby MZV, plně v souladu s potřebami, záměry a projekty MZV prostřednictvím I.CA, podle zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce (dále jen „Zákon o elektronickém podpisu“ či „ZoEP“). Smlouva umožňuje MZV využívat dodané certifikáty, časová razítka a poskytnuté služby ve všech informačních systémech, které provozuje a kde je použití elektronického podpisu nebo časového razítka relevantní.
2. I.CA prohlašuje, že je od 3. 8. 2017 kvalifikovaným poskytovatelem služeb vytvářejících důvěru v souvislosti s vydáváním kvalifikovaných certifikátů pro elektronické podpisy ve smyslu nařízení Evropského parlamentu a Rady (EU) 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 (dále též „eIDAS“).
3. I.CA prohlašuje, že je od 14. 8. 2017 kvalifikovaným poskytovatelem služeb vytvářejících důvěru pro oblast vydávání kvalifikovaných časových razítek a kvalifikovaných certifikátů pro elektronické pečetě dle eIDAS.
4. I.CA 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, ve znění Nařízení Evropského parlamentu a Rady (EU) 2024/1183 ze dne 11. dubna 2024, kterým se mění nařízení (EU) č. 910/2014, pokud jde o zřízení evropského rámce pro digitální identitu („eIDAS2“) a Zákona o elektronickém podpisu, 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. Služba I.CA RemoteSeal, vzhledem k tomu, že není přímo v nařízení eIDAS definována, nemůže být auditována jako kvalifikovaná služba. Nicméně byla posouzena orgánem dohledu, ministerstvem vnitra, a jeho rozhodnutím čj. MV-68158-6/EG-2018 ze dne 21. června 2018 bylo I.CA povoleno poskytovat službu vytváření kvalifikovaných elektronických pečetí na dálku I.CA RemoteSeal v souladu s politikou této služby a v souladu s technickou a uživatelskou dokumentací zařízení ARX CoSign v8.2 a DocuSign Signature Appliance v8.4. Dále bylo stejným Rozhodnutím povoleno I.CA vydávat kvalifikované certifikáty pro elektronické pečetě podle certifikační politiky vydávání kvalifikovaných certifikátů pro

elektronické pečetě na dálku (algoritmus RSA), verze 1.00 (identifikátor 1.3.6.1.4.1.23624.10.1.38.1.0). Identifikátor této služby byl uveřejněn v důvěryhodném seznamu České republiky u služby „(78) I.CA – vydávání kvalifikovaných certifikátů“ společně s identifikátorem „QCQSCDManagedOnBehalf“ podle kap. 5.5.9.2.3 technických specifikací ETSI TS 119 612 v2.1.1. Důvěryhodný seznam je veden na https://tsl.gov.cz/publ/TSL_CZ.xtsl.

Část první

Vydávání certifikátů a dodávky technických nosičů certifikátů

III.

Předmět Smlouvy

1. Předmětem této Smlouvy je komplexní zajištění certifikačních služeb pro potřeby informačních systémů MZV, což kromě jiného zahrnuje i vydávání zaměstnaneckých kvalifikovaných certifikátů, produktů TWINS, systémových certifikátů, kvalifikovaných certifikátů pro elektronickou pečeť, zaměstnaneckých komerčních certifikátů a komerčních technologických (serverových) certifikátů (dále jen „certifikáty“) podle ZoEP a podle příslušných Certifikačních politik I.CA, tj. Certifikační politiky I.CA pro kvalifikované certifikáty (dále jen „CPQC“), Certifikační politiky I.CA pro kvalifikované certifikáty pro elektronickou pečeť (dále jen „CPQEP“), Certifikační politiky I.CA pro komerční certifikáty (dále jen „CPKC“), jejichž aktuální změny je uvedeno na webu I.CA www.ica.cz. Certifikáty, vydávané podle této Smlouvy, budou vydávány prostřednictvím pracovišť RA MZV. Součástí této Smlouvy jsou také dodávky technických nosičů certifikátů.
2. Zaměstnaneckým kvalifikovaným certifikátem se podle této Smlouvy rozumí certifikát a produkt TWINS, u něhož je kromě totožnosti žadatele ověřován také jeho zaměstnanecký poměr k MZV (dále též „žadatel“), a to předložením „Potvrzení o zaměstnaneckém poměru“ (dále jen „Potvrzení o ZP“), jehož vzor je pro kvalifikovaný certifikát uveden v Příloze č. 1 a pro produkt TWINS uveden v Příloze č. 4 této Smlouvy, podepsaného žadatelem, kterému má být kvalifikovaný certifikát nebo produkt TWINS vydán, a statutárním zástupcem nebo jím pověřenou/zmocněnou osobou (dále jen „pověřená osoba“). Toto Potvrzení o ZP může být po vzájemné dohodě obou smluvních stran nahrazeno pro kvalifikovaný certifikát vytisknutým a řádně podepsaným dokumentem „Žádost o vydání kvalifikovaného certifikátu - Potvrzení o zaměstnaneckém poměru“ (dále jen „Žádost o QC – Potvrzení o ZP“), obsahujícím všechny požadované údaje a naplnění položek podle Přílohy č. 1 této Smlouvy a pro produkt TWINS vytisknutým a řádně podepsaným dokumentem „Žádost o vydání produktu TWINS - Potvrzení o zaměstnaneckém poměru“ (dále jen „Žádost o TWINS – Potvrzení o ZP“), obsahujícím všechny požadované údaje a naplnění položek podle Přílohy č. 4 této Smlouvy. Všechny údaje uvedené ve výše uvedených dokumentech musí být beze zbytku doloženy v souladu s požadavky dle platných Certifikačních politik I.CA.
3. Elektronické žádosti o kvalifikované certifikáty nebo produkt TWINS, vydávané podle této Smlouvy, musí splňovat naplnění položky jedinečného jména O a OU uvedené v Potvrzení o ZP.

4. Kvalifikované certifikáty, kvalifikované certifikáty pro produkt TWINS, komerční certifikáty a komerční technologické (serverové) certifikáty jsou vydávány na Registračních autoritách I.CA, provozovaných na MZV.
5. Údaj položky "OU" je variabilní a její obsah se mění podle zaměstnance, kterému má být kvalifikovaný certifikát nebo produkt TWINS vydán. Obsah položek „O“ a „OU“ musí vždy souhlasit s jejím obsahem, uvedeným v Žádosti o QC – Potvrzení o ZP nebo Žádosti o TWINS – Potvrzení o ZP.
6. Předmětem této Smlouvy je dále vydávání kvalifikovaných certifikátů pro elektronickou pečeť pro potřeby MZV; tyto certifikáty budou vydávány při současném splnění požadavků daných ZoEP a platnou Certifikační politikou pro kvalifikované certifikáty pro elektronickou pečeť a naplněné položky musí být vždy shodné s Žádostí o kvalifikovaný certifikát pro elektronickou pečeť – Potvrzením o ZP v souladu s Přílohou č. 3 této Smlouvy.
7. Zaměstnaneckým komerčním certifikátem se podle této Smlouvy rozumí certifikát ve smyslu Certifikační politiky I.CA pro komerční certifikáty, u něhož je kromě totožnosti žadatele ověřován také jeho zaměstnanecký poměr k MZV (dále též „žadatel“), a to předložením „Potvrzení o zaměstnaneckém poměru“ (dále jen „Potvrzení o ZP“), jehož vzor tvoří Přílohu č. 5 této Smlouvy, podepsaného žadatelem, kterému má být komerční certifikát vydán, a statutárním zástupcem nebo jím pověřenou/zmocněnou osobou (dále jen „pověřená osoba“). Toto Potvrzení o ZP může být po vzájemné dohodě obou smluvních stran nahrazeno vytisknutým a řádně podepsaným dokumentem „Žádost o vydání komerčního certifikátu - Potvrzení o zaměstnaneckém poměru“ (dále jen „Žádost o KC – Potvrzení o ZP“), obsahujícím všechny požadované údaje a naplnění položek podle Přílohy č. 5 této Smlouvy. Všechny údaje uvedené ve výše uvedených dokumentech musí být beze zbytku doloženy v souladu s požadavky dle platných certifikačních politik I.CA.
8. Elektronické žádosti o komerční certifikáty, vydávané podle této Smlouvy, musí splňovat naplnění položky jedinečného jména O a OU uvedené v Potvrzení o ZP.
9. Položka "O" (název organizace) je vždy naplněna zněním O = Ministerstvo zahraničních věcí České republiky.
10. Údaj položky "OU" (název organizační jednotky) je variabilní a její obsah se mění podle zaměstnance, kterému má být komerční certifikát vydán. Obsah položek „O“ a „OU“ musí vždy souhlasit s jejím obsahem, uvedeným v Žádosti o KC – Potvrzení o ZP.
11. Předmětem této Smlouvy je dále vydávání komerčních technologických (serverových) certifikátů pro potřeby MZV; tyto certifikáty budou vydávány při splnění požadavků daných platnou Certifikační politikou pro komerční certifikáty a naplněné položky musí být vždy shodné s Žádostí o KC – Potvrzením o ZP v souladu s Přílohou č. 6 této Smlouvy.

IV.

Pověřené osoby

1. Jednotlivá Potvrzení o ZP podle předcházejícího článku III. jsou jménem MZV oprávněny podepisovat statutární zástupce nebo jím pověřené osoby podle vzoru, který tvoří Přílohu č.

2 této Smlouvy. Podpisové vzory pověřených osob jsou uloženy na pracovištích jednotlivých RA, v I.CA a na MZV.

2. MZV se zavazuje, že vytvoří a předá seznam pověřených osob statutárním zástupcem, včetně jím podepsaného pověření/zmocnění, k vyřizování žádostí o kvalifikovaný zaměstnanecký certifikát, produkt TWINS, kvalifikovaný certifikát pro elektronickou pečeť, zaměstnanecký komerční certifikát a komerční technologický (serverový certifikát) na RA provozovaným na MZV, do I.CA a všem operátorům RA nejpozději 3 dny přede dnem zahájení rutinního provozu registračních autorit tak, aby operátoři RA mohli podle kopií těchto „Pověření/Plných mocí“ (Příloha č. 2) a v nich obsažených podpisových vzorů ověřovat podpisy osob pověřených schvalovat jednotlivá Potvrzení o ZP.
3. Veškeré změny pověření/zmocnění a změny v seznamu pověřených osob dle Přílohy č. 2 této Smlouvy jsou vůči I.CA účinné 3 pracovní dny po doručení jejich písemného oznámení na adresu sídla I.CA, podepsaného oprávněným zástupcem MZV. Písemné oznámení je možné nahradit e-mailovou zprávou podepsanou uznávaným elektronickým podpisem. I.CA obdržení takového oznámení stejnou formou (písemně nebo podepsaným e-mailem) potvrdí.

V.

Závazky MZV

1. MZV se zavazuje při používání certifikátů, vydaných na základě této Smlouvy, dodržovat CPQC, CPQEP a CPKC, platné ke dni nabytí účinnosti této Smlouvy.
2. MZV nese plnou a výlučnou odpovědnost za škody vzniklé v souvislosti s nedodržením CPQC, CPKC a CPQEP, zejména s vyzrazením a zneužitím soukromého klíče žadatele o certifikát. Žadatelem o certifikát podle této Smlouvy se rozumí zaměstnanec MZV, jemuž má být s předchozím souhlasem MZV certifikát vydán.
3. Veškeré změny a doplňky CPQC, CPKC a CPQEP, zaslané I.CA na e-mailovou adresu licence@mzv.gov.cz, jsou vůči MZV účinné okamžikem potvrzení ze strany MZV, které učiní do 3 dnů od jejich předání, aniž by bylo nutné měnit přílohu této Smlouvy. Tyto změny a doplňky však nemají vliv na cenu plnění Smlouvy a nemění předmět plnění.

VI.

Závazky I.CA

1. Kvalifikované certifikáty a produkt TWINS budou vydávány při současném splnění následujících požadavků:
 - a) předložení dokladů totožnosti dle CPQC,
 - b) předání Potvrzení o ZP, jehož součástí je souhlas kvalifikovaný certifikát nebo produkt TWINS vydat, a které je podepsáno osobou pověřenou podle článku IV. a Přílohy č. 2 této Smlouvy toto Potvrzení o ZP podepsat,
 - c) předložení elektronické žádosti o vydání kvalifikovaného certifikátu nebo produktu TWINS, vytvořené postupem uvedeným na internetové stránce I.CA <http://www.ica.cz>, jejíž naplnění položek odpovídá článku III. odst. 3. této Smlouvy a podmínkám ZoEP a platné CPQC.

2. Kvalifikované certifikáty pro elektronickou pečeť budou vydávány při současném splnění požadavků daných ZoEP a platnou CPQEP.
3. Komerční certifikáty budou vydávány při současném splnění následujících požadavků:
 - a) předložení dokladů totožnosti dle CPKC,
 - b) předání Potvrzení o ZP, jehož součástí je souhlas komerční certifikát vydat, a které je podepsáno osobou pověřenou podle článku IV. a Přílohy č. 2 této Smlouvy toto Potvrzení o ZP podepsat,
 - c) předložení elektronické žádosti o vydání komerčního certifikátu, vytvořené postupem uvedeným na internetové stránce I.CA <http://www.ica.cz>, jejíž naplnění položek odpovídá článku III. odst. 8. této Smlouvy a podmínkám Certifikační politiky pro komerční certifikáty.
4. Komerční technologické (serverové) certifikáty budou vydávány při splnění požadavků, daných platnou Certifikační politikou pro komerční certifikáty.
5. I.CA ručí za jedinečnost identifikačních údajů žadatele, uvedených v certifikátech, vydaných podle této Smlouvy.
6. I.CA nebude akceptovat žádosti o vydání kvalifikovaných certifikátů, kvalifikovaných certifikátů pro elektronickou pečeť, produktu TWINS, komerčních certifikátů a komerčních technologických (serverových) certifikátů, které nesplňují naplnění položek žádosti o kvalifikovaný certifikát, kvalifikovaný certifikát pro elektronickou pečeť, produkt TWINS, komerční certifikát a komerční technologických (serverový) certifikát podle této Smlouvy.
7. I.CA se zavazuje poskytovat žadatelům o kvalifikovaný certifikát a produkt TWINS podporu zaručenou CPQC a CPKC, žadatelům o kvalifikovaný certifikát pro elektronickou pečeť podporu zaručenou CPQEP, žadatelům o komerční certifikát a komerční technologických (serverový) certifikát podporu zaručenou CPKC.
8. I.CA se zavazuje zajišťovat provoz vydávání kvalifikovaných certifikátů, produktu TWINS, kvalifikovaných certifikátů pro elektronickou pečeť, komerčních certifikátů a komerčních technologických (serverových) certifikátů na registračních autoritách I.CA, provozovaných MZV, v pracovních dnech od 7:00 hod. do 19:00 hod., v případě využití mobilní Registrační autority I.CA (jedná se o vlastní mobilní RA I.CA) pak v pracovních dnech od 8:00 hod. do 17:00 hod. s SLA 99,9 %. Celková nedostupnost činí 8,76 hodiny za kalendářní rok. Maximální jednorázová doba nedostupnosti činí 30 minut.
9. I.CA se zavazuje vydat certifikát do 20 minut od zahájení procesu vydávání s SLA 99,9 %. Celková nedostupnost činí 8,76 hodiny za kalendářní rok. Maximální jednorázová doba nedostupnosti činí 30 minut.
10. I.CA se zavazuje zveřejňovat na své internetové stránce www.ica.cz seznam zneplatněných kvalifikovaných certifikátů a zneplatněných kvalifikovaných certifikátů pro elektronickou pečeť (dále jen „CRL“) vždy v intervalu ne delším než 12 hodin.

11. I.CA se zavazuje zveřejňovat na své internetové stránce www.ica.cz seznam zneplatněných komerčních certifikátů a zneplatněných komerčních technologických (serverových) certifikátů (dále jen „CRL“) vždy v intervalu ne delším než 24 hodin.
12. I.CA se zavazuje poskytovat MZV specializované služby potřebné při implementaci elektronických podpisů a časových razítek do IS elektronické spisové služby (SPI-3) včetně přístupu k testovacímu prostředí.
13. I.CA se taktéž zavazuje realizovat na vyžádání MZV formou samostatné objednávky speciální požadavky, např. na řešení komunikačního rozhraní, reporting, specifický CRLDP apod. Cena programátorských prací je uvedena v článku VII. této Smlouvy.
14. I.CA se zavazuje poskytovat MZV specializované služby pro provoz Informačního systému ePasy, zahrnující speciální rozhraní k tomuto systému (provozní i testovací), speciální proces obnovy a zneplatňování certifikátů. Popis je uveden v Příloze č. 12. V případě, že dojde v projektu ePasy ke změnám, budou tyto změny promítnuty do nového znění Přílohy č. 12; tato změna musí být učiněna formou písemného dodatku k této Smlouvě. Testovací prostředí je poskytováno zdarma na vyžádání MZV. Součástí řešení zneplatňování certifikátů MZV bude zajištění souhlasu zaměstnanců MZV s poskytnutím hesla o zneplatnění. MZV se zavazuje písemný souhlas svých zaměstnanců získat.

Požadavek bude předáván ze strany MZV do I.CA a bude obsahovat text:

Žádám o zneplatnění certifikátu číslo = xxxxxx.

Heslo pro zneplatnění = yyyyyy

nebo

Zadam o zneplatneni certifikatu cislo = xxxxxx.

Heslo pro zneplatneni = yyyyyy.

15. I.CA se zavazuje zpřístupnit pověřeným osobám MZV on-line aplikaci Správa certifikátů, dostupnou na URL https://bica.ica.cz/cgi-bin/client_portal.cgi, sloužící pro kontrolu a zneplatňování certifikátů MZV s naplněním položky O=Ministerstvo zahraničních věcí České republiky. Autentizace k aplikaci je umožněna výhradně komerčním certifikátem, vydaným I.CA k tomuto účelu zdarma. Počet oprávněných osob, tj. počet autentizačních komerčních certifikátů, není omezen.

VII.

Cenové podmínky vydávání certifikátů, technických nosičů certifikátů a programátorských prací

1. Cena vydání jednoho prvotního kvalifikovaného certifikátu s platností 1 rok činí:
220,- Kč bez DPH + DPH v aktuální zákonné výši, jež k datu podpisu této Smlouvy činí 21%;
cena s DPH k datu podpisu této Smlouvy tak činí 266,20 Kč.
2. Cena vydání jednoho následného kvalifikovaného certifikátu s platností 1 rok činí:
220,- Kč bez DPH + DPH v aktuální zákonné výši, jež k datu podpisu této Smlouvy činí 21%;
cena s DPH k datu podpisu této Smlouvy tak činí 266,20 Kč.

3. Cena vydání jednoho prvotního kvalifikovaného certifikátu pro elektronickou pečeť/systémového certifikátu s platností 1 rok činí:
530,- Kč bez DPH + DPH v aktuální zákonné výši, jež k datu podpisu této Smlouvy činí 21%;
cena s DPH k datu podpisu této Smlouvy tak činí 641,30 Kč.
4. Cena vydání jednoho následného kvalifikovaného certifikátu pro elektronickou pečeť/systémového certifikátu s platností 1 rok činí:
530,- Kč bez DPH + DPH v aktuální zákonné výši, jež k datu podpisu této Smlouvy činí 21%;
cena s DPH k datu podpisu této Smlouvy tak činí 641,30 Kč.
5. Cena vydání jednoho prvotního produktu TWINS s platností 1 rok činí:
280,- Kč bez DPH + DPH v aktuální zákonné výši, jež k datu podpisu této Smlouvy činí 21%;
cena s DPH k datu podpisu této Smlouvy tak činí 338,80 Kč.
6. Cena vydání jednoho následného produktu TWINS s platností 1 rok činí:
280,- Kč bez DPH + DPH v aktuální zákonné výši, jež k datu podpisu této Smlouvy činí 21%;
cena s DPH k datu podpisu této Smlouvy tak činí 338,80 Kč.
7. Cena vydání jednoho prvotního komerčního certifikátu s platností 1 rok činí:
185,- Kč bez DPH + DPH v aktuální zákonné výši, jež k datu podpisu této Smlouvy činí 21%;
cena s DPH k datu podpisu této Smlouvy tak činí 223,85 Kč.
8. Cena vydání jednoho následného komerčního certifikátu s platností 1 rok činí:
185,- Kč bez DPH + DPH v aktuální zákonné výši, jež k datu podpisu této Smlouvy činí 21%;
cena s DPH k datu podpisu této Smlouvy tak činí 223,85 Kč.
9. Cena vydání jednoho prvotního komerčního technologického (serverového) certifikátu s platností 1 rok činí:
570,- Kč bez DPH + DPH v aktuální zákonné výši, jež k datu podpisu této Smlouvy činí 21%;
cena s DPH k datu podpisu této Smlouvy tak činí 689,70 Kč.
10. Cena vydání jednoho následného komerčního technologického (serverového) certifikátu s platností 1 rok činí:
570,- Kč bez DPH + DPH v aktuální zákonné výši, jež k datu podpisu této Smlouvy činí 21%;
cena s DPH k datu podpisu této Smlouvy tak činí 689,70 Kč.
11. Cena za čipovou kartu Starcos bez potisku včetně obslužného SW SecureStore činí
325,- Kč bez DPH + DPH v aktuální zákonné výši, jež k datu podpisu této Smlouvy činí 21%;
cena s DPH k datu podpisu této Smlouvy tak činí 393,25 Kč.
12. Cena za čipovou kartu Starcos s potiskem včetně obslužného SW SecureStore činí

395,- Kč bez DPH + DPH v aktuální zákonné výši, jež k datu podpisu této Smlouvy činí 21%;
cena s DPH k datu podpisu této Smlouvy tak činí 477,95 Kč.

