MSMT-43914/2020

PŘÍKAZNÍ SMLOUVA O ZAJIŠTĚNÍ SLUŽEB CERTIFIKAČNÍ AUTORITY

uzavřená dle ust. § 2430 a násl. zákona č. 89/2012 Sb., občanský zákoník, v platném znění (dále jen „občanský zákoník“), mezi smluvními stranami, kterými jsou:

(dále jen „Smlouva“)

Česká republika – Ministerstvo školství, mládeže a tělovýchovy
se sídlem v Praze 1, Karmelitská 529/5, PSČ 118 12
za niž jednají: Ing. Václav Jelen, ředitel odboru informatiky a statistiky
Bc. Jan Frisch, ředitel odboru technické pomoci
IČ: 00022985
bankovní spojení: [redacted]
(dále jen **„příkazník“** nebo **„odběratel“**)

a

První certifikační autorita, a.s.
Sídlo: Podvinný mlýn 2178/6, 190 00 Praha 9
Jednající: Ing. Petr Budiš, Ph.D., MBA, předseda představenstva
Ing. Roman Kučera, člen představenstva
Zapsán v: obchodním rejstříku, vedeném Městským soudem v Praze, spisová značka B 7136
IČO: 26439395
DIČ: CZ26439395
Bankovní spojení: [redacted]
Číslo účtu:
Telefon:
(dále jen **„příkazce“** nebo **„dodavatel“** a společně jako **„smluvní strany“**)

v tomto znění:

Strany uzavírají v souladu s ustanovením § 2430 a násl. občanského zákoníku, nařízením Evropského parlamentu a Rady č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES („eIDAS“), zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, níže uvedeného dne, měsíce a roku tuto Smlouvu
o poskytování služeb příkazce a provozu registrační autority příkazníka pro vydávání kvalifikovaných certifikátů pro elektronický podpis (dále též „kvalifikovaných certifikátů“), komerčních certifikátů, systémových certifikátů a komerčních certifikátů pro server.

Tato Smlouva vzešla ze soutěže o veřejnou zakázku s názvem „**Zajištění služeb certifikační autority“**.

Obě smluvní strany se podpisem této Smlouvy dohodly na spolupráci, jejímž cílem je zajištění veškerých činností nutných pro poskytování elektronických časových razítek, vydávání kvalifikovaných a komerčních certifikátů příkazce pro potřeby příkazníka, vytváření

kvalifikovaných elektronických pečetí na dálku a ověřování platnosti kvalifikovaných elektronických podpisů a pečetí. Smlouva má pět částí:

- Část první – poskytování certifikačních služeb příkazce pro příkazníka,
- Část druhá – provozování registrační autority příkazníka,
- Část třetí – vydávání elektronických časových razítek,
- Část čtvrtá – vytváření kvalifikovaných elektronických pečetí na dálku,
- Část pátá – ověřování platnosti kvalifikovaných elektronických podpisů a pečetí

ČÁST PRVNÍ – poskytování certifikačních služeb příkazce pro příkazníka

1. Úvodní ustanovení

1.1. Příkazce prohlašuje, že je kvalifikovaným dodavatelem služeb vytvářejících důvěru podle zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, a podle nařízení Evropského parlamentu a Rady (EU) č. 910/2014, o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES.

1.2. Příslušné doložení statutu kvalifikovaného dodavatele služeb vytvářejících důvěru tvoří přílohu č. 3 k této Smlouvě.

2. Předmět Smlouvy

2.1. Předmětem této Smlouvy je vydávání všech typů certifikátů podle potřeb příkazníka, tj. vydávání kvalifikovaných certifikátů pro elektronický podpis podle nařízení Evropského parlamentu a Rady (EU) č. 910/2014, o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES, a zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, systémových certifikátů a komerčních certifikátů včetně komerčních certifikátů pro server pro zaměstnance příkazníka, prostřednictvím příkazce.

2.2. Kvalifikované a komerční certifikáty budou vydávány prostřednictvím dvou pracovišť – registrační autority (RA) příkazníka, tedy na RA provozovaných příkazníkem. Taktéž mohou být vydávány prostřednictvím registrační autority příkazce na základě výslovného požadavku a objednávky příkazníka.

2.3. Předmětem této Smlouvy je též podle potřeb příkazníka vydávání kombinace dvou certifikátů – kvalifikovaného a komerčního zajišťující možnost využívat službu elektronického podpisu (osobní kvalifikovaný certifikát) a zároveň službu autentizace a šifrování (komerční certifikát). Pro vydávání této kombinace dvou certifikátů platí stejné požadavky jako pro vydání Kvalifikovaného certifikátu.

2.4. Kvalifikovaným certifikátem se rozumí certifikát ve smyslu odst. 15, článku 3 nařízení Evropského parlamentu a Rady (EU) č. 910/2014, o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES, u něhož je kromě totožnosti žadatele ověřován také jeho zaměstnanecký / služební poměr k příkazníkovi, a to předložením potvrzení

o zaměstnaneckém / služebním poměru podepsaného zaměstnancem příkazníka, pro nějž má být kvalifikovaný certifikát vydán, a osobou oprávněnou jednat za příkazníka.

2.5. Elektronické žádosti o kvalifikované certifikáty musí splňovat naplnění položky jedinečného jména, a to přesné znění názvu organizace, název organizační jednotky příkazníka a název funkce zaměstnance příkazníka variabilně dle potřeb příkazníka, dle potvrzení o zaměstnaneckém / služebním poměru.

2.6. Komerčním certifikátem se rozumí certifikát, u něhož je kromě totožnosti žadatele ověřován také jeho zaměstnanecký / služební poměr k příkazníkovi, a to předložením potvrzení o zaměstnaneckém / služebním poměru podepsaného zaměstnancem příkazníka, pro nějž má být komerční certifikát vydán, a osobou oprávněnou jednat za příkazníka.

2.7. Elektronické žádosti o komerční certifikáty musí splňovat naplnění položky jedinečného jména, a to přesné znění názvu organizace, název organizační jednotky příkazníka a název funkce zaměstnance příkazníka variabilně dle potřeb příkazníka, dle potvrzení o zaměstnaneckém / služebním poměru.

2.8. Systémovým certifikátem se rozumí certifikát vydaný podle zákona č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů, ve znění účinném přede dnem nabytí účinnosti zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce.

2.9. Komerčním certifikátem pro server se rozumí SSL/TLS certifikát pro důvěryhodné ověření domény příkazníka.

2.10. Kvalifikovaným certifikátem pro elektronickou pečeť se rozumí certifikát ve smyslu odst. 30, článku 3 nařízení Evropského parlamentu a Rady (EU) č. 910/2014, o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES.

3. Oprávněné osoby příkazníka

3.1. Jednotlivá potvrzení o zaměstnaneckém / služebním poměru podle předcházejícího článku jsou jménem příkazníka oprávněny podepisovat k tomuto úkonu pověřené osoby. Změna pověření musí být příkazci prokazatelně doručena nejpozději 3 pracovní dny před nabytím účinnosti této změny, pokud se smluvní strany v jednotlivých případech nedohodnou jinak.

4. Povinnosti příkazce

4.1. Certifikáty dle článku 2.3 budou vydávány zaměstnancům příkazníka při současném splnění následujících požadavků:

a) předložení dokladů totožnosti,
b) předání potvrzení o zaměstnaneckém / služebním poměru, jehož součástí je souhlas příkazníka kvalifikovaný certifikát vydat, a které je podepsáno osobou oprávněnou podle této Smlouvy za příkazníka jednat,
c) předložení elektronické žádosti o vydání kvalifikovaného a komerčního certifikátu příkazci, jejíž naplnění položek odpovídá podmínkám této Smlouvy.