13. Cena za USB čtečku čipových karet/token typu MINILECTOR-S EVO činí:

325,- Kč bez DPH + DPH v aktuální zákonné výši, jež k datu podpisu této Smlouvy
činí 21%; cena s DPH k datu podpisu této Smlouvy tak činí 393,25 Kč.

14. Cena za čipovou kartu Starcos plug-in včetně obslužného SW SecureStore činí

325,- Kč bez DPH + DPH v aktuální zákonné výši, jež k datu podpisu této Smlouvy činí 21%;
cena s DPH k datu podpisu této Smlouvy tak činí 393,25 Kč.

15. Cena za celodenní výjezd mobilní registrační autority I.CA pro vydávání certifikátů v případě
požadavku a na základě objednávky MZV činí

4 000,- Kč bez DPH + DPH v aktuální zákonné výši, jež k datu podpisu této Smlouvy činí
21%; cena s DPH k datu podpisu této Smlouvy tak činí 4.840,- Kč.

16. Cena za programátorské práce při řešení specializovaných služeb vychází z vzájemně
odsouhlaseného odhadu pracnosti a ceny 1 člověkodne práce programátora, jež činí

11 616,- Kč bez DPH + DPH v aktuální zákonné výši, jež k datu podpisu této Smlouvy činí
21%; cena s DPH k datu podpisu této Smlouvy tak činí 14 055,36 Kč.

VIII.

Podmínky vydávání SSL certifikátů

1. SSL certifikáty budou vydávány v souladu s Certifikační politikou pro SSL certifikáty (dále jen "CP SSL"), která je uvedena v Příloze č. 13, 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 této Smlouvy budou vydávány na základě elektronické žádosti o SSL certifikáty, která musí být předem zaslána na e-mailovou adresu ssl@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. 14 této Smlouvy z e-mailové adresy stejné domény, pro kterou bude SSL certifikát vystaven.
4. 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.

5. Technické požadavky, konkrétní postupy a jednotlivá povolená naplnění položek v DV a OV certifikátech jsou detailně uvedeny v Příloze č. 15 Informace a postup získání SSL certifikátu, jenž je součástí této Smlouvy.
6. MZV je povinna vytvářet žádosti o SSL certifikáty v souladu s platnou CP SSL a podle postupů uvedených v Příloze č. 15 této Smlouvy.
7. Pokud zasláná žádost nebude v souladu s CP SSL anebo požadavky uvedenými v Příloze č. 15, vyhrazuje si I.CA právo takovou žádost nepřijmout a nevydat příslušný SSL certifikát.
8. 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.
9. 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. 1 170,07 Kč s DPH
10. 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. 4 900,50 Kč s DPH
11. 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. 8 899,55 Kč s DPH.

Část druhá Registrační autority

IX.

Předmět Smlouvy - Části druhé

1. Předmětem plnění Části druhé této Smlouvy je komplexní zajištění certifikačních služeb pro potřeby MZV, což kromě jiného zahrnuje i dodávku, zřízení a zajištění podmínek provozování RA umístěných na MZV, včetně specializovaných služeb pro provoz Informačního systému ePasy zahrnujících speciální rozhraní k tomuto systému (provozní i testovací).
2. Provoz RA se řídí platnou CPQC, CPQEP a CPKC, jejichž aktuální znění je uvedeno na webu I.CA www.ica.cz a dále platnou Provozní směrnici pro pracovníky Registračních autorit I.CA pro vydávání kvalifikovaných certifikátů a kvalifikovaných certifikátů pro elektronickou pečeť (Dále jen „PSQRA“) a Provozní směrnici pro pracovníky Registračních autorit I.CA pro vydávání komerčních certifikátů a komerčních serverových certifikátů (dále jen „PSKRA“), které jsou uvedeny na webu I.CA <https://rainfo.ica.cz>. Veškeré změny a doplňky uvedených

dokumentů, zaslané I.CA na e-mailovou adresu licence@mzv.gov.cz, jsou vůči MZV účinné okamžikem potvrzení ze strany MZV, které učiní do 3 dnů od jejich předání, aniž by bylo nutné měnit přílohu této Smlouvy.

3. Registrační autority, dříve zřízené na MZV na základě „Smlouvy o dodávce, zřízení a provozu klientské registrační autority pro vydávání certifikátů“, podepsané dne 9. 6. 2009 (č.j. MZV 109764/2009-SZI, ev. č. SM6102-16) a Smlouvy o dodávce certifikátů, časových razítek a certifikačních služeb pro informační systémy MZV, podepsané dne 29. 12. 2022 (č.j. 136456/2022-OICT, ev. č. SM7122-038), zůstávají v provozu za podmínek určených touto Smlouvou.
4. Předmětem plnění této Smlouvy je dále zajištění podpory činnosti pracovišť RA, zajišťovaných pracovníky MZV, a to v souladu s obsahem Přílohy č. 10 této Smlouvy.

X.

Statut RA

1. RA provozované na základě této Smlouvy jsou určeny pro podávání a vyřizování žádostí o všechny typy certifikátů.
2. Žádosti o všechny typy certifikátů, vydávané podle této Smlouvy, musí být vydávány v souladu s příslušnými platnými CPQC, CPQSC a CPKC a musí obsahovat naplnění položek jedinečného jména položky „O = Ministerstvo zahraničních věcí České republiky“.
3. I.CA je dále připravena společně s MZV projednat veškeré další případné potřeby vydávání certifikátů na registračních autoritách, provozovaných pro potřeby MZV, na základě uzavřených dodatků k této Smlouvě zajistit odpovídající podmínky pro vydávání certifikátů plně podle potřeb MZV

XI.

Zřízení a provozování RA

1. I.CA zřídí RA v požadovaném počtu instalací a v místech určených MZV.
2. I.CA poskytne MZV programové vybavení pro všechny zřízené RA a současně poskytuje MZV právo užívání tohoto programového vybavení ve smyslu § 46 zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským, a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, tj. I.CA touto Smlouvou poskytuje MZV nevýhradní, nepřenositelnou a časově neomezenou SW licenci k používanému programovému vybavení RA, včetně práva užívání všech upgrade a update tohoto programového vybavení RA. Na základě výslovné dohody I.CA a MZV je licence poskytována bezúplatně.
3. I.CA poskytne MZV, jako součást registrační autority, nezbytný HW, kterým pro jedno pracoviště registrační autority je:
 - Čtečka čipových karet pro operátory 1 ks
 - Čipová karta operátora 2 ks

- Razítko I.CA 2 ks
- Klientská čtečka 1 ks

Na základě výslovné dohody I.CA a MZV jsou výše uvedené HW součásti RA poskytovány bezúplatně.

Počet registračních autorit, zřizovaných podle této Smlouvy, a jejich umístění bude stanoveno písemnou dohodou mezi I.CA a MZV.

Případné rozšíření počtu registračních autorit, včetně dodání HW součástí, podléhá změně výše uvedené dohody a bude poskytováno bezúplatně. Počet registračních autorit není omezen.

4. I.CA provede do zahájení činnosti RA potřebnou instruktáž pracovníků MZV, odpovědných za provoz RA. Seznam pracovníků MZV - budoucích operátorů RA, dodá MZV v termínu nejméně 3 dny před společně naplánovaným školením operátorů RA MZV.
5. Zřízení a zahájení činnosti registrační autority bude stvrzeno protokolem o předání vybavení registrační autority, který bude podepsán oprávněnými zástupci obou smluvních stran. Předávací protokol připraví I.CA v počtu dvou vyhotovení (I.CA a MZV obdrží po jednom vyhotovení).
6. Předání veškerého HW a SW vybavení registrační autority MZV bude provedeno na základě předávacích a převjímacích protokolů, které připraví I.CA v počtu dvou vyhotovení (I.CA a MZV obdrží po jednom vyhotovení).

XII.

Závazek I.CA

1. I.CA se zavazuje poskytovat MZV potřebné informace pro plnění předmětu této Smlouvy.
2. I.CA se zavazuje na své náklady školit zaměstnance MZV tak, aby byli řádně poučeni a schopni plnit činnosti podle této Smlouvy. Tento závazek zahrnuje i doškolování operátorů či školení nových operátorů.
3. I.CA má právo přístupu do dokumentace RA po dohodě s MZV. Jakýkoli přístup musí být stvrzen písemným protokolem o obsahu přístupu a podepsán oprávněnými zástupci obou smluvních stran.
4. I.CA je oprávněna vydávat nové certifikační politiky, které reflektují vždy současnou právní situaci. I.CA též MZV oznámí, zda změna certifikační politiky vyvolá nutnost nového proškolení operátorů registrační autority.
5. I.CA nebude akceptovat žádosti zaměstnanců MZV, podané z registrační autority směrem k I.CA, které nebudou splňovat naplnění položek žádosti o kvalifikovaný certifikát, kvalifikovaný certifikát pro elektronickou pečeť a žádosti o komerční certifikát včetně komerčních technologických (serverových) certifikátů podle podmínek této Smlouvy.

6. I.CA se zavazuje poskytovat MZV odbornou a metodickou podporu pro chod registrační autority a pomoc pracovníkům registrační autority při řešení reklamací. Na základě výslovné dohody I.CA a MZV jsou odborná a metodická podpora pro chod registrační autority a řešení reklamací poskytovány bezúplatně.
7. I.CA se zavazuje poskytovat MZV technickou podporu a konzultace k vydávání certifikátů a k provozování RA. Na základě výslovné dohody I.CA a MZV jsou technická podpora a konzultace poskytovány bezúplatně.
8. I.CA poskytuje službu technické podpory uživatelů (Helpdesk), řešení nestandardních situací a poradenství související s předmětem této Smlouvy prostřednictvím e-mailové adresy support@ica.cz a telefonu 284 081 930. Součástí technické podpory je aktualizace databáze často kladených dotazů na webové stránce <http://www.ica.cz/Dotazy>. Cena za poskytování technické podpory je již zahrnuta do ceny plnění předmětu této Smlouvy. Podrobnosti technické podpory jsou uvedeny v Příloze č. 10 této Smlouvy.

XIII.

Závazek MZV

1. MZV je povinno postupovat při plnění této Smlouvy s odbornou péčí, podle pokynů I.CA a v souladu s jeho zájmy. MZV je povinno oznámit I.CA všechny okolnosti, které zjistilo při zařizování záležitostí I.CA podle této Smlouvy, které mohou mít vliv na změnu pokynů I.CA. MZV činí tato oznámení písemně. Není-li touto Smlouvou stanoveno jinak, považuje se za písemné oznámení i oznámení učiněné elektronicky, opatřené uznávaným elektronickým popisem zaslaným na elektronickou adresu: licence@mzv.gov.cz.
2. Od pokynů I.CA se může MZV odchýlit, jen je-li to naléhavě nezbytné v zájmu I.CA a MZV nemůže včas získat její souhlas. Ani v těchto případech se však MZV nesmí od pokynů odchýlit, jestliže je to výslovně zakázáno touto Smlouvou nebo obecně závaznými právními předpisy, které upravují předmět činnosti I.CA, jak je popsán v článku II. této Smlouvy.
3. MZV odpovídá I.CA za škodu, která jí vznikne prokazatelným zaviněním MZV v souvislosti s plněním této Smlouvy, s výjimkou takové škody, která vznikne v důsledku nedostatečné informovanosti MZV ze strany I.CA.
4. MZV se zavazuje umožnit svým vybraným zaměstnancům proškolení z hlediska profesních, technických a bezpečnostních požadavků. Tohoto školení se dotčení zaměstnanci musí zúčastnit před zahájením činnosti podle této Smlouvy a dále podle potřeby a požadavků I.CA v termínech odsouhlasených MZV. Školení zajistí a jeho cenu uhradí I.CA.
5. MZV prohlašuje, že bylo seznámeno s právními předpisy upravujícími činnosti, které jsou předmětem této Smlouvy, a to s obecně závaznými právními předpisy, tak i s vnitřními předpisy upravujícími tuto činnost ve společnosti I.CA (zejména s poučením o ochraně osobních údajů klientů I.CA, s pravidly I.CA, s přijímáním, nakládáním a uchováváním dokladů, které je I.CA povinna archivovat v souvislosti s poskytováním služeb certifikační autority). MZV se tímto zavazuje provádět činnosti, které jsou předmětem této Smlouvy, v souladu s výše uvedenými právními předpisy.

6. MZV eviduje seznam osob, odpovědných za provoz RA (dále jen „operátoři RA“). V rámci součinnosti je MZV povinno poskytovat veškeré informace nutné k zajištění provozu RA. Rozsah a forma této součinnosti tvoří Přílohu č. 7 této Smlouvy. MZV je oprávněno změnit seznam osob, odpovědných za provoz RA, a to na základě oficiálního předání seznamu změn operátorů RA I.CA. Noví operátoři budou vždy řádně proškoleni a obdrží potřebné dokumenty pro činnost operátora RA.
7. I.CA vystaví operátorům RA plnou moc podle vzoru, tvořícího Přílohu č. 8 této Smlouvy. Předpokladem vystavení plné moci je podepsané čestné prohlášení pověřené osoby (operátora RA) podle vzoru, tvořícího Přílohu č. 9 této Smlouvy. MZV se zavazuje poskytnout I.CA údaje o operátorech RA v rozsahu: jméno, příjmení, titul, adresa trvalého bydliště, datum narození a rodné číslo. V případě změny osoby oprávněné podepisovat plnou moc podle vzoru, tvořícího Přílohu č. 8, je I.CA povinna tuto skutečnost oznámit MZV. Oprávnění podepisovat plné moci mají v době podpisu této Smlouvy vedle předsedy představenstva společnosti I.CA Ing. Petra Budiše, Ph.D., MBA, v zastoupení Ing. Roman Kučera a Aleš Kapusta, členové představenstva společnosti I.CA.
8. MZV se zavazuje dodržovat při provozu RA platnou CPQC, CPQEP a PSQRA a platnou CPKC a PSKRA. Za škody vzniklé v souvislosti s jejím nedodržením, zejména s vyzrazením a zneužitím soukromého klíče žadatele o certifikát, nese plnou a výlučnou odpovědnost MZV.
9. MZV nese plnou odpovědnost za škody způsobené pracovníky resortu MZV jako operátory RA na RA MZV, jakož i odpovědnost za škody způsobené nesprávným postupem operátorů RA. Nesprávným postupem se rozumí postup v rozporu s platnými právními předpisy a touto Smlouvou, prokazatelné nerespektování pokynů I.CA, nebo zneužití vystavené plné moci.
10. MZV se zavazuje zajistit hardwarové vybavení, na kterém je provozována RA, proti neoprávněnému přístupu, dále pak jeho HW a SW administraci pouze oprávněnou osobou. Konfigurace operačního systému, nasazeného na uvedeném zařízení, bude v souladu s výše uvedenými bezpečnostními požadavky.

XIV.

Cenové podmínky zřízení pracovišť RA, místo a termíny plnění

1. I.CA zřídí a vybaví všechny vzájemně odsouhlasené registrační autority na základě podmínek této Smlouvy u MZV zdarma. Počet registračních autorit není omezen.
2. Místem zřízení RA může být na území České republiky pracoviště v působnosti MZV, které bude uvedeno v dohodě mezi I.CA a MZV podle odst. 3 článku X. této Smlouvy.
3. Dodávka, zřízení, případně změna počtu a umístění RA bude uskutečněno nejpozději do 2 týdnů od podpisu dohody uzavřené podle odst. 3 článku X. této Smlouvy, a to v termínu dohodnutém oběma smluvními stranami. Předpokladem je zaslání seznamu budoucích operátorů RA podle odst. 7 článku XIII. této Smlouvy.

XV.

Ukládání a správa dokumentů I.CA

1. Dokumenty I.CA jsou jejím majetkem.
2. Dokumenty I.CA ukládá a spravuje příslušné pracoviště, na kterém je provozována RA.
3. Dokumenty I.CA musí být uloženy vždy k určenému jedinečnému číslu žádosti o poskytnutí služby ze strany I.CA. Všechny Dokumenty, vztahující se k téže žádosti, musí být uloženy pohromadě.
4. Dokumenty I.CA se ukládají vždy na místě zabezpečeném proti zničení, zneužití nebo odcizení.
5. Na písemnou žádost, podepsanou předsedou představenstva či některým z členů představenstva společnosti I.CA, je RA povinna požadované Dokumenty I.CA neprodleně vyhledat a žadateli poskytnout. Při poskytnutí originálů Dokumentů I.CA pořídí RA jejich kopie, které ověří svými podpisy zaměstnanec I.CA, kterému byl originál vydán, a operátor RA, který originál vydal.
6. Vrácení Dokumentů I.CA, poskytnutých podle odstavce 5 tohoto článku zaměstnancem I.CA, se provede protokolárně. Protokol podepíše zaměstnanec I.CA, který Dokument I.CA vrací, a operátor RA, který Dokument I.CA přijímá. Protokol se pořídí ve dvojím vyhotovení, přičemž každý z předávajících obdrží po jednom.
7. V případě změny zaměstnance I.CA, oprávněného podepisovat žádosti podle odstavce 5 tohoto článku, je I.CA povinna tuto změnu neprodleně písemně oznámit MZV. Oznámení je oprávněn podat pouze předseda představenstva společnosti I.CA.

XVI.

Uložení dokumentů I.CA

1. Doba uložení Dokumentů I.CA činí jeden rok do doby jejich předání oprávněným zaměstnancům I.CA, pokud se obě smluvní strany nedohodnou na kratším intervalu předávání.
2. Předání Dokumentů I.CA operátorem RA se provede protokolárně. Protokol podepíše operátor RA, který Dokumenty I.CA předává, a zaměstnanec I.CA, který Dokumenty I.CA přijímá. Protokol se pořídí ve dvojím vyhotovení, přičemž každý z uvedených zaměstnanců obdrží po jednom.

XVII.

Odpovědnost za ztrátu, zničení nebo zneužití dokumentů I.CA

1. Po dobu, kdy jsou Dokumenty I.CA uloženy u operátorů RA, odpovídá MZV za jejich ztrátu, zničení nebo zneužití.

2. I.CA odpovídá za ztrátu, zničení nebo poškození Dokumentů I.CA v době, po kterou byly Dokumenty I.CA poskytnuty jejímu oprávněnému zaměstnanci podle článku XV. odst. 5 této Smlouvy.

Část třetí

Vydávání kvalifikovaných a archivních kvalifikovaných časových razítek

XVIII.

Předmět Smlouvy – Části třetí

1. Předmětem plnění Části třetí této Smlouvy je komplexní zajištění certifikačních služeb pro potřeby MZV, což kromě jiného zahrnuje i vydávání kvalifikovaných časových razítek a kvalifikovaných časových razítek pod obchodním názvem „archivní“ kvalifikovaná časová razítka (u nichž I.CA zajišťuje ověřitelnost jejich platnosti pomocí uznávané elektronické značky a tím jejich průkaznost a ověřitelnost po dobu 10 let od jejich vydání) pro potřeby všech informačních systémů MZV, v souladu s platnou Politikou vydávání kvalifikovaných časových razítek I.CA, která je vždy v aktuální verzi k dispozici na www.ica.cz. V této souvislosti si I.CA, v rámci zabezpečení služeb TSA, vyhrazuje právo změnit požadavky, týkající se HW a SW vybavení u MZV, a to zejména z důvodu změny legislativy či technologie, které mohou tyto změny či požadavky vyvolat. Změny oznámí I.CA MZV předem v dostatečném časovém předstihu. Obchodní označení služby kvalifikovaných časových razítek je eGov Advance ServicesTSA® a archivních kvalifikovaných časových razítek eGov Advance ServicesATSA®.
2. Kvalifikovaná časová razítka, vydávaná podle této Smlouvy, budou vydávána pouze oprávněnému žadateli. Oprávněným žadatelem se pro účely této Smlouvy rozumí fyzická nebo právnická osoba, která se prokazuje (autentizuje) v elektronické komunikaci platným komerčním certifikátem (či komerčním serverovým certifikátem) I.CA, případně přesně definovanou statickou IP adresou či jménem a heslem. Způsob autentizace žadatelů/informačních systémů MZV pro výdej kvalifikovaných časových razítek je uveden v Příloze č. 11 této Smlouvy.
3. Seznam oprávněných žadatelů, resp. informačních systémů a jim odpovídajících způsobů autentizace podle této Smlouvy, může být v případě potřeby na straně MZV změněn/rozšířen na základě písemné žádosti MZV, podané I.CA. Příslušná změna musí být dostatečně transparentní a musí z ní být patrné, kterých oprávněných žadatelů se týká, případně které oprávněné žadatele MZV požaduje zrušit nebo přidat a k jakému datu. Žádost musí MZV předat I.CA nejpozději 2 pracovní dny před datem požadované změny.

XIX.

Závazky MZV

1. I.CA poskytuje služby podle článku XVIII. odst. 1 v souladu se závazným prohlášením v článku II. této Smlouvy. MZV se zavazuje ve svých projektech, využívajících kvalifikovaná časová

razítka, vydaná na základě této Smlouvy, zabezpečit dodržování platné Certifikační politiky I.CA pro vydávání kvalifikovaných časových razítek (dále jen „CPQTSA I.CA“), jejíž aktuální změny je uvedeno na webu I.CA www.ica.cz. Veškeré změny a doplňky uvedeného dokumentu jsou vůči MZV účinné okamžikem předání změn a doplňků na e-mail adresu: licence@mzv.gov.cz. Tyto změny a doplňky však nemají vliv na cenu plnění Smlouvy a nemění předmět plnění.

XX. Závazky I.CA

1. I.CA se zavazuje MZV jako oprávněnému žadateli o služby časové autority poskytovat danou službu pro jím realizovaná řešení v souladu s platnou CPQTSA I.CA.
2. I.CA se zavazuje poskytovat MZV podporu zaručenou platnou CPQTSA I.CA.
3. I.CA garantuje dostupnost služby časové autority s SLA 99,9 % za běžný kalendářní rok v nepřetržitém režimu 24 hodin denně 7 dní v týdnu (365 x 24) po celou dobu platnosti Smlouvy. Celková nedostupnost tedy činí 0,1 %, tj. 8,76 hodiny za běžný kalendářní rok. Do této doby nejsou zahrnuty plánované a ohlášené odstávky služby (realizované výhradně o víkendech či svátcích), jež je I.CA povinna ohlásit MZV nejméně 7 dní předem. Maximální jednorázová doba nedostupnosti činí 60 minut. I.CA je dále povinna pravidelně kontrolovat, zda je systém vydávání kvalifikovaných časových razítek nakonfigurován podle požadavků ZoEP.
4. I.CA se zavazuje poskytovat MZV statistiky odběru kvalifikovaných časových razítek, a to po jednotlivých uživateliích autentizujících se ke službě odběru kvalifikovaných časových razítek z přístupových míst, definovaných MZV. Počet přístupových míst není omezen.
5. I.CA se zavazuje poskytovat službu kvalifikovaných časových razítek s propustností 20 ks kvalifikovaných časových razítek/s.
6. U kvalifikovaných časových razítek, vydávaných jako archivní, se I.CA zavazuje zajistit ověřitelnost platnosti kvalifikovaného časového razítka pomocí uznávané elektronické značky a tím i jeho průkaznost a ověřitelnost po dobu 10 let od jeho vydání. Ukončení smluvního vztahu odstoupením, výpovědí nebo jiným způsobem se nedotýká doby trvání tohoto závazku I.CA. Výsledek ověření je ukládán v interních systémech I.CA.
7. I.CA se zavazuje poskytnout webovou on-line aplikaci, dostupnou MZV k ověření stavu archivního kvalifikovaného časového razítka, po zadání SN razítka či hash dokumentu.
8. I.CA se dále zavazuje na vyžádání MZV poskytnout dokumenty nutné pro ověření platnosti archivního kvalifikovaného časového razítka dle odstavce 6 tohoto článku:
 - kvalifikovaná časová razítka a data nutná pro jejich ověření,
 - protokol o kvalifikovaných časových razítkách, označený uznávanou elektronickou značkou I.CA, kterou stvrzuje, že kvalifikovaná časová razítka jsou technicky ověřitelná v době podání žádosti o protokol,
 - kompletní strukturu pro potřeby např. soudního znalce.

9. I.CA se taktéž zavazuje:

- zajistit, aby časová razítka jí vydávaná jako kvalifikovaná, obsahovala všechny náležitosti, stanovené příslušnými obecně závaznými právními předpisy,
- zajistit, aby časový údaj vložený do kvalifikovaného časového razítka, odpovídal hodnotě koordinovaného světového času při vytváření kvalifikovaného časového razítka,
- zajistit, aby data v elektronické podobě, která jsou předmětem žádosti o vydání kvalifikovaného časového razítka, jednoznačně odpovídala datům v elektronické podobě obsaženým ve vydaném kvalifikovaném časovém razítku,
- k uplatnění postupů, které jsou v souladu s normou ETSI TS 102 176-1 v aktuální verzi,
- přijmout odpovídající opatření proti padělání kvalifikovaných časových razítek,
- poskytovat na vyžádání třetím osobám podstatné informace o podmínkách pro využívání kvalifikovaných časových razítek, včetně omezení pro jejich použití a informace o tom, zda je, či není akreditována Digitální a informační agenturou; tyto informace lze poskytovat elektronicky.

XXI.

Přerušení poskytování služby

1. I.CA je oprávněna přerušit poskytování služby vydávání kvalifikovaných časových razítek na základě soudního příkazu nebo v případě, že MZV nebude plnit povinnosti, vyplývající z této Smlouvy.
2. Přerušení poskytování služby vydávání kvalifikovaných časových razítek, zde uvedená, budou ukončena bezprostředně poté, co zanikly důvody, které k přerušení poskytování služby vedly.

XXII.

Cenové podmínky

1. Cena za vydání kvalifikovaných časových razítek je stanovena za 1 ks razítka v příslušném objemovém pásmu:

Objemové pásmo množství razítek ks/měsíc	Cena Kč za 1 ks razítka
Do 100	1,40
Do 200	1,25
Do 500	1,20
Do 1.000	1,00
Do 2.000	0,80
Do 5.000	0,72
Do 7.500	0,61
Do 10.000	0,56
Do 20.000	0,55
Do 30.000	0,50
Do 50.000	0,42
Do 100.000	0,36
Do 150.000	0,31
Do 200.000	0,28

Do 250.000	0,232
Do 300.000	0,197
Do 350.000	0,171
Do 400.000	0,153
Do 450.000	0,138
Do 500.000	0,132

2. Cena za vydání archivních kvalifikovaných časových razítek je stanovena za 1 ks razítka v příslušném objemovém pásmu:

Objemové pásmo	množství razítek	Cena Kč za 1 ks razítka
Do 100		2,52
Do 200		2,25
Do 500		2,16
Do 1.000		1,80
Do 2.000		1,44
Do 5.000		1,30
Do 7.500		1,10
Do 10.000		1,00
Do 20.000		0,97
Do 30.000		0,90
Do 50.000		0,76
Do 100.000		0,65
Do 150.000		0,56
Do 200.000		0,50
Do 250.000		0,42
Do 300.000		0,35
Do 350.000		0,30
Do 400.000		0,28
Do 450.000		0,25
Do 500.000		0,24

2. Celková cena bude stanovena jako součin skutečně odebraného počtu kvalifikovaných časových razítek a archivních kvalifikovaných časových razítek v příslušném kalendářním měsíci a ceny bez DPH za 1 ks razítka v příslušném odběrovém pásmu. K ceně bude připočtena DPH podle aktuálně platných předpisů.

Část čtvrtá

Poskytování služby vytváření kvalifikovaných elektronických pečetí na dálku I.CA RemoteSeal

Článek A.I. Předmět Smlouvy – Části čtvrté

1. Předmětem plnění této části Smlouvy je zajištění provozu služby vytváření kvalifikovaných elektronických pečetí na dálku v souladu s platnou Politikou služby vytváření kvalifikovaných elektronických pečetí na dálku, která je vždy v aktuální verzi k dispozici na www.ica.cz. Obchodní označení služby je I.CA RemoteSeal.

Článek A.II. Povinnosti objednatele

1. I.CA poskytuje službu vytváření kvalifikovaných elektronických pečetí na dálku v souladu se závazným prohlášením uvedeným v článku II. odst. 4 Smlouvy. MZV se zavazuje zabezpečit dodržování platné Politiky služby vytváření kvalifikovaných elektronických pečetí na dálku („Politika“).
2. MZV se zavazuje neposkytovat plnění poskytnuté I.CA dalším osobám bez souhlasu I.CA a nezneužívat poskytování služeb I.CA.

Článek A.III. Povinnosti I.CA

1. I.CA poskytuje MZV službu vytváření kvalifikovaných elektronických pečetí na dálku (dále též „I.CA RemoteSeal“) v souladu s nařízením Evropského parlamentu a Rady č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES, ve znění Nařízení Evropského parlamentu a Rady (EU) 2024/1183 ze dne 11.dubna 2024, kterým se mění nařízení (EU) č. 910/2014, pokud jde o zřízení evropského rámce pro digitální identitu („eIDAS2“). Popis služby je uveden v Příloze č. 17 Smlouvy.
2. I.CA se zavazuje poskytovat službu I.CA RemoteSeal v režimu 24/7, tedy 24 hodin denně, 7 dní v týdnu, s SLA 99,5 % a kapacitou alespoň 30 vytvořených pečetí za minutu.
3. I.CA se zavazuje poskytovat:
 - a) technickou podporu při provozu služby, řešení nestandardních situací a poradenství související s předmětem plnění prostřednictvím e-mailové adresy remoteseal@ica.cz a telefonní linky 284 081 930.
 - b) Hotline v rozsahu Po – Pá 8:00 – 17:00 hod. na výše uvedených kontaktech a provozní pohotovost služby v režimu 24/7 na telefonním čísle 731 657 586.
 - c) právní a technickou aktuálnost komponenty pro zajištění komunikace s I.CA, jakož i celou službu I.CA RemoteSeal, s relevantními právními a technickými předpisy a normami v návaznosti na eIDAS.
 - d) za účelem otestování nových verzí služby I.CA RemoteSeal před nasazením do ostrého provozu službu I.CA RemoteSeal v testovacím prostředí s funkcionalitou obdobnou službě I.CA RemoteSeal v ostrém

prostředí, pro testovací prostředí platí SLA 95 % a kapacita 5 vytvořených pečetí za minutu.

4. I.CA garantuje a nese odpovědnost za vytvoření kvalifikované elektronické pečetě pouze za předpokladu, že data nutná k vytvoření pečetě (odesílaná do prostředí I.CA), generovaná komponentou dodanou I.CA, nebyla jakkoliv pozměněna a nebylo s nimi nijak manipulováno.

Článek A.IV.

Smluvní cenové podmínky

1. Cena za poskytování služby I.CA RemoteSeal, tj. za vytvoření kvalifikované elektronické pečetě, bude stanovena podle počtu vytvořených kvalifikovaných elektronických pečetí v daném kalendářním měsíci podle příslušného objemového pásma, a to jako součin „Ceny za 1 ks pečetění Kč bez DPH“ a počtu skutečně vytvořených kvalifikovaných elektronických pečetí v příslušném pásmu dle přiloženého rozpisu za kalendářní měsíc. K této ceně bude připočten paušální poplatek ve výši pro dané množstevní pásmo. K celkové ceně bude připočtena DPH podle aktuálně platných předpisů.

počet pečetění od - do za měsíc	paušální poplatek Kč bez DPH/měsíc	Cena za 1 ks pečetění Kč bez DPH
1 - 100	1 000	4,00
101 - 300	2 000	3,50
301 - 500	3 000	3,00
501 - 1.000	5 000	2,50
1.001 - 3.000	7 000	2,10
3.001 - 5.000	9 000	1,70
5.001 - 10.000	11 000	1,40
10.001 - 30.000	14 000	1,10
30.001 - 50.000	17 000	0,80
50.001 - 100.000	21 000	0,50
100.001 - 300.000	24 000	0,30
300.001 - 500.000	29 000	0,20
500.001 - 1.000.000	35 000	0,16
1.000.001 - 5.000.000	42 000	0,12
5.000.001 - 10.000.000	49 000	0,08

2. Ceny uvedené v odst. 1. tohoto článku jsou cenami neměnnými, nejvýše přípustnými a zahrnují veškeré náklady I.CA související s poskytováním služby I.CA RemoteSeal. Ceny mohou být změněny pouze v souvislosti se změnou daňových předpisů týkající se DPH, a to nejvýše o částku odpovídající této legislativní změně.
3. Úhrada poskytování služby I.CA RemoteSeal bude prováděna vždy jednou měsíčně zpětně za uplynulý kalendářní měsíc, v němž I.CA vytvořila kvalifikované elektronické pečetě, a to podle počtu skutečně provedených a poskytnutých

vytvořených pečetí. Daňový doklad bude obsahovat počet skutečně vytvořených pečetí; cena bude stanovena jako součin „Ceny za 1 pečetění Kč bez DPH“ a počtu skutečně vytvořených pečetí v příslušném pásmu za kalendářní měsíc dle rozpisu uvedeného v odst. 1. tohoto článku A.IV. + paušální poplatek v příslušném pásmu. DPH bude vyjádřena dle aktuálně platné legislativy.

4. I.CA je povinna vystavit řádný daňový doklad do 15. dne kalendářního měsíce následujícího po kalendářním měsíci, za který je účtována cena za poskytování služby I.CA RemoteSeal.
5. MZV je povinno uhradit daňové doklady převodem na účet I.CA do 30 dnů ode dne doručení daňového dokladu, vystaveného I.CA, na adresu sídla MZV a doručeného písemně na adresu sídla MZV podle údajů v této Smlouvě.
6. Daňový doklad musí mít náležitosti daňových a účetních dokladů stanovených platnými a účinnými právními předpisy. MZV je oprávněno daňový doklad, který nebude splňovat náležitosti podle platných a účinných právních předpisů nebo je nesprávně či neoprávněně účtován, 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 MZV neocitá v prodlení. Lhůta splatnosti počíná běžet znovu od opětovného doručení náležitě doplněného či opraveného daňového dokladu.

Článek A.V.

Sankční ustanovení, odstoupení od smlouvy

1. V případě nedodržení parametru SLA dostupnosti služby I.CA RemoteSeal uvedeného v článku A.III. odst. 2. této Smlouvy, tj. pokud dostupnost služby klesne pod 99,5 % za kalendářní den, je I.CA povinna uhradit MZV smluvní pokutu ve výši 1.000,- Kč bez DPH za každých započatých 0,1 %, o kterých klesne dostupnost poskytované služby pod požadovanou hodnotu.
2. V případě nesplnění povinností uvedených v článku A.III. odst. 3. písm. a) a b) této Smlouvy je I.CA povinna uhradit MZV smluvní pokutu ve výši 1.000,- Kč bez DPH za každé takové porušení.
3. V případě nesplnění povinností uvedených v článku A.III. odst. 3. písm. c) této Smlouvy je I.CA povinna uhradit MZV smluvní pokutu ve výši 10.000,- Kč bez DPH za každé takové porušení.
4. Uplatněním smluvní pokuty není dotčen případný nárok na náhradu škody v plné výši za porušení ustanovení, kterého se týká smluvní pokuta.
5. Každá ze smluvních stran má právo odstoupit od Smlouvy v případě, poruší-li jedna ze smluvních stran své závazky a povinnosti stanovené Smlouvou, a to podstatným nebo opakovaným způsobem. Odstoupení musí mít písemnou formu s uvedením důvodů odstoupení a musí být doručeno druhé smluvní straně, jinak je odstoupení neplatné. Odstoupení od Smlouvy má právní účinky dnem doručení. Od toho dne nesmí smluvní strana, které takto bylo odstoupení doručeno, pokračovat v plnění předmětu Smlouvy vyjma případů, kdy by nečinností hrozila újma na jmění druhé smluvní strany. V takovém případě má smluvní strana za povinnost pokračovat v plnění Smlouvy a zabezpečit předmět Smlouvy takovým způsobem, aby bylo odstraněno nebezpečí shora uvedené újmy na jmění. Odstoupení od smlouvy se řídí § 2001 a násl. Občanského zákoníku.

Část pátá

Společná a závěrečná ustanovení

XXIII.

Místo plnění a fakturační místo

1. Místem plnění a fakturačním místem je:

**Ministerstvo zahraničních věcí České republiky
Praha 1, Loretánské náměstí 101/5, PSČ 118 00
Odbor rozvoje informačních a komunikačních technologií (ORIKT)**

XXIV.

Platební podmínky a limit celkové ceny

1. Úhrady dodávek certifikačních služeb budou prováděny měsíčně zpětně za certifikační služby odebrané MZV v předchozím kalendářním měsíci.
2. MZV nebude poskytovat zálohové platby předem na určité období, zboží nebo za služby, které ještě nebyly provedeny a jejich provedení nebylo prokázáno. I.CA je oprávněna fakturovat vždy až na základě potvrzeného dodacího listu, předávacího/akceptačního protokolu nebo výkazu práce či jejich kombinace (podle charakteru dodávky).
3. Daňový doklad (faktura) bude vystaven podle skutečně dodaného objemu certifikačních služeb (zaměstnanecké kvalifikované certifikáty, kvalifikované certifikáty pro elektronickou pečeť, produkty TWINS, zaměstnanecké komerční certifikáty, komerční technologické (serverové) certifikáty, technické nosiče certifikátů, kvalifikovaná časová razítka, archivní kvalifikovaná časová razítka, doprovodné služby) za uplynulý kalendářní měsíc. Datem uskutečnění zdanitelného plnění je poslední den kalendářního měsíce, v němž byly služby poskytnuty a za něž je faktura vystavena.
4. Ceny budou uvedeny s DPH, samostatně DPH včetně sazby DPH a cena bez DPH.
5. Splatnost řádně vystaveného daňového dokladu - faktury, obsahující náležitosti dle § 29 zákona č. 235/2004 Sb., o dani z přidané hodnoty (DPH), ve znění pozdějších předpisů (dále jen „Zákon o DPH“) činí 30 dnů od doručení MZV. Faktura je zaplacená odepsáním příslušné částky z účtu objednatele ve prospěch účtu poskytovatele, uvedeného na faktuře ve shodě s údajem uvedeným v záhlaví této Smlouvy.
6. Překročení smluvených cen, uvedených v člancích VII., XIV. a XXII. této Smlouvy, se nepřipouští – cenu není možné překročit, cena obsahuje veškeré náklady I.CA nutné k realizaci předmětu Smlouvy.
7. Cenu je možné změnit pouze v případě, že dojde v průběhu realizace ke změnám daňových předpisů, upravujících výši DPH, a to v rozsahu aktuální zákonné výše DPH k datu uskutečnění

zdanitelného plnění; taková změna nepodléhá sjednání dodatku dle článku XXXIII. odst. 1 této Smlouvy.

8. Právo fakturovat předmět plnění (jeho část) vzniká po jeho převzetí a potvrzení dodacího listu, předávacího/přejímacího/akceptačního protokolu aj. – dále též jen „dodací doklady“ o dodávce či službě, oprávněným zástupcem MZV v místě plnění.
9. Vystavený daňový doklad/ faktura musí obsahovat ve svém těle nebo v příloze:
 - a) rozpis položek předmětu plnění přesně dle této Smlouvy, resp. přesné a úplné označení předmětu fakturace, s případným uvedením fakturované dílčí etapy plnění, resp. zúčtovacího období,
 - b) faktura musí odpovídat svojí strukturou položek rozdělení dle následujících účetních položek – služby, hardware a software,
 - c) uvedení jednotkových cen jednotlivých položek,
 - d) číselný, popř. písemný identifikátor Smlouvy,
 - e) pokud to z povahy dodávky zboží nebo služeb bude vyplývat, bude na dodacím listu uvedena záruka na poskytnuté zboží a služby,
 - f) k fakturám, kde to z povahy dodávané služby bude vyplývat, musí být přiložen pracovní výkaz, potvrzený oprávněným zástupcem MZV, který u každé vykazované položky bude obsahovat datum, jméno pracovníka I.CA, stručný popis vykonané práce, počet odpracovaných hodin v rozlišení dle prostor MZV, a cenu, která v konečném součtu za pracovní výkaz bude odpovídat ceně uvedené na faktuře,
 - g) u faktur za paušální servisní nebo hotovostní služby musí být explicitně uveden druh/typ služby a dále (buď přímo v těle faktury nebo v příloze) kdo, kdy, v jakém rozsahu službu/servisní zásah provedl, na jakém zařízení a co bylo jeho příčinou, případně, že v zúčtovacím období žádné konkrétní servisní služby poskytnuty nebyly,
 - h) úplné bankovní spojení I.CA, včetně zejména čísla účtu,
 - i) přílohou faktury bude dodací list o převzetí předmětu fakturace ze strany MZV, který musí obsahovat jednoznačné označení dodávky či služby, a to včetně přesných názvů položek, jejich počet, jednotkové ceny, značku (výrobce), typ, výrobní čísla a u nehmotných věcí čísla licencí. Dodací list nebo předávací/akceptační protokol, potvrzený oprávněným zástupcem (přímým uživatelem) MZV, dokládá, že zboží nebo služba byla dodána včas, v požadované kvalitě a ceně podle Smlouvy.
10. Za doručení faktury se považuje den předání faktury do poštovní nebo elektronické evidence MZV, nebo v případě sporu třetí den po jejím doporučeném odeslání ze strany I.CA.
11. V kalendářním roce, v němž je uskutečňováno plnění, musí být faktura doručena MZV nejpozději do 15. 12. za služby odebrané do tohoto data, nedohodnou-li se smluvní strany jinak. Služby odebrané v období 15. – 31. 12. kalendářního roku budou fakturovány na základě faktury – daňového dokladu v únoru následujícího kalendářního roku společně s fakturací služeb odebraných v lednu.
12. MZV má právo fakturu - daňový doklad I.CA před uplynutím lhůty splatnosti vrátit, aniž by došlo k prodlení s její úhradou, obsahuje-li faktura nesprávné údaje, nesprávné náležitosti požadované ve Smlouvě, nebo je jinak neúplná, nedoložená nebo nesprávně či neoprávněně účtovaná, chybí-li na daňovém dokladu – faktuře některá z náležitostí, chybí-li originál dodacího dokladu, nebo obsahuje-li jiné cenové údaje nebo jiný druh či množství předmětu

plnění než dohodnuté ve Smlouvě. Nová lhůta splatnosti v délce 30 dnů počne plynout ode dne doručení opraveného nebo nového daňového dokladu na MZV.