4.2. Kvalifikované certifikáty budou vydávány zaměstnancům příkazníka při současném splnění následujících požadavků:

a) předložení dokladů totožnosti,
b) předání potvrzení o zaměstnaneckém / služebním poměru, jehož součástí je souhlas příkazníka kvalifikovaný certifikát vydat, a které je podepsáno osobou oprávněnou podle této Smlouvy za příkazníka jednat,
c) předložení elektronické žádosti o vydání kvalifikovaného certifikátu příkazci, jejíž naplnění položek odpovídá podmínkám této Smlouvy.

4.3. Komerční certifikáty budou vydávány zaměstnancům příkazníka při současném splnění následujících požadavků:

a) předložení dokladů totožnosti,
b) předání potvrzení o zaměstnaneckém / služebním poměru, jehož součástí je souhlas příkazníka komerční certifikát vydat, a které je podepsáno osobou oprávněnou podle této Smlouvy za příkazníka jednat,
c) předložení elektronické žádosti o vydání komerčního certifikátu příkazci, jejíž naplnění položek odpovídá podmínkám této Smlouvy.

4.4. Systémové certifikáty budou vydávány příkazníkovi dle podmínek stanovených příkazcem.

4.5. Komerční certifikáty pro server budou vydávány příkazníkovi dle podmínek stanovených příkazcem.

4.6. Kvalifikované certifikáty pro elektronickou pečeť budou vydávány příkazníkovi dle podmínek stanovených příkazcem.

4.7. Certifikáty dle článku 2.3, kvalifikované a komerční certifikáty, kvalifikované certifikáty pro elektronickou pečeť, systémové certifikáty a komerční certifikáty pro server budou vydávány podle potřeb příkazníka počínaje dnem následujícím po podpisu této Smlouvy, a to po celou dobu její platnosti.

4.8. Příkazce ručí za jedinečnost identifikačních údajů žadatele, uvedených v kvalifikovaných a v komerčních certifikátech, vydaných podle této Smlouvy.

4.9. Příkazce nebude akceptovat žádosti o vydání kvalifikovaných a komerčních certifikátů, které nesplňují naplnění položek žádosti o kvalifikovaný certifikát a žádosti o komerční certifikát.

4.10. Příkazce se zavazuje poskytovat žadatelům o certifikáty nezbytnou součinnost a podporu.

4.11. Příkazce se zavazuje zajišťovat provoz vydávání kvalifikovaných a komerčních certifikátů v pracovních dnech od 8:00 hod. do 16:00 hod.

4.12. Příkazce se zavazuje zveřejňovat na svých webových stránkách seznam zneplatněných kvalifikovaných certifikátů v intervalu ne delším, než každých 12 hodin, a komerčních certifikátů v intervalu ne delším, než každých 24 hodin.

ČÁST DRUHÁ – provozování registrační autority příkazníka

5. Úvodní ustanovení

5.1. Příkazce je společností, jejímž předmětem činnosti jsou služby kvalifikovaného dodavatele služeb vytvářejících důvěru.

5.2. Příkazce je kvalifikovaným dodavatelem služeb vytvářejících důvěru podle zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce. Oznámení o změně tohoto statutu je příkazce povinen zaslat prostřednictvím provozovatele poštovních služeb / datové schránky příkazce do datové schránky příkazníka, a to do 10 pracovních dní od změny statutu. Ztráta statutu kvalifikovaného dodavatele služeb vytvářejících důvěru je důvodem k okamžitému ukončení této Smlouvy.

6. Předmět Smlouvy

6.1. Příkazník se tímto zavazuje jménem příkazce zajišťovat služby provozu registrační autority. Provozováním služeb registrační autority se pro účely této Smlouvy rozumí:

a) poskytnutí vhodného pracoviště (dále jen „registrační autorita“). Technické, procesní a bezpečnostní požadavky, které musí registrační autorita splňovat, jsou uvedeny v platné legislativě a v dokumentech dle přílohy č. 1 této Smlouvy, která tvoří nedílnou součást této Smlouvy.
b) zajištění služeb registrační autority prostřednictvím zaměstnanců příkazníka (dále jen „operátor registrační autority“). Příkazce udělí určeným zaměstnancům příkazníka oprávnění k zajišťování služeb provozu registrační autority.
c) uvolnění určených operátorů registrační autority k účasti na školení tak, aby byli schopni vykonávat své povinnosti řádně, v souladu s platnou legislativou a dalšími předpisy, které upravují pravidla provozování registrační autority, včetně vnitřních předpisů, upravujících výkon činností příkazce v oblasti, která je předmětem této Smlouvy.