13. Daň z přidané hodnoty bude účtována v souladu se Zákonem o DPH k datu uskutečnění zdanitelného plnění.
14. Platby budou probíhat výhradně v korunách českých a rovněž veškeré cenové údaje budou uvedeny v této měně.
15. Veškeré platební podmínky vychází ze Všeobecných platebních podmínek MZV.
16. Celková cena Smlouvy je limitována částkou 499 474,- Kč (slovy: čtyři sta devadesát devět tisíc čtyři sta sedmdesát čtyři korun českých) bez DPH. Tento cenový limit bude, v souladu s postupnou fakturací ceny podle této Smlouvy, sledovat MZV. V dostatečném předstihu před očekávaným dosažením tohoto cenového limitu zahájí oprávněný zástupce MZV, uvedený v článku XXVI. Smlouvy, jednání se zástupcem I.CA o potřebné změně Smlouvy nebo o jiném způsobu řešení situace.
17. Služby uvedené v článku VII. Cenové podmínky vydávání certifikátů, technických nosičů certifikátů a programátorských prací, odst. 11. až 16., jsou oprávněni jménem MZV objednávat pouze jeho oprávnění zástupci, uvedení v článku XXVI. Smlouvy.
18. V případě, že se poskytovatel stane nespolehlivým plátcem ve smyslu § 106a zákona o DPH, je povinen o tom neprodleně písemně informovat objednatele. Bude-li poskytovatel k datu uskutečnění zdanitelného plnění veden jako nespolehlivý plátcem, objednatel uhradí část ceny odpovídající dani z přidané hodnoty, vzniká-li povinnost k její úhradě, přímo na účet správce daně v souladu s ust. § 109a zákona o DPH. O tuto částku bude ponížena cena plnění a poskytovatel obdrží cenu bez DPH. V případě, že se poskytovatel stane nespolehlivým plátcem ve smyslu tohoto odstavce, má objednatel současně právo od této Smlouvy odstoupit.

XXV.

Dodání předmětu plnění

1. I.CA se zavazuje, že předmět plnění, který navazuje na plnění ze Smlouvy o dodávce certifikátů, časových razítek a certifikačních služeb pro informační systémy MZV, podepsané dne 29. 12. 2022 (č.j. 136456/2022-OICT, ev. č. SM7122-038), bude věcně a právně bezvadný a odpovídající právním předpisům a závazným i doporučujícím normám platným v České republice.
2. Předmět plnění musí vyhovovat bezpečnostním standardům, jejichž použití je obvyklé u obdobných produktů, a musí svou technickou úroveň odpovídat podmínkám MZV v oblasti bezpečnosti a provozu informačních a komunikačních technologií.
3. Před uskutečněním předání předmětu plnění bude I.CA prokazatelně informovat oprávněného zástupce MZV, uvedeného v této Smlouvě, o připravenosti k předání. Datum převzetí musí být stanoveno po projednání s oprávněným zástupcem MZV tak, aby mezi

doručením oznámení o dokončení a datem převzetí uplynulo nejméně pět (5) pracovních dní.

4. Dílčí dodávka předmětu plnění a dílčí fakturace se připouští pouze v případě uvedení této skutečnosti ve Smlouvě.
5. Pokud to není v rozporu s povahou předmětu plnění, musí být ke každému funkčnímu celku přiloženy doklady nutné k jeho převzetí a užívání, návod k použití a případná další nezbytná dokumentace (např. prohlášení o shodě, atesty, prohlášení, že byly použity materiály a technologie v souladu s příslušnými zákony a předpisy, prohlášení o respektování enviromentálních požadavků daných platnými závaznými předpisy). Veškeré dokumenty uvedené v předchozí větě musí být v českém jazyce.
6. Předání předmětu plnění bude doloženo dodacím dokladem podepsaným oprávněným zástupcem MZV v místě plnění.
7. V případě neposkytnutí nezbytné součinnosti MZV lze po vzájemné dohodě prodloužit příslušné dílčí plnění Smlouvy. Dohoda podle předchozí věty musí být písemná a mít formu dodatku k této Smlouvě.

XXVI.

Oprávnění zástupci smluvních stran

1. Oprávněným zástupcem I.CA pro věcná plnění této Smlouvy je:


Podvinný mlýn 2178/6, 190 00 Praha 9
Tel.: 
E-mail: 

2. Oprávněným zástupcem MZV pro věcná plnění této Smlouvy je:


Loretánské náměstí 101/5, 118 00 Praha 1
Tel.: 
E-mail: 

v zastoupení 
Loretánské náměstí 101/5, 118 00 Praha 1
Tel.: 
E-mail: 

3. Změny oprávněných zástupců smluvních stran, uvedených v tomto článku Smlouvy, jsou druhé smluvní straně oprávněni písemně sdělovat pouze předseda představenstva I.CA a ředitel odboru rozvoje komunikačních a informačních technologií MZV (ORIKT).

XXVII.

Odpovědnost za škodu, smluvní pokuty a úrok z prodlení

1. I.CA odpovídá MZV za škodu způsobenou porušením povinností daných touto Smlouvou. I.CA neodpovídá za škodu, která vznikla z důvodu prokazatelně nesprávného nebo neoprávněného využívání certifikačních služeb na straně MZV.
2. I.CA neodpovídá za škodu způsobenou zejména:
 - porušením povinností, plynoucích MZV z této Smlouvy
 - jednáním nebo opomenutím třetí strany, dodávající MZV produkty nebo služby požadované MZV v souvislosti s využíváním certifikačních služeb
 - zaviněním MZV, jeho zaměstnanců, jeho zástupců nebo jeho smluvních partnerů.
3. MZV nese plnou a výlučnou odpovědnost za škody vzniklé v souvislosti s nedodržením CPQC, CPQEP, CPKC a CPQ TSA I.CA.
4. V případě nedodržení SLA 99,9 % pro vydávání certifikátů, uvedeného v článku VI. odst. 7. této Smlouvy, je I.CA povinna uhradit MZV smluvní pokutu ve výši 10.000,- Kč za takové porušení. Za další porušení je I.CA povinna uhradit MZV smluvní pokutu ve výši 20.000,- Kč.
5. V případě nedodržení lhůty vydání certifikátu uvedené v článku VI. odst. 8. této Smlouvy je I.CA povinna uhradit MZV smluvní pokutu ve výši 10.000,- Kč za každé takové porušení a každý jednotlivý případ.
6. V případě překročení nedostupnosti 0,1 % uvedené v článku XX. odst. 3. o více než 2 hodiny za kalendářní rok, je I.CA povinna uhradit MZV smluvní pokutu ve výši 10.000,- Kč. Za každou další hodinu nedostupnosti činí smluvní pokuta 20.000,- Kč.
7. V případě nesplnění propustnosti 20 ks kvalifikovaných časových razítek/s uvedené v článku XX. odst. 5. je I.CA povinna uhradit MZV smluvní pokutu ve výši 10.000,- Kč za každé takové porušení. Za další porušení je I.CA povinna uhradit MZV smluvní pokutu ve výši 20.000,- Kč.
8. V případě nesplnění povinnosti uvedené v článku XX. odst. 6. je I.CA povinna uhradit MZV smluvní pokutu ve výši 50.000,- Kč za takové porušení. Za další porušení je I.CA povinna uhradit MZV smluvní pokutu ve výši 100.000,- Kč.
9. V případě nesplnění povinností uvedených v článku XX. odst. 8. a 9. je I.CA povinna uhradit MZV smluvní pokutu ve výši 10.000,- Kč za každé takové porušení a každý jednotlivý případ.
10. V případě prodlení I.CA s plněním jakýchkoliv dalších povinností, neuvedených v předchozích odstavcích tohoto článku Smlouvy, v termínu vyplývajícím ze Smlouvy či právních předpisů má MZV právo uplatnit vůči I.CA smluvní pokutu ve výši 0,05 % (slovy: pět setin procenta) z celkové ceny měsíčního předmětu plnění včetně DPH za každý i započatý den prodlení.
11. Při nedodržení termínu splatnosti řádně vystavené faktury – daňového dokladu ze strany MZV je I.CA oprávněna požadovat úhradu úroku z prodlení, a to ve výši stanovené na základě § 1802 a 1970 občanského zákoníku podle nařízení vlády č. 351/2013 Sb. za každý den prodlení.

12. V případě, že některá ze smluvních stran poruší některou z povinností, uložených článkem XXVIII. Ochrana informací nebo článkem XXX. Přechod vlastnictví, práva duševního vlastnictví, má druhá smluvní strana právo účtovat smluvní pokutu ve výši 50.000 Kč za každý případ porušení.
13. V případě, že I.CA nedodrží pravidla a závazky, spojené s poskytováním služeb, vyplývající z ustanovení této Smlouvy, a ani po písemné výzvě MZV nezjedná nápravu ve lhůtě stanovené v této výzvě MZV, je I.CA povinna zaplatit MZV jednorázově smluvní pokutu ve výši 5 % z ceny poskytnutých služeb v daném fakturačním období, za každý jednotlivý případ nedodržení uvedených pravidel.
14. V případě, že I.CA nedodrží sjednaný a písemně potvrzený termín, spojený s poskytováním služeb podle této Smlouvy, je I.CA povinna zaplatit MZV jednorázově smluvní pokutu ve výši 2 % z ceny poskytnutých služeb za dané fakturační období, za každý započatý den zpoždění, nejvýše však 20 % z ceny služby v jednotlivém případě. I.CA není povinna zaplatit pokutu podle tohoto odstavce, pokud prokáže, že zpoždění bylo vyvoláno chybějící nebo nedostatečnou součinností ze strany MZV, která byla pro poskytnutí dané služby potřebná.
15. V případě prodlení I.CA s odstraněním vady předmětu plnění nebo nahrazením vadného předmětu plnění shodným předmětem plnění novým, bezvadným ve lhůtě dle článku XXXII. odst. 2., je I.CA povinna uhradit MZV smluvní pokutu ve výši 5.000 Kč (slovy: pět tisíc korun českých) za každý následný den nefunkčnosti poskytované dodávky nebo služby. Den ohlášení problému se nepočítá do doby rozhodné pro určení výše pokuty.
16. Za prokazatelné porušení povinnosti při uložení a správě Dokumentů I.CA na RA je I.CA oprávněna uplatnit vůči MZV náhradu škody, která I.CA v důsledku tohoto porušení vznikla.
17. Náhradu škody podle tohoto článku nelze uplatnit, došlo-li k závadě v důsledku vyšší moci.
18. Při odcizení, ztrátě nebo poškození Dokumentů I.CA v době, kdy byly poskytnuty I.CA, je I.CA povinna na své náklady pořídit duplikáty. MZV je v tomto případě oprávněno uplatnit vůči I.CA náhradu škody, která MZV v důsledku tohoto porušení vznikla.
19. Při odcizení, ztrátě nebo poškození Dokumentů I.CA uložených u operátora RA, je pracoviště RA povinno na své náklady neprodleně pořídit duplikáty.
20. Zaplacením jakékoliv smluvní pokuty, uvedené ve Smlouvě, není dotčeno právo smluvních stran na náhradu způsobené škody v plné výši, vzniklé v souvislosti s plněním předmětu této Smlouvy.
21. I.CA odpovídá MZV v plné výši za veškeré škody, které mu způsobila porušením svých povinností. I.CA odpovídá zejména za škody způsobené porušením ustanovení Smlouvy, škody způsobené jiným protiprávním jednáním a škody vzniklé v důsledku vad plnění. O náhradě škody platí obecná ustanovení občanského zákoníku.
22. Jakákoliv ustanovení, týkající se omezení výše či druhu náhrady škody či limitace sankcí, se nepřipouští.

23. Žádná ze smluvních stran není odpovědná za prodlení svých závazků v rozsahu, v jakém je prodlení způsobeno prodlením s plněním závazků druhé smluvní strany, zejména v případě neposkytnutí požadované součinnosti vymezené ve Smlouvě.
24. Zaplacení smluvní pokuty nezbavuje I.CA povinnosti splnit závazek stanovený Smlouvou.

XXVIII.

Ochrana a poskytování informací

1. Obě smluvní strany se zavazují udržovat v tajnosti a nezpřístupnit třetím osobám důvěrné informace (jak jsou vymezeny níže).
2. Poskytování informací:
Povinnost poskytovat informace podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, není ustanovením tohoto článku XXVII. dotčena, stejně jako poskytování informací kontrolním, policejním, justičním a bezpečnostním orgánům při plnění jejich zákonných oprávnění a povinností.
3. Dále je předmětem této Smlouvy závazek smluvních stran zachovávat mlčenlivost o všech údajích o smluvních stranách či třetích osobách, majících charakter osobních údajů dle ustanovení zák. č. 110/2019 Sb., o zpracování osobních údajů. Smluvní strany jsou si vzájemně rovněž povinny na žádost druhé smluvní strany prokázat způsob, jakým je dodržování povinností stanovených zákonem zajištěno.
4. Smluvní strany budou považovat za důvěrné informace:
 - veškeré informace poskytnuté ze strany MZV I.CA v souvislosti s plněním této Smlouvy
 - informace, na které se vztahuje zákonem uložená povinnost mlčenlivosti MZV
 - veškeré další informace, které MZV označí jako důvěrné ve smyslu § 1730 občanského zákoníku
 - informace jako důvěrné označené, to je informace, které budou při předání nebo zpřístupnění druhé smluvní straně označeny jako „důvěrné“ nebo „důvěrné v obchodním styku“
 - informace, u kterých se z povahy věci dá předpokládat, že se jedná o informace podléhající závazku mlčenlivosti nebo informace o MZV, které by mohly z povahy věci být považovány za důvěrné a které se dozvědí v souvislosti s plněním této Smlouvy.
5. Smluvní strany se zavazují, že nezpřístupní jakékoliv třetí osobě důvěrné informace druhé smluvní strany bez jejího souhlasu, a to v jakékoliv formě, a že podniknou všechny nezbytné kroky k zabezpečení těchto informací. I.CA je povinna zabezpečit veškeré důvěrné informace MZV proti odcizení nebo jinému zneužití. Závazek mlčenlivosti a ochrany důvěrných informací zůstává v platnosti po dobu 5 let po ukončení platnosti této Smlouvy.
6. Obě smluvní strany se zavazují, že budou s důvěrnými informacemi nakládat jako s vlastním obchodním tajemstvím. Smluvní strany nepovažují skutečnosti uvedené v této Smlouvě za obchodní tajemství ve smyslu § 504 občanského zákoníku.
7. Žádná ze smluvních stran není oprávněna důvěrné informace podle této Smlouvy, týkající se druhé smluvní strany, se kterými byla při své činnosti seznámena nebo které při poskytování

služeb získala, využívat v rozporu se zájmy druhé smluvní strany ani pro třetí osoby, a to ani po skončení platnosti této Smlouvy.

8. Smluvní strany jsou povinny vytvářet podmínky pro zabezpečení ochrany informací důvěrného charakteru a jejich ochranu zajistit.
9. Smluvní strany jsou oprávněny využívat důvěrné informace pouze a výhradně pro účely spolupráce vyplývající ze Smlouvy mezi nimi uzavřené.
10. Smluvní strany jsou povinny zabezpečit, že povinnosti vyplývající z této Smlouvy budou dodržovány všemi zaměstnanci, pokud tito zaměstnanci získají nebo jsou jim k dispozici informace důvěrného charakteru.
11. Na základě výše uvedeného se smluvní strany zavazují:
 - neposkytnout důvěrné informace získané v písemné, elektronické či ústní formě třetí straně bez předchozího výslovného písemného souhlasu té smluvní strany, které se informace bezprostředně týká,
 - důvěrné informace nezneužít, nepoužít v rozporu s oprávněnými zájmy druhé smluvní strany ve prospěch svůj nebo třetích osob, a přijmout dostatečná opatření, aby se předešlo nepovolanému užívání důvěrných informací třetí stranou bez předchozího výslovného písemného souhlasu příslušné smluvní strany,
 - poskytovat důvěrné informace výhradně pracovníkům, kteří se podílejí přímo na spolupráci a užití jejích výsledků a pouze k účelům, které jsou v souladu s účelem spolupráce a vedou přímo ke splnění jejích cílů,
 - nekopírovat důvěrné informace ani jiným způsobem je nereprodukovat bez výslovného souhlasu smluvní strany, která je zpřístupnila, kromě užití pro konkrétní, smluvními stranami stanovenou interní potřebu smluvních stran,
 - pokud mají informace, zpřístupněné některou ze smluvních stran smluvní straně druhé, charakter údajů chráněných zákonem č. 110/2019 Sb., o zpracování osobních údajů, je povinností dodržovat zásady tímto zákonem stanovené. Každá ze smluvních stran je rovněž povinna prokázat druhé smluvní straně na její žádost, zda zákonem stanovené povinnosti dodržuje a jakým způsobem je jejich dodržování zajištěno.
12. Důvěrné informace, které budou v souladu s ustanoveními této Smlouvy zpřístupněny druhé smluvní straně „hmotnou formou“ (písemnou, elektronickou apod.), včetně jejich kopií, budou vráceny druhé smluvní straně nebo zničeny, jakmile:
 - bude ukončena spolupráce nebo
 - smluvní strana, která tyto důvěrné informace zpřístupnila, o to požádá.
13. I.CA je povinna zabezpečit veškeré podklady, mající charakter důvěrné informace, poskytnuté jí MZV, proti zcizení nebo jinému zneužití. I.CA se zavazuje, že důvěrné informace užije pouze za účelem plnění Smlouvy. Jiná použití nejsou bez písemného svolení MZV přípustná.
14. I.CA je povinna svého případného subdodavatele a jeho pracovníky, podílející se na plnění předmětu Smlouvy, zavázat povinností mlčenlivosti a respektováním práv MZV nejméně ve stejném rozsahu, v jakém je v tomto závazkovém vztahu zavázána sama a její pracovníci.

15. Povinnost zachovávat mlčenlivost, o níž se hovoří v tomto článku, se nevztahuje na informace:

- které je MZV povinno poskytnout třetím osobám podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů,
- které jsou nebo se stanou všeobecně a veřejně přístupnými jinak, než porušením ustanovení tohoto článku ze strany I.CA,
- které jsou I.CA známy a byly jí volně k dispozici ještě před přijetím těchto informací od MZV,
- u nichž je I.CA schopna prokázat, že jí byly známy ještě před přijetím těchto informací od MZV, avšak pouze za podmínky, že se na tyto informace nevztahuje povinnost mlčenlivosti z jiných důvodů,
- které budou I.CA po uzavření Smlouvy sděleny bez závazku mlčenlivosti třetí stranou, jež rovněž není ve vztahu k nim nijak vázána,
- jejichž sdělení se vyžaduje ze zákona.

16. Za prokázané porušení ustanovení v tomto článku má druhá smluvní strana právo požadovat náhradu takto vzniklé škody.

17. Důvěrné informace zahrnují rovněž veškeré informace získané náhodně nebo bez vědomí MZV a dále veškeré informace získané od jakékoliv třetí strany, které se týkají MZV či plnění Smlouvy.

18. Závazky vyplývající z tohoto článku Smlouvy není I.CA oprávněna vypovědět ani jiným způsobem jednostranně ukončit.

19. MZV neposkytne I.CA utajované informace.

XXIX.

Ochrana osobních údajů

1. Tato Smlouva je současně i smlouvou o zpracování osobních údajů ve smyslu nařízení Evropského parlamentu a Rady (EU) 2016/679, 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 „Obecné nařízení“) a § 34 zákona č. 110/2019 Sb., o zpracování osobních údajů (dále jen „Zákon o zpracování osobních údajů“) a ve smyslu Zákona o elektronickém podpisu.
2. MZV má pro účely ochrany osobních údajů postavení zpracovatele ve smyslu Obecného nařízení a Zákona o zpracování osobních údajů I.CA má pro účely ochrany osobních údajů postavení správce ve smyslu Obecného nařízení a Zákona o zpracování osobních údajů.
3. Podrobné podmínky zpracování osobních údajů jsou uvedeny v Příloze č. 16.

XXX.

Přechod vlastnictví, práva duševního vlastnictví

1. MZV se stává vlastníkem hmotných částí předmětu plnění dnem převzetí předmětu plnění.
2. MZV nabývá práva k užívání předmětu plnění (například licenci k užití počítačového programu) dnem převzetí předmětu plnění ze strany MZV.
3. MZV je oprávněno užívat předmět plnění od data jeho protokolárního převzetí a nebezpečí škody na předmětu plnění přechází na MZV převzetím tohoto plnění. Za užití předmětu plnění podle předchozí věty se však nepovažuje jeho ověřování a testování.
4. I.CA prohlašuje, že předmět plnění dle této Smlouvy je bez právních vad, zejména že není a nebude zatížen žádnými právy třetích osob, z nichž by pro MZV vyplynul jakýkoliv finanční nebo jiný závazek ve prospěch třetí strany nebo které by jakkoliv omezovalo užití předmětu plnění. V případě porušení tohoto závazku je I.CA v plném rozsahu odpovědná za případné následky takového porušení, přičemž právo MZV na případnou náhradu škody a smluvní pokutu zůstává nedotčeno.
5. Ustanovení tohoto článku XXX. zůstávají účinná i po skončení účinnosti této Smlouvy.

XXXI.

Rozhodné právo, řešení sporů

1. Tato Smlouva se řídí právním řádem České republiky.
2. Není-li touto Smlouvou nebo jejími dodatky sjednáno jinak, řídí se vztahy mezi smluvními stranami zákonem č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů a zákonem č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce (zákon o elektronickém podpisu), ve znění pozdějších předpisů.
3. Veškeré spory mezi smluvními stranami vyplývající z této Smlouvy nebo z jejího porušení, ukončení nebo neplatnosti, budou rozhodovány obecnými soudy České republiky.
4. Smluvní strany se zavazují vyvinout maximální úsilí k odstranění vzájemných sporů vzniklých v průběhu plnění této Smlouvy nebo v souvislosti s touto Smlouvou. Všechny spory budou primárně řešeny formou dohody na úrovni odpovědných zástupců, zastupujících smluvní strany ve smluvních záležitostech. Výsledek dohody o řešení sporu musí být zaznamenán písemně. Nedojde-li do 60 dní od začátku jednání odpovědných zástupců k dohodě mezi smluvními stranami, může smluvní strana žalující podat žalobu k místně a věcně příslušnému obecnému soudu. V případě soudního řešení sporů mezi smluvními stranami je místně příslušným soudem Městský soud v Praze, rozhodným je české právo.

XXXII.

Záruční podmínky a sankce za prodlení s odstraněním vady předmětu plnění

1. I.CA poskytuje na předmět plnění specifikovaný ve Smlouvě záruku v délce trvání dvaceti čtyř (24) měsíců ode dne převzetí dokončeného a funkčního předmětu plnění ze strany MZV.

2. I.CA se zavazuje v záruční době bezplatně odstranit vady předmětu plnění do 2 pracovních dnů od prokazatelného nahlášení vady. Lhůta stanovená v předchozí větě platí, pokud není v záručních podmínkách stanovena lhůta kratší. I.CA je povinna vady odstranit opravou, výměnou nebo opětovným provedením vadné části předmětu plnění nebo jiným způsobem stanoveným právními předpisy podle volby MZV. O odstranění vady smluvní strany sepíše protokol.
3. Pokud I.CA vady neodstraní ve lhůtě uvedené v odst. 2 tohoto článku, je MZV oprávněno odstranit vady nebo zajistit služby samo nebo prostřednictvím třetích osob a požadovat o I.CA úhradu nákladů účelně vynaložených v souvislosti s odstraňováním vad. Uplatněním práva podle tohoto článku není dotčeno právo MZV na odstoupení od Smlouvy a náhradu škody.
4. I.CA v rámci záruky odpovídá za to, že předmět plnění bude v souladu s touto Smlouvou a podmínkami stanovenými platnými právními předpisy. I.CA zejména odpovídá za shodu funkčního chování a vlastností předmětu plnění s dodanou dokumentací a akceptačním (nebo dle oboustranné dohody jiným) protokolem a za použitelnost předmětu plnění pro účely vyplývající ze Smlouvy a jejích příloh.
5. I.CA neodpovídá za vady způsobené následujícími okolnostmi:
 - a) nevhodnými zásahy do předmětu plnění, provedenými MZV či třetí stranou nad rámec úprav schválených I.CA či uvedených v dokumentaci předmětu plnění. To se netýká odst. 3. tohoto článku XXXII., jehož znění zůstává ujednáním tohoto bodu a) nedotčeno;
 - b) vlivy změn technického a programového vybavení, které není součástí předmětu plnění, s výjimkou případů, kdy I.CA takové změny schválila nebo kdy takové změny byly uvedeny v dokumentaci předmětu plnění;
 - c) obsluhou ze strany MZV či třetích osob, která je v rozporu s dokumentací předmětu plnění;
 - d) užitím předmětu plnění, které je v rozporu s dokumentací předmětu plnění.
6. Pokud MZV nemůže předmět plnění nebo jeho část pro vady užívat, prodlužuje se záruční doba o dobu od oznámení vad I.CA do jejich úplného odstranění ze strany I.CA., potvrzeného protokolem o odstranění vady.
7. Právy, vyplývajícími z tohoto článku, nejsou dotčena ani omezena práva MZV z odpovědnosti za vady, vyplývající z právních předpisů a této Smlouvy.
8. I.CA nenese odpovědnost za neposkytnutí certifikační služby, za zhoršení kvality poskytovaných služeb a za zpoždění v jejich dodávce, pokud:
 - bude zaviněno jednáním nebo opomenutím MZV, jeho zaměstnanců nebo třetích osob najatých MZV
 - vznikne v průběhu nutné plánované údržby nebo nutné odstávky systémů I.CA, nahlášené MZV nejméně 7 dní před termínem plánované údržby, nebo nutné odstávky v souladu s postupy uvedenými ve Smlouvě
 - bude způsobeno událostmi vyšší moci
 - bude způsobeno přerušením služeb popsaným v článku XXI. Přerušení poskytování služby.

XXXIII.

Změny Smlouvy

1. Smlouvu lze měnit, doplňovat či zrušit před termínem uvedeným v článku XXXVI. odst. 2. této Smlouvy pouze dohodou smluvních stran, a to písemnými dodatky takto označovanými, chronologicky řazenými a číslovanými vzestupnou řadou, podepsanými zástupci smluvních stran, oprávněnými podepsat tuto Smlouvu, a vydanými ve stejném počtu vyhotovení jako tato Smlouva. Jiná ujednání jsou neplatná.

XXXIV.

Ukončení smluvního vztahu

1. Smluvní vztah založený touto Smlouvou lze ukončit výpovědí, písemnou dohodou obou smluvních stran, odstoupením a dalšími způsoby stanovenými právními předpisy.
2. Každá ze smluvních stran je oprávněna tuto Smlouvu vypovědět písemnou výpovědí i bez udání důvodu. V případě výpovědi zaniká smluvní vztah založený Smlouvou uplynutím třetího měsíce následujícího po měsíci, ve kterém byla písemná výpověď doručena druhé smluvní straně.
3. MZV je oprávněno od Smlouvy odstoupit v následujících případech:
 - a) bude rozhodnuto o likvidaci I.CA;
 - b) I.CA podá insolvenční návrh jako dlužník, insolvenční návrh podaný proti I.CA bude zamítnut pro nedostatek majetku, bude rozhodnuto o úpadku I.CA nebo bude ve vztahu k I.CA vydáno jiné rozhodnutí s obdobnými účinky;
 - c) I.CA bude odsouzena za úmyslný trestný čin;
 - d) I.CA byla odebrána akreditace, která je pro výkon certifikačních služeb vyžadována zákonem.
4. Za podstatné porušení Smlouvy ze strany I.CA, které je důvodem pro odstoupení od Smlouvy ze strany MZV, se považuje zejména:
 - a) prodlení I.CA s dodáním předmětu plnění o více jak 5 kalendářních dní po termínu plnění;
 - b) neplnění závazků, zejména nedodržení termínů plnění nebo nefunkčnost poskytovaných služeb po dobu delší než 5 dnů;
 - c) porušení povinnosti I.CA odstranit vady předmětu plnění ve lhůtě 5 kalendářních dní od jejich oznámení ze strany MZV;
 - d) realizace předmětu Smlouvy v rozporu se Smlouvou či právními předpisy;
 - e) porušení povinností uvedených v článku XXVIII. Ochrana informací;
 - f) nedodržování jiných závazných dokumentů či předpisů ze strany I.CA (zejména předpisů upravujících bezpečnost a ochranu zdraví při práci, požární bezpečnost apod.);
 - g) jiné porušení povinností ze strany I.CA, které nebude odstraněno ani do 10 kalendářních dní od doručení výzvy MZV.

5. Za podstatné porušení Smlouvy ze strany MZV, které je důvodem pro odstoupení od Smlouvy ze strany I.CA, se považuje:
 - a) prodlení MZV s úhradou faktury – daňového dokladu o více jak 30 kalendářních dní po lhůtě splatnosti, přičemž nárok na úrok z prodlení není tímto ustanovením dotčen;
 - b) prodlení MZV s poskytnutím součinnosti o více než 30 kalendářních dní od prokazatelného doručení písemné výzvy ze strany I.CA.
6. V případě odstoupení podle odst. 4. písm. a), b), d) či e) tohoto článku XXXIV., je po marném uplynutí příslušné lhůty MZV oprávněno od Smlouvy jednostranně odstoupit, a to bez jakýchkoliv sankcí ze strany I.CA.
7. MZV je v případě odstoupení od Smlouvy oprávněno podle své volby buď odstoupit od Smlouvy jako celku nebo odstoupit pouze od části Smlouvy, která bude v době odstoupení nesplněna. V případě částečného odstoupení od Smlouvy se cena díla snižuje o částky připadající na plnění, která v důsledku odstoupení I.CA není povinna provést či poskytnout. V případě úplného či částečného odstoupení od Smlouvy je I.CA povinna vrátit MZV cenu díla (byla-li již uhrazena) sníženou o hodnotu plnění, která nejsou dotčena odstoupením.
8. MZV má v případě odstoupení od Smlouvy (kromě jiného) nárok na náhradu škody spočívající v náhradě prokazatelných nákladů, které mu vzniknou v souvislosti se zajištěním náhradního plnění.
9. Oznámení o jednostranném odstoupení od této Smlouvy (dále jen „oznámení“) musí být učiněno písemně a doručeno druhé smluvní straně. Musí obsahovat důvody odstoupení s odkazem na ustanovení Smlouvy, která byla porušena. Oznámení musí dále obsahovat přeměřenou lhůtu k nápravě uvedených nedostatků, která nebude kratší než 15 (patnáct) kalendářních dnů. Pokud nebudou nedostatky uvedené v oznámení ve stanovené lhůtě odstraněny a smluvní strany se nedohodnou jinak, nabývá odstoupení od Smlouvy účinnosti dnem následujícím po marném uplynutí lhůty k nápravě nedostatků, uvedené v oznámení.
10. Práva smluvních stran vzniklá před platným odstoupením od Smlouvy nejsou odstoupením dotčena.
11. V případě částečného odstoupení od této Smlouvy zůstává tato Smlouva v platnosti ohledně těch částí díla, které nejsou dotčeny odstoupením.
12. V případě částečného odstoupení od této Smlouvy ze strany MZV je I.CA povinna do 5 pracovních dnů od prokazatelného doručení odstoupení předat MZV ty části díla, které nebyly dotčeny odstoupením, včetně případných zdrojových kódů a dalších podkladů nezbytných k dokončení díla ze strany MZV či třetími osobami.
13. V případě částečného odstoupení od této Smlouvy má MZV právo dokončit dílo samo nebo prostřednictvím jí určené osoby a je oprávněno použít za tímto účelem veškeré části díla, které nebyly dotčeny odstoupením.
14. Smluvní vztah skončí dnem doručení oznámení o odstoupení od Smlouvy druhé smluvní straně, nebo dnem uvedeným v oznámení.

15. Odstoupení od této Smlouvy či jiné ukončení smluvního vztahu založeného touto Smlouvou se nedotýká nároku na náhradu škody, smluvních pokut, ochrany neveřejných informací, zajištění pohledávky kterékoliv ze smluvních stran, řešení sporů a ustanovení týkající se těch práv a povinností, z jejichž povahy toto vyplývá.
16. V případě jednostranného odstoupení od Smlouvy podle tohoto článku má každá ze smluvních stran nárok na úhradu závazků, vzniklých před doručením oznámení, z ceny prokazatelně poskytnutého plnění. MZV má kromě toho nárok na úhradu prokazatelně vynaložených nákladů na náhradní řešení.

XXXV.

Zvláštní podmínky

1. I.CA se zavazuje, že v případě ukončení smluvního vztahu zajistí technickou podporu:
 - a) vydaných certifikátů minimálně po dobu jejich platnosti,
 - b) vydaných archivních kvalifikovaných časových razítek, včetně zajištění jejich přerazítkování, aby bylo možno plně ověřit jejich platnost po dobu 10 let ode dne jejich vydání.

XXXVI.

Závěrečná ustanovení

1. Smlouva nabývá platnosti dnem podpisu Smlouvy poslední smluvní stranou. Smlouva nabývá účinnosti dnem uveřejnění v registru smluv podle zákona č. 340/2015 Sb., o registru smluv, ve znění pozdějších předpisů, nejdříve však dne 1. 1. 2025. Uveřejnění Smlouvy zajistí objednatel.
2. Tato smlouva se uzavírá na dobu určitou do 31. 12. 2026, nejdéle však do vyčerpání celkové ceny Smlouvy dohodnuté v článku XXIV. odst. 16., nedojde-li dodatkem ke Smlouvě k jinému ujednání.
3. Zánikem Smlouvy není MZV zbaveno povinnosti vyrovnat veškeré závazky vzniklé v důsledku provozu RA a učinit veškeré úkony, které nesou odkladu a které jsou nutné k zabránění vzniku škody na straně I.CA.
4. Dnem účinnosti této Smlouvy končí platnost všech smluv uzavřených mezi MZV a I.CA a nahrazují se touto Smlouvou. Pro vypořádání závazků ze zrušených smluv se použije ustanovení odst. 3. tohoto článku XXXVI. Smlouvy.
5. Ustanovení článku XXXV. odst. 1. této Smlouvy se vztahuje na všechny certifikáty vydané I.CA pro MZV před účinností této Smlouvy.
6. Ustanovení této Smlouvy se dnem její účinnosti vztahují i na RA zřízené I.CA a provozované na MZV před účinností této Smlouvy.

7. I.CA se zavazuje, že jakékoli plánované odstávky systému certifikačních služeb budou prováděny pouze a výhradně mimo pracovní dobu MZV, tj. v nočních hodinách o víkendech či svátcích.
8. I.CA není oprávněna postoupit práva ani převést povinnosti vyplývající z této Smlouvy na třetí osobu bez předchozího písemného souhlasu MZV. Započtení vzájemných pohledávek se vylučuje.
9. V případě, že by některé ustanovení této Smlouvy bylo z jakýchkoliv důvodů neplatné či neúčinné, nezpůsobuje tato skutečnost neplatnost ani neúčinnost ostatních částí Smlouvy. Smluvní strany se zavazují nahradit po vzájemné dohodě dotčené ustanovení jiným ustanovením, blízcím se svým obsahem nejvíce účelu neplatného či neúčinného ustanovení.
10. Práva a závazky z této Smlouvy přecházejí na právní nástupce smluvních stran jen s předchozím písemným souhlasem druhé smluvní strany.
11. Tato Smlouva je uzavírána elektronicky a bude opatřena elektronickými podpisy oprávněných zástupců obou smluvních stran uvedených v záhlaví této Smlouvy.
12. Tato Smlouva představuje úplnou dohodu smluvních stran ohledně vzájemných vztahů, které upravuje, a nahrazuje veškerá předcházející ujednání a dohody v této předmětné věci, ať už ústní či písemné.
13. V případě rozporu Smlouvy a jejích příloh mají vždy přednost ustanovení Smlouvy.
14. Seznam příloh této Smlouvy:
 1. VZOR „Potvrzení o zaměstnaneckém poměru“ pro kvalifikovaný certifikát
 2. VZOR „Plná moc“
 3. VZOR „Žádost o vydání kvalifikovaného certifikátu pro elektronickou pečeť (systémového certifikátu) – plná moc“
 4. VZOR „Potvrzení o zaměstnaneckém poměru“ pro produkt TWINS
 5. VZOR „Potvrzení o zaměstnaneckém poměru“ pro komerční certifikát
 6. VZOR „Žádost o vydání komerčního serverového certifikátu – plná moc“
 7. Součinnost I.CA a osob odpovědných za provoz RA (operátorů RA)
 8. VZOR „Plná moc“ (operátora RA)
 9. VZOR „Prohlášení“ (čestné prohlášení operátora RA)
 10. Zajištění podpory pro činnost pracovišť RA, provozovaných pro potřeby MZV
 11. Způsoby autentizace žadatelů/informačních systémů MZV pro výdej kvalifikovaných časových razítek
 12. Popis projektu ePasy
 13. Certifikační politika pro SSL certifikáty
 14. VZOR „Potvrzení o zaměstnaneckém poměru – plná moc“
 15. Informace a postup získání SSL certifikátu
 16. Podmínky zpracování osobních údajů
 17. Popis služby vytváření kvalifikovaných elektronických pečetí na dálku.

V Praze dne

Za I.CA:



předseda představenstva



člen představenstva

V Praze dne

Za MZV:



ředitel odboru rozvoje informačních
a komunikačních technologií
(ORIKT)

(VZOR)
Potvrzení o zaměstnaneckém poměru

Tímto potvrzujeme, že pan/paní

.....,

R.Č.

Č. OP

je k dnešnímu dni naším zaměstnancem.

Název: **Česká republika - Ministerstvo zahraničních věcí**
Adresa: Loretánské náměstí 101/5, Praha 1, PSČ 118 00
IČO: 45769851

Souhlasíme s tím, aby mu/jí byl společností První certifikační autorita, a.s. vydán kvalifikovaný zaměstnanecký certifikát s uvedením názvu naší společnosti.

V položce „O“ žádosti o kvalifikovaný certifikát pro zaměstnance bude uvedeno:

O = Ministerstvo zahraničních věcí České republiky

V položce „OU“ žádosti o kvalifikovaný certifikát pro zaměstnance bude uvedeno:

OU = osobní číslo zaměstnance MZV ČR

V položce „E-mail“ žádosti o kvalifikovaný certifikát pro zaměstnance bude uvedeno:

E-mail = jmeno_prijmeni@mzv.gov.cz

Vdne

.....
jméno a funkce
pověřené osoby k jednání za
Ministerstvo zahraničních věcí ČR

.....
podpis zaměstnance

Příloha č. 2

(VZOR) Plná moc

Zmocnitel (organizace): Česká republika – Ministerstvo zahraničních věcí

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

IČO: 45769851

jednající

Jméno, příjmení:....., funkce

tímto pověřuje / uděluje plnou moc všem níže uvedeným pověřeným osobám / zmocněncům k vyřizování žádostí o vydání certifikátů a s nimi spojených agend na Registračních autoritách I.CA (První certifikační autorita, a.s.), provozovaným na MZV, v rozsahu:

- samostatné jednání za MZV ve vztahu ke schvalování výdeje certifikátů, včetně podpisu příslušných dokumentů např. „Potvrzení o zaměstnaneckém poměru“ zaměstnancům výše uvedené organizace,
- podpis žádosti o zneplatnění certifikátu,
- podání žádosti o komerční technologický (serverový), kvalifikovaný certifikát pro elektronickou pečeť (systémový certifikát) včetně následných certifikátů.

Jednající pověřené osoby / zmocněnci souhlasí s písemným i elektronickým zpracováním uvedených osobních údajů pro výše uvedené činnosti.

Pověřená osoba / Zmocněnec:

(podpisový vzor)

<i>Jméno a příjmení :</i>	<i>Datum narození:</i>	<i>Podpis pověřené osoby / zmocněnce:</i>
<i>Adresa trvalého bydliště:</i>	<i>Rodné číslo:</i>	
<i>Jméno a příjmení :</i>	<i>Datum narození:</i>	<i>Podpis pověřené osoby / zmocněnce:</i>
<i>Adresa trvalého bydliště:</i>	<i>Rodné číslo:</i>	

Tato plná moc má účinnost do dne jejího odvolání

Vdne.....

.....
jméno a příjmení statutárního zástupce
funkce statutárního zástupce

Příloha č. 3

(VZOR)

Žádost o vydání Certifikátu pro elektronickou pečeť - plná moc

Tímto žádám o vydání certifikátu pro elektronickou pečeť (dále jen „certifikát“) s následujícím vyplněním položek:

Jméno certifikátu - položka „CN“:

Název organizace - položka „O“: **Ministerstvo zahraničních věcí České republiky**

IČO: 45769851

Název organizační jednotky - položka "OU:

E-mailová adresa - položka „E-mail“:

Název domény

Účel použití certifikátu

K realizaci žádosti určuji níže uvedeného zmocněnce.

Datum

Jméno a funkce a organizační útvar,
žadatele o certifikát

Podpis

Plná moc

Níže podepsaný zmocnitel dává tímto plnou moc **zmocněnci**

Jméno, příjmení.....Titul

Adresa trvalého bydliště:.....

Datum narození:.....

Rodné číslo:.....

Číslo OP:.....

Osobní číslo

k těmto úkonům souvisejícím s poskytnutí služeb I.CA, a.s.:

- podat žádost o výše uvedený certifikát a tento certifikát převzít*)
- podat žádost o následný certifikát*)
- podat žádost zneplatnění certifikátu*)

Osoba oprávněná jednat za organizaci – funkce - Zmocnitel:

Název organizace: Ministerstvo zahraničních věcí ČR

IČO:45769851

Sídlo organizace: Loretánské náměstí 101/5, Praha 1, PSČ 118 00

Jméno, příjmení.....titul

Adresa trvalého bydliště:.....