7. Další specifikace předmětu činnosti

7.1. Činnost uvedená v čl. 6. zahrnuje zejména:

a) podávání a vyřizování žádostí o kvalifikované certifikáty,
b) podávání a vyřizování žádostí o komerční certifikáty,
c) podávání a vyřizování žádostí o systémové certifikáty,
d) podávání a vyřizování žádostí o kvalifikované certifikáty pro elektronickou pečeť,
e) podávání a vyřizování žádostí o komerční certifikáty pro server.

7.2. Příkazce poskytne příkazníkovi programové vybavení pro dvě registrační autority a současně poskytuje příkazníkovi právo užívání tohoto programového vybavení ve smyslu § 46 zákona č. 121/2000 Sb., ve znění pozdějších předpisů, tj. příkazce touto Smlouvou poskytuje příkazníkovi nevýhradní, nepřenositelnou a časově neomezenou SW licenci k používanému programovému vybavení registračních autorit včetně práva užívání všech upgrade a update tohoto programového vybavení. Na základě této Smlouvy je licence poskytována bezúplatně.

7.3. Příkazce poskytne příkazníkovi nezbytné hardwarové vybavení registrační autority pro dvě pracoviště registrační autority

7.4. Příkazce provede před zahájením činnosti registrační autority potřebné zaškolení zaměstnanců příkazníka (budoucích operátorů), odpovědných za provoz registrační autority. Školení bude provedeno v termínu dohodnutém mezi příkazníkem a příkazcem. Školení bude zaměřeno na veškeré oblasti znalostí, které jsou potřebné pro splnění podmínek uvedených v příloze č. 1 této Smlouvy. Případné školení dalších operátorů registrační autority, pokud by tato potřeba vznikla, bude dohodnuto rovněž mezi příkazníkem a příkazcem způsobem nevyžadujícím písemnou formu.

7.5. Zřízení a zahájení činnosti registrační autority bude stvrzeno protokolem o předání vybavení registrační autority, který bude podepsán oprávněnými zástupci obou stran a který připraví příkazce v počtu dvou vyhotovení (příkazce a příkazník obdrží po jednom vyhotovení). Oprávněnými zástupci ve všech smluvních záležitostech jsou za stranu příkazce Ing. Lucie Urbanová, za stranu příkazníka Ing. Jan Výška nebo Ing. Robert Basl.

7.6. Předání veškerého HW a SW vybavení registrační autority příkazníkovi bude provedeno na základě předávacích a přejímacích protokolů, které připraví příkazce v počtu dvou vyhotovení (příkazce a příkazník obdrží po jednom vyhotovení).

8. Práva a povinnosti příkazníka

8.1. Příkazník je povinen postupovat při plnění této Smlouvy podle pokynů příkazce a v souladu s jeho zájmy. Příkazník je povinen oznámit příkazci všechny okolnosti, které zjistil při zařizování záležitostí příkazce podle této Smlouvy a které mohou mít vliv na změnu pokynů příkazce. Příkazník činí tato oznámení písemně cestou datové schránky.

8.2. Od pokynů příkazce se může příkazník odchýlit, jen je-li to naléhavě nezbytné v zájmu příkazce a příkazník nemůže včas obdržet jeho souhlas. Ani v těchto případech se však příkazník nesmí od pokynů odchýlit, jestliže je to výslovně zakázáno touto Smlouvou nebo obecně závaznými právními předpisy, které upravují předmět činnosti příkazce, tak jak je popsán v čl. 5 této Smlouvy.