Datum narození.....rodné číslo..... osobní číslo

Prohlašuji tímto, že výše uvedená doména je přidělena k používání organizaci uvedené v položce „O“ **Tato plná moc má účinnost do:**.....

Vdne

.....	
Podpis zmocnitele (Osoba oprávněná povolit výdej certifikátu podle podpisového vzoru na plné moci vydané statutárním orgánem)	Podpis zmocněnce (Osoba oprávněná podat žádost na RA)

*) Nehodící se škrtněte

Příloha č. 4

(VZOR) Potvrzení o zaměstnaneckém poměru

Tímto potvrzujeme, že pan/paní

.....,

R.Č.

Č. OP

je k dnešnímu dni naším zaměstnancem.

Název: Česká republika - Ministerstvo zahraničních věcí
Adresa: Loretánské náměstí 101/5, Praha 1, PSČ 118 00
IČO: 45769851

Souhlasíme s tím, aby mu/jí byl společností První certifikační autorita, a.s. vydán produkt TWINS s uvedením názvu naší společnosti.

V položce „O“ žádosti o produkt TWINS pro zaměstnance bude uvedeno:

O = Ministerstvo zahraničních věcí České republiky

V položce „OU“ žádosti o produkt TWINS pro zaměstnance bude uvedeno:

OU = osobní číslo zaměstnance MZV ČR

V položce „E-mail“ žádosti o produkt TWINS pro zaměstnance bude uvedeno:

E-mail = jmeno.prijmeni@mzv.gov.cz

Vdne

.....
jméno a funkce
pověřené osoby k jednání za
Ministerstvo zahraničních věcí ČR

.....
podpis zaměstnance

Příloha č. 5

(VZOR) Potvrzení o zaměstnaneckém poměru

Tímto potvrzujeme, že pan/paní

.....,

R.Č.

Č. OP

je k dnešnímu dni naším zaměstnancem.

Název: Česká republika - Ministerstvo zahraničních věcí
Adresa: Loretánské náměstí 101/5, Praha 1, PSČ 118 00
IČO: 45769851

Souhlasíme s tím, aby mu/jí byl společností První certifikační autorita, a.s. vydán zaměstnanecký
komerční certifikát s uvedením názvu naší společnosti.

V položce „O“ žádosti o komerční certifikát pro zaměstnance bude uvedeno:

O = Ministerstvo zahraničních věcí České republiky

V položce „OU“ žádosti o komerční certifikát pro zaměstnance bude uvedeno:

OU = osobní číslo zaměstnance MZV ČR

V položce „E-mail“ žádosti o komerční certifikát pro zaměstnance bude uvedeno:

E-mail = jmeno.prijmeni@mzv.gov.cz

Vdne

.....
jméno a funkce
pověřené osoby k jednání za
Ministerstvo zahraničních věcí ČR

.....
podpis zaměstnance

Příloha č. 6

(VZOR)

Žádost o vydání komerčního technologického (serverového) certifikátu - plná moc

Tímto žádám o vydání komerčního technologického (serverového) certifikátu (dále jen „certifikát“)
s následujícím vyplněním položek:

Jméno certifikátu - **položka „CN“**:

Název organizace - **položka „O“**: **Ministerstvo zahraničních věcí České republiky**
IČO: 45769851

Název organizační jednotky - **položka „OU“**:

E-mailová adresa - **položka „E-mail“**:

Název domény

Účel použití certifikátu

K realizaci žádosti určuji níže uvedeného zmocněnce.

Datum

.....
Jméno a funkce a organizační útvar,

.....
Podpis žadatele o certifikát

Plná moc

Níže podepsaný zmocnitel dává tímto plnou moc **zmocněnci**

Jméno, příjmení.....Titul

Adresa trvalého bydliště:.....

Datum narození:.....

Rodné číslo:.....

Číslo OP:.....

Osobní číslo

k těmto úkonům souvisejícím s poskytnutí služeb I.CA, a.s.:

- podat žádost o výše uvedený certifikát a tento certifikát převzít*)
- podat žádost o následný certifikát*)
- podat žádost zneplatnění certifikátu*)

Osoba oprávněná jednat za organizaci – funkce - Zmocnitel:

Název organizace: Ministerstvo zahraničních věcí ČR

IČO:45769851

Sídlo organizace: Loretánské náměstí 101/5, Praha 1, PSČ 118 00

Jméno, příjmení.....titul

Adresa trvalého bydliště:.....

Datum narození.....rodné číslo..... osobní číslo

Prohlašuji tímto, že výše uvedená doména je přidělena k používání organizaci uvedené v položce „O“

Tato plná moc má účinnost do:.....

Vdne

.....	
Podpis zmocnitele (Osoba oprávněná povolit výdej certifikátu podle podpisového vzoru na plné moci vydané statutárním orgánem)	Podpis zmocněnce (Osoba oprávněná podat žádost na RA)

*) Nehodící se škrtněte

Součinnost I.CA a osob odpovědných za provoz RA (operátorů RA)

I. Úvod

První certifikační autorita, a.s. (dále jen „provozovatel“ nebo „I.CA“) uzavírá s Ministerstvem zahraničních věcí České republiky (dále jen „MZV“ nebo „vykonavatel“) smlouvu, na základě které bude MZV provozovat registrační autority, vydávající v ní uvedené typy certifikátů.

MZV pověřilo osoby odpovědné za provoz RA (dále jen „operátor RA“), které budou v rámci služeb I.CA zajišťovat fungování této registrační autority, vykonáváním následujících činností:

- přijímání žádostí o kvalifikované certifikáty a kvalifikované certifikáty pro elektronickou pečeť
- ověřování totožnosti žadatelů o kvalifikované certifikáty a o kvalifikované certifikáty pro elektronickou pečeť v souladu s platnou Certifikační politikou I.CA pro kvalifikované certifikáty (dále jen „CPQC“), Certifikační politikou I.CA pro kvalifikované certifikáty pro elektronickou pečeť (dále jen „CPQEP“) a Provozní směrnici pro pracovníky Registračních autorit I.CA vydávajících kvalifikované certifikáty a kvalifikované certifikáty pro elektronickou pečeť (dále jen „PSQRA“),
- vydávání kvalifikovaných certifikátů a vydávání kvalifikovaných certifikátů pro elektronickou pečeť
- přijímání žádostí o komerční certifikáty a komerční technologické (serverové) certifikáty
- ověřování totožnosti žadatelů o komerční certifikáty a o komerční technologické (serverové) certifikáty v souladu s platnou Certifikační politikou I.CA pro komerční certifikáty (dále jen „CPKC“) a Provozní směrnici pro pracovníky Registračních autorit I.CA vydávajících komerční certifikáty a komerční technologické (serverové) certifikáty (dále jen „PSKRA“),
- vydávání komerčních certifikátů a vydávání komerčních technologických (serverových) certifikátů
- ostatní s tím související činnosti.

II. Práva a povinnosti vykonavatele

Vykonavatel je oprávněn:

1. obdržet od provozovatele školení, metodické materiály a další dokumenty pro činnost podle této smlouvy,
2. požadovat po provozovateli další nezbytné informace a konzultace,
3. obdržet od provozovatele potřebné softwarové a speciální hardwarové vybavení.

Vykonavatel je povinen:

1. dodržovat platnou CPQC, CPQEP, CPKC a platnou PSQRA a PSKRA.

2. řídit se pokyny provozovatele.

III.

Práva a povinnosti provozovatele

Provozovatel je oprávněn:

1. požadovat od vykonavatele dodržování platné CPQC, CPQEP, CPKC, PSQRA a PSKRA a upozornit jej na zjištěné nedostatky a požadovat v přiměřené lhůtě nápravu,
2. provádět u vykonavatele kontrolu věcného plnění této smlouvy.

Provozovatel je povinen:

1. poskytnout vykonavateli školení, nezbytné pro jeho činnost, metodické materiály a další nezbytné dokumenty,
2. poskytnout vykonavateli na jeho vyžádání další potřebné informace a konzultace.

(VZOR)
PLNÁ MOC

První certifikační autorita, a.s.

Se sídlem Praha 9, Podvinný mlýn 2178/6 PSČ 190 00,

IČO: 264 39 395

DIČ: CZ264 39 395

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

Jednající svým Ing. Petrem Budišem, Ph.D., MBA, předsedou představenstva

t í m t o u d ě l u j e p l n o u m o c

pracovníkovi (organizace) **Ministerstvo zahraničních věcí České republiky,**

jméno a příjmení:, nar.:, rodné číslo, doručovací adresa organizace: Loretánské náměstí 101/5, Praha 1, PSČ 118 00, pracovníku Registrační autority oprávněné vydávat kvalifikované certifikáty, kvalifikované certifikáty pro elektronickou pečeť, komerční certifikáty a komerční technologické (serverové) certifikáty a produkt TWINS pro potřeby MZV,

aby

za akciovou společnost První certifikační autorita, a.s. jednal a zastupoval ji při vydávání všech typů certifikátů, tj. kvalifikovaných certifikátů, kvalifikovaných certifikátů pro elektronickou pečeť, produktu TWINS, komerčních certifikátů a komerčních technologické (serverových) certifikátů, a to včetně podepisování všech dokumentů, které v průběhu vydávání všech typů certifikátů pro potřeby resortu MZV vznikají.

Plná moc byla vystavena v Praze, dne

Platnost této plné moci končí okamžikem ukončení platnosti Smlouvy, jejíž je tato plná moc součástí, nebo ukončením pracovně právního vztahu nebo jiného smluvního poměru pracovníka.

Ing. Roman Kučera

člen představenstva

První certifikační autorita, a.s.

.....

podpis

Zplnomocnění přijímám:

.....

podpis

(VZOR)

Prohlášení

Já,,

zaměstnanec/pracovník Ministerstva zahraničních věcí České republiky

prohlašuji, že jsem:

1. Byl/a instruován/a a jsem připraven/a, pro potřeby MZV, zastávat činnost pracovníka Registrační autority, vydávající kvalifikované certifikáty a kvalifikované certifikáty pro elektronickou pečeť a produkt TWINS podle zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce (zákon o elektronickém podpisu), ve znění pozdějších předpisů, a komerční certifikáty a komerční technologické (serverové) certifikáty podle Certifikační politiky I.CA pro komerční certifikáty.
2. Obdržela odkazy na zpřístupnění níže uvedených dokumentů:
 - Certifikační politiku I.CA pro kvalifikované certifikáty
 - Certifikační politiku I.CA pro kvalifikované certifikáty pro elektronickou pečeť
 - Certifikační politiku I.CA pro komerční certifikáty
 - Provozní směrnici pro pracovníky Registračních autorit vydávajících kvalifikované certifikáty a kvalifikované certifikáty pro elektronickou pečeť
 - Provozní směrnici pro pracovníky Registračních autorit vydávajících komerční certifikáty
 - Uživatelskou příručku pro používání SW Registrační autority vydávající kvalifikované certifikáty, kvalifikované certifikáty pro elektronickou pečeť, komerční certifikáty a komerční technologické (serverové) certifikáty.
3. Převzal/a hardwarové vybavení pro činnost Registrační autority:
 - Operátorskou čtečku č.
 - Čtečku čipových karet č.
 - Čipovou kartu č. ...
 - Razítko I.CA č.....

Dne..... v

.....
podpis prohlašujícího

**Zajištění podpory pro činnost pracovišť RA,
provozovaných operátory RA**

Zajištění technické podpory operátorům RA při provozování RA

Součástí této podpory je určení telefonního čísla a e-mailových adres na pracovníky technické podpory I.CA pro poskytování služeb technické podpory pro operátory RA. Jedná se o konzultační služby, poskytované při provozu RA.

Telefon: 284 081 930

E-mail: podpora@ica.cz

Součástí této služby je:

- konzultace k náležitostem vydávání kvalifikovaných certifikátů, kvalifikovaných certifikátů pro elektronickou pečeť, komerčních certifikátů, komerčních technologických (serverových) certifikátů a produktu TWINS
- konzultace k provozování RA
- doškolení operátorů RA.

Zajištění provozu Helpdesk pro potřeby řešení provozních problémů

Helpdesk pro operátory RA při vydávání certifikátů. Využití bude v případech, kdy operátor potřebuje radu či pomoc přímo během vydávání certifikátů. Jedná se o konzultace o náležitostech dokladů, o vrácených chybách v RA, o problémech při komunikaci RA – I.CA apod., zejména:

- dotazy týkající se chybových hlášení v RA a jejich odstranění
- dotazy k požadovaným dokumentům v nestandardních případech.

Součástí této služby je i zapůjčení HW pro případ náhrady za nefungující (poškozenou) čtečku.

Poskytování update a upgrade dodávaného programového vybavení zejména podle legislativních změn či potřeb MZV

I.CA věnuje maximální pozornost sledování vývoje legislativy a požadavků klientů tak, aby SW aplikace ICARA na registračních autoritách byla v souladu s legislativou i s potřebami klientů I.CA a jejich operátorů RA.

Aplikace ICARA je pod kontrolou I.CA a společnost I.CA v ní má možnost provádět všechny změny sama svými vlastními pracovníky.

Veškeré update a upgrade jsou dodávány zdarma.

Způsoby autentizace žadatelů/informačních systémů MZV pro výdej kvalifikovaných časových razítek a archivních kvalifikovaných časových razítek

Kvalifikovaná časová razítka a archivní kvalifikovaná časová razítka budou pro potřeby MZV vydávána kvalifikovanou časovou autoritou I.CA se způsoby autentizace:

> autentizace komerčním certifikátem:

a) Politika časové autority - 1.3.6.1.4.1.23624.10.1.50.2.0

b) Server časové autority - <https://tsa.ica.cz/cgi-bin/razitko2.cgi>

> autentizace jménem a heslem HTTPS

a) Politika časové autority - 1.3.6.1.4.1.23624.10.1.50.2.0

b) Server časové autority - https://tsabase.ica.cz/cgi-bin/razitko_base2.cgi

> autentizace jménem a heslem HTTP

a) Politika časové autority - 1.3.6.1.4.1.23624.10.1.50.2.0

b) Server časové autority - http://tsabase.ica.cz/cgi-bin/razitko_base2.cgi

> autentizace statickou IP adresou

a) Politika časové autority - 1.3.6.1.4.1.23624.10.1.50.2.0

b) Server časové autority - http://tsabase.ica.cz/cgi-bin/razitko_ip2.cgi

Popis projektu ePasy

Již od roku 2006 využívá projekt ePasy MZV certifikátů a dalších certifikačních služeb ICA, z nich některé byly upraveny dle požadavku projektu. Pro další fungování projektu ePasy, spolu s podporou ICA, budou služby zachovány.

Dodávka upraveného SW SecureStore

Pro projekt MZV je relevantní část SecureStorePKCS11.dll, které obsahuje všechny patche realizované v rámci testování použití modulu PKCS11 v aplikaci odběratele.

Modul SecurestoreCSP není v projektu používán, ale je standardní součástí instalačního balíčku.

Securestore je předáván ve tvaru instalačního balíčku:

securestore_mzv_mzv_x_x_x_x64.exe

securestore_mzv_mzv_x_x_x_x86.exe

SecurestorePKCS11 obsahuje úpravy požadované projektem doklady s biometrickými prvky:

- Specifické chování funkce přidání objektu na kartu dle nastavení registry
- Specifické práce se selfsign certifikáty
- Mazání a listování kořenových certifikátů

Registrační autorita

Pro projekt jsou k dispozici 2 klientské registrační autority. SW je standardní, není speciální instalace.

Zneplatňování certifikátů

Žádost o zneplatnění certifikátu je odesílána standardním protokolem SMTP a obsahuje tento text:

Zadam o zneplatneni certifikatu cislo = xxxxxxxx

Heslo pro zneplatneni = yyyyyy

kde „xxxxxxx“ je sériové číslo certifikátu a „yyyyyy“ je heslo pro zneplatnění. Sériové číslo je v dekadickém tvaru. Tato zpráva je zaslána z aplikačního serveru MZV přes vyhrazené ISDN spojení na server mail.ica.cz na adresu revoke@ica.cz.

Vydávání a přístup k seznamu zneplatněných certifikátů – CRL

V položkách certifikátů pro MZV je uveden CRL Distribution Point. Pro komerční certifikáty

URL=http://scrl dp1.ica.cz/sica09.crl a URL=hhttp://scrl dp2.ica.cz/sica09.crl.

Pro kvalifikované certifikáty URL=http://qcrl dp1.ica.cz/qica09.crl, URL=http://qcrl dp2.ica.cz/qica09.crl a URL=http://qcrl dp3.ica.cz/qica09.crl.

Pro MZV jsou CRL Distribution point dostupné na následujících serverech:

193.86.94.141	http://scrl dp1.ica.cz	(pro sica09.crl a sica08.crl)
62.168.46.147	http://scrl dp2.ica.cz	(pro sica09.crl a sica08.crl)
193.86.94.143	http://qcrl dp1.ica.cz	(pro qica09.crl a qica08.crl)
195.47.14.194	http://qcrl dp2.ica.cz	(pro qica09.crl a qica08.crl)
62.168.46.147	http://qcrl dp3.ica.cz	(pro qica09.crl a qica08.crl)

Obnova certifikátů

Obnova certifikátů probíhá speciální cestou. Podpora pro obnovu certifikátu je integrována do klientské aplikace ePasy která odesílá autentizovanou cestou žádosti o obnovu v dohodnutém formátu na speciální aplikaci na CA. Podstatou je vytvoření nové žádosti o certifikát (včetně klíčového páru), podpis této žádosti dosud platným certifikátem a odeslání na I.CA.

Žádost o obnovu je podepsaná příslušným platným certifikátem a zpráva je ve formátu PKCS#10 v kódování PEM. Podmínkou obnovy certifikátu je, že vlastní PKCS#10 žádost musí obsahovat shodné DN žádosti jako obnovovaný certifikát. Tento postup je stejný jak u kvalifikovaných certifikátů, tak u certifikátů komerčních.

Certifikát použitý při autentizaci k aplikaci na CA je jakousi vzdálenější analogií certifikátu operátora a musí být v systému CA přiřazen k tzv. virtuálnímu RA.

Pro komunikaci je použito neanonymní HTTPS spojení (autentizace certifikátem I.CA). Klientem je subjekt zasílající žádost o obnovení certifikátu, serverem pak systém I.CA. Požadavek je zaslán metodou POST protokolu HTTP. Na straně ICA je žádost zpracována skriptem distrib.cgi. Spojení na straně I.CA zajišťuje zakomponovaný WWW server a skript distrib.cgi serverech:

- 193.86.94.143 <https://q.ica.cz/cgi-bin/distrib.cgi> pro kvalifikované certifikáty,
- 193.86.94.144 <https://q2.ica.cz/cgi-bin/distrib.cgi> pro kvalifikované certifikáty,
- 193.86.94.141 <https://s.ica.cz/cgi-bin/distrib.cgi> pro komerční certifikáty.
- 193.86.94.142 <https://s2.ica.cz/cgi-bin/distrib.cgi> pro komerční certifikáty.

Vydané certifikáty a reporty o vydaných certifikátech

Obnova certifikátů probíhá ještě v době platnosti stávajícího platného certifikátu, a to elektronickou cestou bez nutnosti osobní přítomnosti žadatele na RA.

Jedenkrát denně je v ranních hodinách za uplynulých 24 hodin vystaven seznam vydaných certifikátů a karet v dohodnutém tvaru. Autentizace je certifikátem.

První den v měsíci je vystaven seznam o vydaných certifikátech v předchozím měsíci.

Seznamy certifikátů jsou dostupné na serveru:

- 193.86.94.153 https://cdbp.ica.cz/ep_bica/MZV_DEN_EP_rrrrmdd.txt,
resp 193.86.94.153 https://cdbp.ica.cz/ep_bica/MZV_MES_EP_rrrrmm.txt

Obnovený certifikát je ze seznamu vydaných certifikátů stažen a doručen aplikací ePasy MZV, která komunikuje s I.CA, do databáze na serveru MZV. Ze zaslaných souborů je pak provedena obnova na příslušné čipové kartě. Není potřeba osobní návštěva RA.

Podpora virtuální RA pro ePasy

Při startu projektu bylo definováno, že certifikáty virtuálních RA budou jejich majitelé obnovovat a přiřazení obnoveného certifikátu k virtuálnímu RA proběhne automatizovaně.

V praxi však nejsou certifikáty obnovovány, nýbrž jsou každý rok vydávány nové prvotní certifikáty.

Po vydání prvotního certifikátu je nutno zajistit jeho přiřazení k virtuálnímu RA ručně viz dále.

K této akci dochází u každého virtuálního RA jednou ročně.

Postup zavedení nového prvotního certifikátu virtuální RA

1. Majitel certifikátu zajistí vydání nového certifikátu pro virtuální RA
2. Majitel certifikátu informuje I.CA o tom, že byl vydán nový certifikát, který bude nadále používán pro virtuální RA. Sdělí pracovníkovi I.CA SN nového certifikátu.
3. Pracovník I.CA zašle SN certifikátu a kód virtuálního RA provoznímu oddělení I.CA (prasek@ica.cz) s žádostí o přiřazení nového certifikátu k virtuálnímu RA a webovému serveru pomocí rozhraní pro správu.
Ostré prostředí: MZV – používá RA 'OU'
4. Provozní oddělení I.CA zajistí nastavení přístupu tímto certifikátem do konfigurace webu pro stahování reportů.