8.3. Příkazník odpovídá příkazci za újmu na jmění, která mu vznikne zaviněním příkazníka v souvislosti s plněním této Smlouvy s výjimkou újmy na jmění, která vznikne v důsledku nedostatečné informovanosti příkazníka ze strany příkazce.

8.4. Příkazník 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 příkazce v termínech odsouhlasených příkazníkem. Školení zajistí a jeho cenu uhradí příkazce.

8.5. Příkazník prohlašuje, že byl seznámen s právními předpisy upravujícími činnosti, které jsou předmětem této Smlouvy, a to s obecně závaznými právními předpisy (zejména se zákonem č. 110/2019 Sb., o zpracování osobních údajů a nařízením Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES), tak i s vnitřními předpisy upravujícími tuto činnost ve společnosti příkazce.

8.6. Příkazník pověří osoby odpovědné za provoz registrační autority. Tyto osoby přebírají od příkazce potřebné vybavení a v rozsahu činností registrační autority spolupracují s příkazcem. V rámci této součinnosti je příkazník povinen poskytovat veškeré informace nutné k zajištění provozu registrační autority. Rozsah a forma této součinnosti tvoří přílohu č. 2 této Smlouvy a je její nedílnou součástí.

8.7. Po proškolení dle bodu 8.4 tohoto článku příkazce vystaví osobám pověřeným pro činnost registrační autority oprávnění.

8.8. Příkazník se zavazuje při provozu registrační autority dodržovat příslušné platné ustanovení příkazce, a to ve znění platném k okamžiku podpisu této Smlouvy. Za škody vzniklé v souvislosti s jejím nedodržením nese plně a výlučně povinnost k náhradě příkazník.

8.9. Příkazník nese plně povinnost k náhradě škody způsobené svými zaměstnanci při provozování služeb registrační autority, jakož i povinnost k náhradě škody způsobené nesprávným postupem osob pověřených podle této Smlouvy odpovědností za provozování služeb registrační autority.

8.10. Příkazník se zavazuje hardwarové vybavení, na kterém je provozována registrační autorita, zajistit proti neoprávněnému přístupu, a dále pak provádět jeho HW a SW administraci pouze oprávněnou osobou. Konfigurace operačního systému, nasazeného na uvedeném zařízení, bude v souladu s bezpečnostními požadavky uvedenými v příloze č. 1 Smlouvy.

8.11. Případné změny příslušných platných ustanovení příkazce budou zasílány kontaktní osobě příkazníka a na email [redacted] formou elektronické nebo písemné komunikace, a to v dostatečném časovém předstihu. Tyto změny jsou vůči příkazníkovi účinné okamžikem potvrzení ze strany příkazníka. Pokud příkazník nebude se změnou příslušných platných ustanovení příkazce souhlasit, oznámí tuto skutečnost cestou datové schránky ve lhůtě 3 pracovních dnů od předání příkazce, a ten je oprávněn Smlouvu vypovědět. Výpovědní doba v tomto případě činí 15 dnů a začíná běžet dnem následujícím po dni, ve kterém bylo příkazci oznámeno, že příkazník se změnou nesouhlasí.
V takovémto případě nejsou změny pro příkazníka účinné.

9. Práva a povinnosti příkazce

9.1. Příkazce se zavazuje poskytovat příkazníkovi potřebné informace pro plnění předmětu této Smlouvy.

9.2. Příkazce se zavazuje na své náklady školit zaměstnance příkazníka tak, aby byli řádně poučeni a schopni plnit činnosti podle této Smlouvy.

9.3. Příkazce má právo přístupu do dokumentace registrační autority v rozsahu dokumentace stanovené v příloze č. 1 této Smlouvy. Jakýkoli přístup musí být stvrzen písemným protokolem o obsahu přístupu a podepsán oprávněnými zástupci obou smluvních stran.