Testovací prostředí ePasy

Testovací prostředí ePasy je napojeno na testovací prostředí ICA.

V testovacím prostředí ICA jsou pro ePasy stejné funkce a služby jako v prostředí provozním. Rozdílné jsou pouze přístupové body ke službám.

Zneplatňování certifikátů

Server mail.ica.cz 193.86.94.135 na adresu test_revoke@ica.cz.

Vydávání a přístup k seznamu zneplatněných certifikátů – CRL

Pro MZV test jsou CRL Distribution point dostupné na následujících serverech:

193.86.94.175 <http://tests.ica.cz> (pro tsica10.crl, tsica09.crl a sica08.crl)

193.86.94.176 <http://testq.ica.cz> (pro tqica10.crl, tqica09.crl a tqica08.crl)

Obnova certifikátů

193.86.94.179 <https://testq2.ica.cz/cgi-bin/distrib.cgi> pro kvalifikované certifikáty,

193.86.94.178 <https://tests2s.ica.cz/cgi-bin/distrib.cgi> pro komerční certifikáty.

Vydané certifikáty a reporty o vydaných certifikátech

193.86.94.177 https://cdbpt.ica.cz/ep_tbica/MZV_DEN_EP_rrrrmdd.txt,

resp 193.86.94.177 https://cdbpt.ica.cz/ep_tbica/MZV_MES_EP_rrrrmm.txt

Případné změny technických údajů uvedených v Příloze č. 12 této Smlouvy jsou smluvní strany povinny písemně oznámit dopisem podepsaným oprávněným zástupcem. Písemné oznámení je možné nahradit e-mailovou zprávou, podepsanou uznávaným elektronickým podpisem.

Příloha č. 13

Certifikační politika pro SSL certifikáty
(CP SSL)

CP SSL

(Certifikační politika I.CA pro SSL certifikáty)

aktuální verze – viz

WWW.ICA.CZ

Příloha č. 14

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 – Ministerstvo zahraničních věcí**

Adresa: Loretánské náměstí 101/5, 118 00 Praha 1

IČO: 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: **Česká republika – Ministerstvo zahraničních věcí**

Adresa: Loretánské náměstí 101/5, 118 00 Praha 1

IČO: 45769851

E-mailová adresa žadatele:

.....

Účel použití SSL certifikátu:

.....

V Praze dne

.....
jméno a funkce
pověřené osoby k jednání za
Ministerstvo zahraničních věcí

.....
Podpis zaměstnance

Příloha č. 15

Informace a postup získání SSL certifikátu

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

3. 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

4. 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

5. 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).

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

7. 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).

8. 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 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.

9. 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.

10. 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.

Podmínky zpracování osobních údajů

1. ZPŮSOB, ROZSAH A DOBA ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

- 1.1 Správce opravňuje Zpracovatele po dobu účinnosti této smlouvy ke zpracování Osobních údajů zákazníků/klientů Správce (dále též „Subjekt údajů“) v souvislosti s plněním povinností dle této smlouvy, kdy Osobní údaje budou Zpracovateli předávány Subjektem údajů za výše uvedeným Účelem smlouvy v podobě elektronických a/nebo tištěných dokumentů, které mohou obsahovat níže uvedené kategorie Osobních údajů:
- a) jméno a příjmení,
 - b) funkce osoby,
 - c) titul (před i za jménem),
 - d) údaje o adrese trvalého pobytu
 - e) datum narození,
 - f) rodné číslo,
 - g) číslo občanského průkazu, osobní číslo,
 - h) e-mailová adresa.
- 1.2 Osobní údaje uvedené výše v odst. 1.1 je Zpracovatel oprávněn zpracovávat zejména za účelem:
- a) obsluhy Subjektu údajů jako zákazníka/klienta Správce při provozu Registrační autority sloužící k vydávání kvalifikovaných a komerčních certifikátů,
 - b) uzavírání smluvních vztahů o vydání a používání certifikátu se zákazníky/klienty,
 - c) vyřizování návrhů na změnu a zánik smluvních vztahů uvedených v písm. b) tohoto odst.
- 1.3 Zpracovatel bude zpracovávat Osobní údaje zákazníků zejména jejich shromažďováním a předáváním Správci, a to manuálně v listinné podobě a elektronicky ukládáním v interním systému Správce, v souladu se smlouvou.
- 1.4 Osobní údaje Subjektů údajů je Zpracovatel oprávněn zpracovávat nejdéle po dobu stanovenou pro jednotlivé účely zpracování, nejdéle však po dobu trvání této smlouvy.

2. PRÁVA A POVINNOSTI STRAN

- 2.1 Zpracovatel se zavazuje zpracovávat Osobní údaje poskytnuté Subjektem údajů v souladu s touto smlouvou a výlučně k výše uvedenému Účelu.

- 2.2 Zpracovatel je povinen řídit se při zpracování Osobních údajů na základě této smlouvy doloženými pokyny Správce. Zpracovatel je rovněž povinen upozornit Správce bez zbytečného odkladu na nevhodnou povahu pokynů.
- 2.3 Pokud by Zpracovatel zjistil, že Správce porušuje povinnosti vyplývající pro něj z nařízení Evropského parlamentu a Rady (EU) 2016/679, 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 „Nařízení“) nebo zákona č. 110/2019 Sb., o zpracování osobních údajů (dále jen „Zákona o zpracování OÚ“), je ve smyslu článku 28 písm. h) věty druhé Nařízení povinen neprodleně Správce o této skutečnosti informovat.
- 2.4 Zpracovatel je povinen dbát, aby žádný Subjekt údajů neutrpěl újmu na svých právech, zejména na právu na zachování lidské důstojnosti, a také dbát na ochranu před neoprávněným zasahováním do soukromého a osobního života Subjektů údajů.
- 2.5 V případě, že se kterýkoli Subjekt údajů bude domnívat, že Správce nebo Zpracovatel provádí zpracování jeho Osobních údajů, které je v rozporu s ochranou soukromého a osobního života Subjektu údajů nebo v rozporu se Zákonem o zpracování OÚ, zejména budou-li Osobní údaje nepřesné s ohledem na účel jejich zpracování, a tento Subjekt údajů ve smyslu § 49 Zákona o zpracování OÚ požádá Zpracovatele o vysvětlení nebo o odstranění vzniklého stavu, zavazuje se Zpracovatel o tom neprodleně informovat Správce.
- 2.6 Správce je oprávněn uveřejnit nebo jinak sdělit svým klientům, a to formou dle uvážení Správce, že se Zpracovatel podílí na zpracování Osobních údajů, s nimiž Správce nakládá, a za jakým účelem.
- 2.8 Zpracování Osobních údajů Zpracovatelem a jejich ochrana podle této smlouvy probíhá bez nároku Zpracovatele na zvláštní odměnu.
- 2.9 Strany tímto sjednávají, že Správce má právo kdykoli požadovat předložení veškeré dokumentace Zpracovatelem, která souvisí s činností Zpracovatele dle této smlouvy. Správce je oprávněn ke kontrole prostor, které využívá Zpracovatel k činnosti dle smlouvy, za účelem zjištění, zda jsou předané Osobní údaje zpracovávány v souladu s touto smlouvou a s Nařízením a Zákonem o zpracování ÚO.
- 2.10 Veškerá oznámení dle této smlouvy se považují za řádně doručená, pokud jsou doručena osobně nebo doporučenou poštou na níže uvedené adresy případně zaslána na uvedené e-mailové adresy:

První certifikační autorita, a.s., Podvinný mlýn 2178/6, 190 00 Praha 9 – Libeň
e-mail: sales@ica.cz

Česká republika – Ministerstvo zahraničních věcí, Loretánské náměstí 101/5, 118 00 Praha 1
e-mail: registracni_autorita@mzv.cz

Veškerá oznámení budou považována za doručená k datu jejich přijetí, pokud jsou doručena osobně, a po čtrnácti (14) dnech, pokud jsou zasílána doporučenou poštou či e-mailem. Adresa a osoby, k jejichž rukám se oznámení zasílají, mohou být kdykoli změněny na základě písemného oznámení, které je nutno zaslat způsobem uvedeným v tomto odstavci.

- 2.11 Při provádění činností dle této smlouvy Zpracovatel nejedná v zastoupení Správce a není oprávněn činit žádná jednání v zastoupení Správce, zejména v zastoupení Správce podepisovat smluvní dokumenty anebo přijímat plnění od třetích stran, s výjimkou podpisu

Protokolu o podání žádosti o vydání certifikátu a Smlouvy o vydání a používání certifikátu se zákazníkem/klientem/žadatelem o certifikát.

- 2.12 Zpracovatel i Správce se zavazuje zachovat mlčenlivost o skutečnostech, které se při své činnosti dozví a které by mohly ohrozit ekonomické zájmy, podnikatelské záměry nebo dobrou pověst Správce a Zpracovatele, a o skutečnostech, které Správce a Zpracovatel označí za předmět obchodního tajemství nebo za důvěrnou informaci. Tato povinnost trvá i po ukončení účinnosti této smlouvy.
- 2.13 Správce je povinen v případě, že pro plnění povinností Zpracovatele dle této smlouvy jsou nutné jakékoli písemné podklady, předat tyto podklady Zpracovateli bez zbytečného odkladu poté, co o to bude Zpracovatelem požádán.

3. ZÁRUKY TECHNICKÉHO A ORGANIZAČNÍHO ZABEZPEČENÍ OCHRANY OSOBNÍCH ÚDAJŮ

- 3.1 Zpracovatel je povinen zajistit přiměřené technické a organizační zabezpečení ochrany Osobních údajů a přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k Osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, zpracování, jakož i k jinému zneužití těchto Osobních údajů.
- 3.2 Zpracovatel se zavazuje chránit Osobní údaje před přístupem neoprávněných osob zamezením přístupu neoprávněných osob do prostor, v nichž Zpracovatel poskytuje své služby podle této smlouvy.
- 3.3 Zpracovatel se zavazuje zajistit mlčenlivost svých zaměstnanců, kteří při výkonu své činnosti přichází do styku s Osobními údaji podle této smlouvy, v souladu se Zákonem o zpracování OÚ a Nařízením.
- 3.4 Zpracovatel se zavazuje zajistit, aby Osobní údaje předané jemu Subjektem údajů či Správcem byly chráněny v souladu se Zákonem o zpracování OÚ a Nařízením.
- 3.5 Zpracovatel je povinen Osobní údaje uchovávat v náležitě zabezpečených objektech a místnostech a o pohybu písemných dokumentů obsahujících Osobní údaje bude Zpracovatel vést řádnou evidenci.
- 3.6 Zpracovatel se zavazuje provádět činnost dle této smlouvy osobně, resp. prostřednictvím svých zaměstnanců.
- 3.7 Bez předchozího konkrétního nebo obecného písemného souhlasu Správce Zpracovatel nesdělí Osobní údaje obdržené od Subjektu údajů či od Správce žádné třetí osobě a nepoužije žádnou třetí osobu pro plnění jejích povinností podle této smlouvy. Pokud s předchozím písemným souhlasem Zpracovatel použije třetí osobu pro plnění jejích povinností podle této smlouvy, učiní tak pouze na základě takové písemné smlouvy uzavřené s touto třetí osobou, která zajistí, že plnění povinností Zpracovatele z této smlouvy pomocí této třetí osoby bude v souladu s Nařízením, Zákonem o zpracování OÚ a touto smlouvou. Zpracovatel bude vůči Správci plně odpovědný za plnění povinností vyplývajících z této smlouvy, které Zpracovatel plní prostřednictvím třetí osoby. V případě obecného písemného povolení Zpracovatel informuje Správce o veškerých zamýšlených změnách týkajících se přijetí třetích osob jako dalších zpracovatelů nebo jejich nahrazení a poskytne tak Správci příležitost vyslovit vůči těmto změnám námitky.
- 3.8 Zpracovatel prohlašuje a zavazuje se, že předané Osobní údaje jako celek budou k dispozici pouze přesně vymezené skupině zaměstnanců Zpracovatele, kteří se podílejí na plnění Účelu a jejichž účast na plnění Účelu je přesně definována a dokumentována. Jednotliví

zaměstnanci pak budou dostávat pouze ty Osobní údaje, které jsou nezbytné pro zajištění jejich podílu na činnostech Zpracovatele podle této smlouvy. Osobní údaje budou uloženy způsobem, který zabrání přístupu nepovolaných osob k nim. Úplný seznam všech zaměstnanců Zpracovatelem s přístupem k Subjektům údajů či Správcem předaným Osobním údajům, včetně jejich podílu na jednotlivých činnostech, eviduje Správce společně se záznamy o jejich poučení o režimu nakládání s těmito Osobními údaji.

3.9 Osobní údaje v elektronické podobě Zpracovatel neuchovává na nosičích dat, veškerá komunikace včetně šifrování dat při přenosu a uchovávání je zajištěna programovým vybavením Registrační autority u Správce, který zajišťuje přístup pouze pověřených osob na základě přístupových kódů či hesel, a Osobní údaje pravidelně zálohují. Zpracovatel není oprávněn jakkoli zasahovat do programového vybavení registrační autority.

3.10 Zpracovatel zajišťuje níže uvedené povinnosti prostřednictvím programového vybavení Registrační autority dodaného Správcem bez možnosti zásahu:

- dálkový přenos Osobních údajů probíhá prostřednictvím zabezpečeného (šifrovaného) přenosu po veřejných sítích,
- zpracování Osobních údajů je prováděno v co největší míře pouze pseudonymizované a šifrované podobě, je-li takové opatření vhodné a nezbytné ke snížení rizik plynoucích ze zpracování Osobních údajů.
- neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování.
- prostřednictvím vhodných technických prostředků schopnost obnovuje dostupnost Osobních údajů a přístup k nim včas v případě fyzických či technických incidentů.
- pravidelně testuje, posuzuje a hodnotí účinnost zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování. Zpracovatel je povinen zpracovat a dokumentovat přijatá a provedená technicko-organizační opatření k zajištění ochrany Osobních údajů v souladu se Zákonem o zpracování OÚ, Nařízením a jinými právními předpisy.

4. NÁHRADA ÚJMY

4.1 Správce je odpovědný za újmu, kterou způsobí zpracováním, jež je v rozporu s relevantními právními předpisy, tj. zejména s Nařízením. Zpracovatel je za újmu způsobenou zpracováním odpovědný pouze v případě, že nesplnil povinnosti stanovené Nařízením a ostatními relevantními právními předpisy konkrétně pro zpracovatele nebo že jednal nad rámec zákonných pokynů Správce nebo v rozporu s nimi. Správce nebo Zpracovatel jsou odpovědní podle tohoto odstavce zproštěni, pokud prokáží, že nenesou žádným způsobem odpovědnost za událost, která ke vzniku újmy vedla.

4.2 Smluvní strany se zavazují vzájemně odškodnit v souladu s § 2916 Občanského zákoníku, ve znění pozdějších předpisů, za jakékoliv nároky, a to zejména zadostiučinění, peněžité náhrady nebo pokuty, úspěšně uplatněné v pravomocně skončeném soudním, popř. správním řízení třetími osobami, a to zejména subjekty údajů nebo Úřadem pro ochranu osobních údajů, které vznikly porušením povinností stanovených platnými právními předpisy nebo touto Smlouvou.

5. TRVÁNÍ SMLOUVY A LIKVIDACE DAT

- 5.1 Po ukončení účinnosti této smlouvy Zpracovatel zničí veškeré obdržené či předané Osobní údaje a písemně potvrdí Správci, že tak učinil, ledaže zničení všech anebo části předaných údajů brání právní předpisy, které jsou pro Zpracovatele závazné. V takovém případě bude Zpracovatel povinen zajistit důvěrnost příslušných nezničených Osobních údajů a nebude oprávněn tyto Osobní údaje nadále aktivně zpracovávat.
- 5.2 Na žádost Správce Zpracovatel bezodkladně zničí Osobní údaje týkající se jednotlivého Subjektu údajů a písemně potvrdí Správci, že tak učinil, ledaže zničení všech anebo části takových údajů brání právní předpisy, které jsou pro Zpracovatel závazné. V takovém případě bude Zpracovatel povinen zajistit důvěrnost příslušných nezničených Osobních údajů a nebude oprávněn tyto Osobní údaje nadále aktivně zpracovávat.
- 5.3 Na žádost Správce nebo dohlížecího orgánu jim Zpracovatel umožní zkontrolovat svá zařízení používaná ke zpracování Osobních a dalších údajů, a to za účelem kontroly splnění opatření, které je Zpracovatel povinen zajistit.
- 5.4 Zpracovatel je po zániku této smlouvy povinen dodržovat veškeré povinnosti plynoucí z Nařízení a ze Zákona o zpracování OÚ, zejména předejít jakémukoliv neoprávněnému nakládání s Osobními údaji do doby, než dle pokynů Správce tyto Osobní údaje předá Správci nebo provede jejich bezpečnou likvidaci.

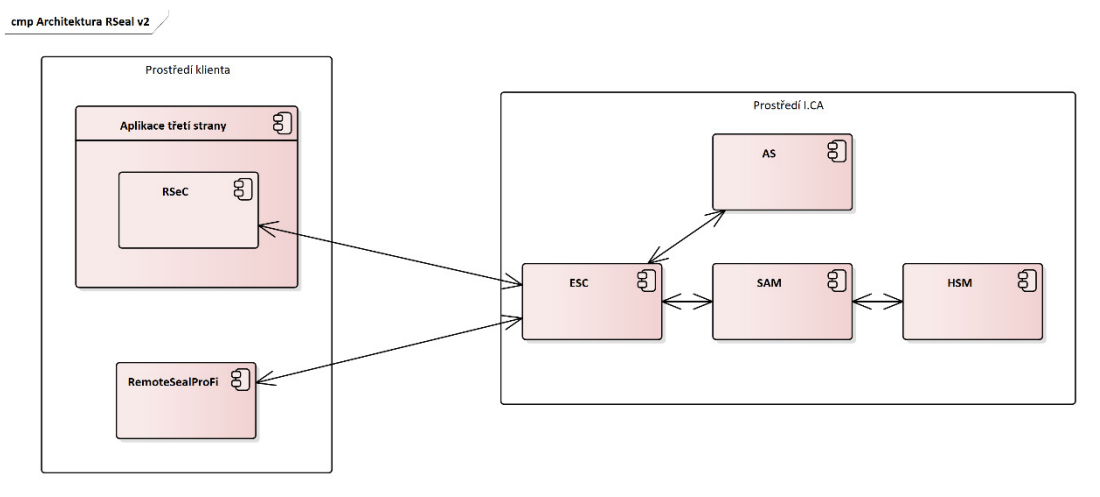
Popis služby vytváření kvalifikovaných elektronických pečetí na dálku

Co je služba I.CA RemoteSeal v2

Služba I.CA RemoteSeal v2 (dále už jen „RemoteSeal“ nebo „služba“) je služba vytváření kvalifikovaných elektronických pečetí na dálku. Služba umožňuje vygenerovat a držet data pro vytváření elektronických pečetí (tj. zejména privátní klíč) v QSealCD certifikovaném HSM zařízení ve správě I.CA a k němu pak zprostředkovat přístup pro účely vytváření kvalifikovaných elektronických pečetí.

Klient (tj. právnická osoba) má k dispozici klientskou komponentu a příslušné autentizační markanty, pomocí kterých může dokument opatřit kvalifikovanou elektronickou pečetí. Samotný obsah dokumentu přitom neopouští klientskou komponentu, a tudíž ani prostředí klienta.

Architektura



- **RSeC** (RemoteSeal Client) - klientská komponenta určená pro strojové pečetění dokumentů a pro integraci do spisové služby nebo jiného systému, který potřebuje autonomně vytvářet kvalifikované pečeti. Existuje ve vícero variantách pro snadnou integraci do různých systémů.
- **RemoteSealProFi** - klientská desktop aplikace pro Windows, která slouží ke správě pečetění dané organizace a ručnímu vytváření kvalifikovaných pečetí.
- **ESC** (Evolved Signature Core) - základní aplikační server provozovaný I.CA, přes který jdou veškeré komunikace týkající se pečetění z klientských komponent.
- **SAM** (Signature Activation Module) - povinná součást QSCD pro vzdálený podpis/pečet, který zajišťuje kontrolu přístupu ke klíčům uloženým na HSM modulu
- **HSM** (Hardware Security Module) - povinná součást QSCD pro vzdálený podpis/pečet, která zajišťuje samotné bezpečné generování, uchovávání a používání privátních klíčů.
- **AS** (Authorization Server) - aplikační server, který zajišťuje ověření autentizace koncového uživatele (držitele klíče) a vytváření SAD (Signature Activation Data) tj. datové struktury autorizující použití příslušného privátního klíče pro podpis příslušných dat pro SAM.

Použité QSCD

Služba využívá certifikované Remote QSealCD skládající se ze:

- SAM modulu Entrust SAM

<https://eidas.ec.europa.eu/efda/browse/notification/qscd-sscd>

Austria List of SSCDs	
Name Qualified Signature and Seal Creation Device (QSCD) Entrust Signature Activation Module, version 1.0.3	
Applicant Entrust Solutions Spain S.L. Parque Empresarial 'La Finca', Paseo del Cid, 200, 1. 48940 Leizor, 48940 Leizor (Vizcaya), Spain	
Remote QSCD Yes <i>QSCD v1.0.3.2 is not a remote QSCD as it is not a QSCD for use in a QSCD (other QSCD) or a QSCD for use in a QSCD (other QSCD) as defined in Article 3(2) of Regulation (EU) 910/2014.</i>	
Qualified Signature Creation Device (QSigCD) Yes	
Issuer Entrust for Software Information Technology - Austria (Q-SIG)	
Reference A-071021-008	
URL https://www.entrust.com/secure/1000/	
Effective starting date 20/10/2021	
Expiration date 10/10/2026	
Art 30.3 (b) notified alternative certification method https://www.entrust.com/secure/1000/ https://www.entrust.com/secure/1000/	
CC certification report(s) Reference NSC-01-000000-01 NSC-01-000000-01 URL report https://www.entrust.com/secure/1000/ URL security report https://www.entrust.com/secure/1000/ Security issue 1/10/2021	
Qualified Seal Creation Device (QSealCD) Yes	
Issuer Entrust for Software Information Technology - Austria (Q-SIG)	
Reference A-071021-008	
URL https://www.entrust.com/secure/1000/	
Effective starting date 20/10/2021	
Expiration date 10/10/2026	
Art 30.3 (b) notified alternative certification method https://www.entrust.com/secure/1000/ https://www.entrust.com/secure/1000/	
CC certification report(s) Reference NSC-01-000000-01 NSC-01-000000-01 URL report https://www.entrust.com/secure/1000/ URL security report https://www.entrust.com/secure/1000/ Security issue 1/10/2021	
Annex	

- HSM modulu Entrust nShield Connect XC

An official website of the European Union How do you know? Privacy statements of eIDAS Dashboard	
European Commission eIDAS Dashboard EU LOGIN	
Business, Economy, Euro	
DISCOVER BROWSE COMPLIANCE INTERNATIONAL	
Home Browse Compiled list of notified SSCDs/QSCDs	
Qualified Signature/Seal Creation Devices and Secure Signature Creation Devices	
Compiled list of Qualified electronic Signature Creation Devices (QSigCDs) as defined in point 23 of Article 3 of Regulation 910/2014, Qualified electronic Seal Creation Devices (QSealCDs) as defined in point 32 of Article 3 of Regulation 910/2014, and Secure Signature Creation Devices (SSCDs) benefiting from the transitional measure set in Article 51(1) of Regulation 910/2014. These devices are listed under the country where the issuer of the designation report (or designated certification body) is established. Some devices may, therefore, be listed under a country that is different from the country where they are actually used.	
Disclaimer: The European Commission maintains this list only as an informative tool. Our goal is to keep this information timely and accurate, based on information from the Member States. If errors are brought to our attention, we will try to correct them. However, the Commission accepts no responsibility or liability whatsoever with regard to the content or completeness of the list.	
Export list as PDF Export list as XML	
Filter by	
Country Netherlands	Name nShield Solo XC Hardware Security Module v12.60.15
Show QSCD Show SSCD	
Netherlands List of QSCDs	
nShield Solo XC Hardware Security Module v12.60.15	
Name nShield Solo XC Hardware Security Module v12.60.15	
Applicant Entrust	
Remote QSCD No	
Qualified Signature Creation Device (QSigCD) Yes	
Issuer TUV Rheinland Nederland B.V.	
Reference NSC-01-000000-01	
URL https://www.tuv-rheinland.nl/assets/files/certificates/2021/06/eidas-certificate-21-0366256.pdf	
Effective starting date 10/06/2021	
Expiration date 10/06/2026	
Art 30.3 (b) notified alternative certification method https://www.tuv-rheinland.nl/assets/files/general/files/2019/12/190724-n-eidas-dutch-conformity-assessment-process-v3.0.pdf	

Certificate eIDAS

Standard REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

Certificate number **CC-21-0368256-eIDAS**

TÜV Rheinland Nederland B.V. certifies:

Certificate holder **Entrust**
Minneapolis1187 Park Place, Shakopee, MN 55379, USA

TOE developer **nCipher Security Limited (an Entrust company)**
One Station Square, Cambridge CB1 2GA, UK

Product and assurance level **nShield Solo XC Hardware Security Module v12.60.15**

Assurance Package:

- EAL4 augmented with AVA_VAN.5 and ALC_FLR.2

Protection Profile Conformance:

- EN419221-5 Protection Profiles for TSP Cryptographic Modules - Part 5, Version 1.0, registered under the reference ANSSI-CC-PP-2016/05-M01, 18 May 2020

Project number **0368256**

Evaluation facility **Brightsight BV located in Delft, the Netherlands**

Applying the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 5 (ISO/IEC 18045)

The Designated Body from The Netherlands under Article 30(2) and 39(2) of Regulation 910/2014 declares that:

- The IT product identified in this certificate is a Qualified Signature/Seal Creation Device (QSCD) where the electronic signature/seal creation data is held in an entirely but not necessarily exclusively user-managed environment.
- The IT product meets the requirements laid down in Annex II of REGULATION (EU) No 910/2014 of THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014.
- Conformity of the IT product with the requirements of Annex II of REGULATION has been certified with an evaluation process that fulfils the requirements of Article 30(3.(b)) of REGULATION and the Dutch Conformity Assessment Process (DCAP).
- The IT product identified in this certificate is not a Qualified Signature/Seal Creation Device (QSCD) where a Qualified Trust Service Provider (QTSP) manages the electronic signature/seal creation data on behalf of a signatory/creator of a seal, but might be used as a component of such a QSCD in conformity with the applicable certification of that QSCD against REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014.

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using the Common Methodology for IT Security Evaluation version 3.1 Revision 5 for conformance to the Common Criteria for IT Security Evaluation version 3.1 Revision 5. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report. The evaluation has been conducted in accordance with the provisions of the Netherlands scheme for certification in the area of IT security [NSCIB] and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by TÜV Rheinland Nederland B.V. or by other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Rheinland Nederland B.V. or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Evaluated and approved 'assessment documents of referral':

NSCIB Certification Report dated 17 March 2021 with ID: NSCIB-CC-0368256
Assessment Reporting Sheet eIDAS dated with ID: NSCIB-CC-0368256; version 1.0, March 9, 2021

Validity De validity of this certificate coincides with the published NSCIB-certificate with ID: CC-21-0368256 with the following validity-dates:

Date of 1st issue : **10-06-2021**
Certificate expiry : **10-06-2026**

R.L. Kruit, LFM Systems
TÜV Rheinland Nederland B.V.
Westervoortsedijk 73, 6827 AV Arnhem
P.O. Box 2220, NL-6802 CE Arnhem
The Netherlands



TÜVRheinland®
Precisely Right.

Version 2020-4

© TÜV, TÜV and TÜV are registered trademarks. Any use or application requires prior approval.



www.tuv.com/nl

Varianty klientských komponent

RemoteSeal poskytuje několik variant klientských komponent, které je možné rozdělit do dvou skupin:

- Klientské komponenty pro ruční pečetění uživatelem, tedy člověkem
- Klientské komponenty pro automatizované/strojové pečetění

Klientské komponenty pro ruční pečetění uživatelem, tedy člověkem

Pro ruční pečetění člověkem - tj. zaměstnanci dané organizace existuje desktopová GUI aplikace pro Windows RemoteSealProFi, která umožňuje ručně vybrat dokument/dokumenty a opatřit je kvalifikovanou elektronickou pečetí.

Aplikace RemoteSealProFi má zároveň správcovskou (administrátorskou) funkci - uživatel s rolí správce pečetění organizace pomocí aplikace spravuje instance RSeC, další uživatele a obnovu pečetícího certifikátu.

Klientské komponenty pro automatizované/strojové pečetění

Klientské komponenty pro automatizované/strojové pečetění souhrnně nazýváme RSeC (Remote Seal Client) a jsou určeny pro integraci do informačního systému/aplikace třetí strany, který má autonomně pečeti dokumenty jejichž je organizace původcem.

RSeC je vždy založen na nativním (C/C++) jádře, ke kterému je pak nadstavba pro danou platformu:

- **jRSeC** (Linux i Windows) - nadstavba nad RSeC určená pro integraci do aplikací v jazyce Java formou Java class library.
- **RSeC.NET** (Linux i Windows) - nadstavba nad RSeC určená pro integraci do aplikací v jazyce .NET
- **RSeProxy** (Windows) - serverová aplikace určená pro instalaci do sítě klienta, která do vnitřní sítě klienta poskytuje SOAP webové služby pro funkcionality pečetění, přičemž vůči systému RemoteSeal vystupuje jako klientská komponenta RSeC.

Zřízení služby

1. Prvním krokem je uzavření smlouvy mezi organizací a I.CA.
2. Oprávněná osoba žadatele (tj. organizace) dohodne se zástupcem I.CA způsob vydání osobního autentizačního komerčního certifikátu – obvykle navštíví pobočku RA v sídle společnosti I.CA s potřebnými doklady ke zřízení služby I.CA RemoteSeal na danou organizaci.
3. Operátor RA vydá oprávněné osobě osobní autentizační komerční certifikát na čipovou kartu Starcos 3.5 nebo 3.7. Tato osoba se tímto automaticky stává prvním (a v tento okamžik prozatím také jediným) správcem služby pečetění pro danou organizaci.
4. Operátor RA provede zřízení služby I.CA RemoteSeal vč. vydání kvalifikovaného pečetícího certifikátu (kvalifikovaný certifikát pro elektronickou pečeť) pro danou organizaci, přičemž privátní klíč pro tento certifikát je generován a spravován QSCD zařízením služby I.CA RemoteSeal.
5. V rámci vydání pečetícího certifikátu oprávněná osoba žadatele podepisuje dokumentaci k vydání certifikátu, přičemž tyto mohou být podepsány:
 - klasicky vlastnoručním podpisem na papír, nebo
 - bezpapírově/elektronicky pomocí osobního autentizačního komerčního certifikátu oprávněné osoby (v tom případě žadatel podepisuje pouze smlouvu)
6. Oprávněná osoba žadatele odchází z RA s čipovou kartou s autentizačním komerčním certifikátem.

Uživatelské účty RemoteSealProFi

Aplikace RemoteSealProFi umožňuje na jednom PC (přesněji jednomu uživateli Windows na daném PC) mít současně vytvořeno více uživatelských účtů a při startu aplikace se přihlásit do uživatelského účtu dle volby.

Uživatelské účty jsou dvojího druhu:

- Přenosný uživatelský účet
- Fixní uživatelský účet

Přenosný uživatelský účet

Přenosný uživatelský účet není vázán na jedno konkrétní PC, ale je možné k němu přistupovat z různých PC, na nichž je nainstalována aplikace RemoteSealProFi.

Pro autentizaci uživatele slouží:

- čipová karta Starcos 3.5 nebo 3.7 s (autentizačním) osobním komerčním certifikátem
- PIN k čipové kartě
- heslo uživatele ke službě RemoteSeal

Uživatel, jenž pro autentizaci používá výše uvedené, si může na libovolném množství PC založit přenosný uživatelský účet a pomocí čipové karty atd. se do aplikace přihlásit a dále s ní pracovat. Bez čipové karty však přihlášení k přenosnému uživatelskému účtu není možné.

Aktivace přenosného uživatelského účtu

Pro aktivaci přenosného uživatelského účtu je potřeba mít čipovou kartu s komerčním certifikátem, na který byl uživatelský účet založen (buďto na RA nebo správcem pečeti). K aktivaci přenosného uživatelského účtu dojde při prvním pokusu o přihlášení do RemoteSealProFi pomocí příslušné čipové karty s komerčním certifikátem. Tedy:

1. Uživatel zvolí přidání uživatelského profilu => přenosný profil
2. Vloží čipovou kartu, případně vybere příslušný certifikát
3. Zadá PIN
4. Aplikace detekuje, že tento uživatelský účet ještě nebyl aktivován a vyzve uživatele k volbě hesla pro službu RemoteSeal
5. Po dvojím zadání hesla proběhne aktivace a uživatel se může standardně přihlásit do aplikace.

Poznámka

To je případ i prvotní aktivace oprávněnou osobou, jež navštívila RA pro zřízení služby.

Fixní uživatelský účet

Fixní uživatelský účet je oproti tomu vázán na konkrétní PC, resp. na konkrétní uživatelský profil v OS Windows, na kterém proběhla aktivace a jinde se k němu není možné přihlásit.

K přihlášení však nejsou potřeba žádné fyzické markanty, postačuje:

- data uložená na daném PC (a uživatelském profilu Windows) jež vznikla při aktivaci
- heslo uživatele ke službě RemoteSeal

Použití fixních uživatelských účtů však vyžaduje použití doplňkového zabezpečení zdroje komunikace (viz níže).

Aktivace fixního uživatelského účtu

Po zřízení nového fixního uživatelského účtu (správcem pečetění) obdrží uživatel tzv. aktivační mail, který v příloze obsahuje tzv. aktivační soubor. Tento slouží pro provedení aktivace následovně:

1. Uživatel zvolí přidání uživatelského profilu => fixní profil
2. Vloží aktivační soubor (jež dostal mailem)
3. Následně mu na telefonní číslo (uvedené při zřízení účtu) přijde tzv. aktivační SMS kód
4. Tento kód uživatel přepíše do aplikace
5. V případě správného zadání je následně vyzván k volbě hesla pro službu RemoteSeal
6. Po dvojím zadání hesla proběhne aktivace a uživatel se může standardně přihlásit do aplikace.

Uživatelské role RemoteSealProFi

Jednotliví uživatelé aplikace RemoteSealProFi mají v rámci daného pečetíciho accountu dané organizace vždy jednu ze dvou rolí:

- **správce pečetění**
 - Má přístup do administrátorské sekce RemoteSealProFi, kde může:
 - spravovat instance RSeC (přidávání, (od)blokace, přejmenování, zrušení)
 - požádat o vydání následného pečetíciho certifikátu
 - vidět a nastavovat okamžik nasazení nového (následného) pečetíciho certifikátu
 - spravovat další uživatele pod daným pečetícím accountem (přidávání, (od)blokace, zrušení, nastavení role) *(a to vč. možnosti přidat dalšího správce pečetění)*
 - Může libovolně vytvářet kvalifikované elektronické pečetě.
- **běžný uživatel**
 - Nemá přístup do administrátorské sekce RemoteSealProFi.
 - Může libovolně vytvářet kvalifikované elektronické pečetě.

Aktivace RSeC

Komponenta RSeC pro autentizaci vůči systému RemoteSeal vyžaduje:

- přístupový soubor tzv. RSealAccessFile
- heslo (pro instanci RSeC definovanou daným přístupovým souborem)

Držitel certifikátu (organizace) může současně provozovat více různých aplikací, které pečetí pomocí stejného accountu RemoteSeal, tj. stejného pečetíciho certifikátu. Tedy může provozovat více samostatných instancí RSeC, přičemž pro každou je potřeba vygenerovat dvojici přístupový soubor + heslo.

Generování přístupového souboru provádí uživatel (typicky zaměstnanec dané organizace) s rolí správce pečetění dané organizace v administrátorské části aplikace RemoteSealProFi:

1. Uživatel se přihlásí do aplikace RemoteSealProFi
2. Otevře administrátorskou část aplikace => správa RSeC => Přidat nový
3. Pro ověření zadá své heslo a následně vyplní
 - název nové instance RSeC (určeno zejména pro interní identifikaci v rámci dané organizace - např.: "Spisová služba - server 1")
 - heslo pro novou instanci RSeC
 - znovu heslo pro novou instanci RSeC
4. RemoteSealProFi poté provede založení nové instance RSeC a po dokončení nabídne uložení vygenerovaného aktivačního souboru na disk

Do komponenty RSeC se pak přístupový soubor a heslo předávají přes API příslušné knihovny - způsob jejich vložení/uložení do příslušné aplikace je tedy odvislý od implementace v dané aplikaci. Z principu je možné, aby přístupový soubor "ležel" někde na disku daného stroje, na kterém probíhá pečetení přes RSeC. Heslo by však mělo být danou aplikací uloženo bezpečnějším způsobem a nikdy by nemělo ležet v plaintextu někde v souboru.

Volající aplikace pak předává přístupový soubor a heslo k němu pro každé pečetení, resp. pro každou inicializaci objektu třídy SealClient. RSeC si sám nezajišťuje žádnou persistenci přístupového souboru ani hesla.

Opečetění dokumentu

Opečetění dokumentu přes RSeC

1. Volající aplikace vytvoří instanci třídy SealClient z RSeC, které předá přístupový soubor a heslo k němu
2. Volající aplikace předá do RSeC 1 až N dokumentů k opečetění spolu s nastavením opečetění jednotlivých dokumentů (viditelný/neviditelný podpis, formát, přidání časového razítka, atp.)
3. RSeC připraví dokumenty k podpisu, založí pro každý dokument pečetící transakci, autorizuje použití privátního klíče na HSM modulu, získá z backendu vytvořenou podpisovou strukturu vč. případného časového razítka a sestaví kompletní podepsané dokumenty
4. Sestavené podepsané dokumenty RSeC vrátí volající aplikaci

Opečetění dokumentu přes RemoteSealProFi

1. Uživatel se přihlásí do aplikace RemoteSealProFi
2. Uživatel vybere "profil pečete" podle kterého chce pečetit
 - profil pečete jsou de-facto uložené parametry vytvářené pečete (viditelný podpis, vložení časového razítka, atp), které mohou sloužit jako fixně předepsané parametry pro druh dokumentu (např.: všechna potvrzení o studiu mají stejné parametry) - jako základní nastavení parametrů, které jsou pro daný případ uživatele následně upraveny a je možné je sdílet s dalšími uživateli pod stejným pečetícím accountem.
3. Volitelně uživatel upraví parametry pečete
4. Následně uživatel vybere dokumenty, které se mají opečetit a potvrdí
5. RemoteSealProFi postupně opečetí všechny vybrané dokumenty

Obnova pečetícího certifikátu

S předstihem před koncem platnosti aktuální pečetícího certifikátu (30, 15 a 5 dní) jsou uživatelé s rolí správce pečetení informováni e-mailem o blížícím se konci platnosti pečetícího certifikátu. Správce pečetení:

1. Se přihlásí do aplikace RemoteSealProFi a otevře administrátorskou část aplikace => správa pečetícího certifikátu
2. Stiskne tlačítko obnovit certifikát
3. Aplikace zajistí vytvoření žádosti o následný certifikát a zobrazí uživateli detail servisní transakce k podpisu žádosti o vydání následného certifikátu
4. Uživatel stiskne tlačítko podepsat a zadá své heslo k uživatelskému účtu ke službě RemoteSeal
5. Služba následně zajistí vydání následného pečetícího certifikátu a po jeho vydání naplánuje odložené nasazení nově vydaného pečetícího certifikátu (za + 15 dní)
6. Správce pečetení si může po vydání certifikátu v aplikaci zobrazit informace o novém certifikátu, uložit si nový certifikát do souboru, vidět přesný čas plánovaného nasazení nového certifikátu a tento čas může v aplikaci také změnit.

Podporované formáty podpisu

- **CAdES**
 - CAdES-B-B, CAdES-B-T
 - Dle normy EN 319 122, ve variantách:
 - Interní
 - Externí
- **PAdES**
 - PAdES-B-B, PAdES-B-T
 - Dle normy EN 319 142, ve variantách:
 - Neviditelný
 - Viditelný – Text/Obrázek/Text+Obrázek + volitelně obrázek na pozadí
- **XAdES**
 - XAdES-B a XAdES-T
 - XAdES Enveloping podle TS 103 171
 - XAdES Detached podle TS 103 171
 - XAdES DetachedExtern podle TS 103 171
 - XAdES Enveloped podle EN 319 132
 - XAdES Enveloping podle EN 319 132
 - XAdES Detached podle EN 319 132
 - XAdES DetachedExtern podle EN 319 132
- **ASiC-E XAdES**
 - ASiC-E XAdES-B a ASiC-E XAdES-T
 - Dle normy ETSI TS 103 174, přičemž:
 - Je možné opečetřit právě jeden datový objekt právě jednou kvalifikovanou pečeti

- Není podporováno rozšíření stávajícího ASiC-E souboru o další pečeť/podpis, ani několik podpisů/pečetí v rámci jednoho ASiC-E souboru.
- Pro soubory typu .txt, .pdf, .xml, .png je implicitně doplněn příslušný mimetype odpovídající dané příponě. Tuto implicitní volbu je možné v rozhraní explicitně přenastavit na jiný mimetype, popř. lze explicitní cestou nastavit mimetype pro ostatní (implicitně nepodporované) typy datových objektů.
- Samotná XAdES pečeť uvnitř ASiC-E kontejneru obsahuje pouze minimální nezbytně nutnou množinu podepisovaných a nepodepisovaných properties vyžadovanou danou ETSI normou.

Doplňkové zabezpečení zdroje komunikace

Pro jednotlivé pečetící accounty je možné nastavit doplňkové zabezpečení zdroje komunikace, které umožňuje omezit, "odkud" může daná aplikace pro daný account kontaktovat službu RemoteSeal - např.: že fixní uživatelské účty RemoteSealProFi musejí komunikovat přes určitou VPN mezi klientem a I.CA, nebo musí být tato komunikace zabezpečena mTLS spojením s konkrétním klientským certifikátem, atp.