9.4. Příkazce v dostatečném časovém předstihu příkazníkovi oznámí vydání nové certifikační politiky, a zda změna certifikační politiky vyvolá nutnost nového proškolení operátorů registrační autority. Na změnu certifikační politiky je příkazce povinen upozornit

příkazníka cestou datové schránky. Tímto není dotčeno ustanovení čl. 8 bodu 11 této Smlouvy.

9.5. Příkazce nebude akceptovat žádosti zaměstnanců příkazníka podané z registrační autority směrem k příkazci, které nebudou splňovat naplnění položek žádosti o kvalifikovaný certifikát podle podmínek této Smlouvy.

9.6. Příkazce se zavazuje poskytovat příkazníkovi podporu pro chod registrační autority a pomoc pracovníkům registrační autority při řešení reklamací.

9.7. Příkazce poskytuje službu technické podpory uživatelů, řešení nestandardních situací a poradenství související s předmětem této Smlouvy prostřednictvím e-mailové adresy [redacted]Cena za poskytování technické podpory je již zahrnuta do ceny plnění předmětu této Smlouvy.

10. Cenové podmínky zřízení a vybavení registrační autority

10.1. Příkazce zřídí a vybaví registrační autoritu na základě podmínek této Smlouvy u příkazníka za 0 Kč bez DPH.

10.2. Cenové podmínky vydávání certifikátů pro zaměstnance příkazníka jsou uvedeny v obecné části této Smlouvy.

ČÁST TŘETÍ – vydávání elektronických časových razítek

11. Úvodní ustanovení

11.1. Dodavatel je oprávněn vydávat kvalifikovaná elektronická časová razítka dle nařízení Evropského parlamentu a Rady (EU) č. 910/2014, o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES.

12. Předmět Smlouvy

12.1. Předmětem plnění této Smlouvy je vydávání kvalifikovaných elektronických časových razítek a archivních kvalifikovaných elektronických časových razítek (dále též „archivní časová razítka“) pro potřeby odběratele v souladu s platnou politikou vydávání časových razítek (dále jen „PTSA“), která je vždy v aktuální verzi k dispozici na URL https://www.ica.cz/certifikacni-politika a současně závazek odběratele za odebraná kvalifikovaná časová razítka uhradit sjednanou cenu.

12.2. Kvalifikovaná elektronická časová razítka a archivní časová razítka (dále společně též „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 certifikátem, jménem a heslem nebo IP adresou.

13. Povinnosti odběratele

13.1. Odběratel se zavazuje při využívání časových razítek vydaných na základě této Smlouvy zabezpečit dodržování platné Politiky vydávání časových razítek (algoritmus RSA) (dále jen „PTSA“). Aktuální verze PTSA 2.04. Veškeré změny a doplňky uvedeného dokumentu jsou vůči odběrateli účinné okamžikem předání změn a doplňků na e-mailovou adresu: 

13.2. Odběratel nese plnou a výlučnou odpovědnost za újmy na jmění vzniklé v souvislosti s nedodržením PTSA.

13.3. Odběratel se zavazuje neposkytovat plnění poskytnuté dodavatelem dalším osobám bez souhlasu dodavatele.

14. Povinnosti dodavatele

14.1. Dodavatel se zavazuje příkazníkovi jako oprávněnému žadateli o služby časové autority poskytovat danou komplexní službu vydávání archivních časových razítek v souladu s platnou PTSA a veškerými relevantními právními předpisy, a to bez omezení počtu vydaných časových razítek po celou dobu platnosti Smlouvy.

14.2. Dodavatel se zavazuje zajistit ověřitelnost platnosti archivního časového razítka po dobu 10 let od vydání každého prvotního archivního časového razítka vydaného po datu účinnosti této Smlouvy. Výsledek ověření je ukládán v interních systémech dodavatele. Ukončení smluvního vztahu odstoupením, výpovědí nebo jiným způsobem se nedotýká doby trvání závazku dodavatele plynoucího z tohoto ustanovení.

14.3. Dodavatel se zavazuje poskytnout k datu podpisu této Smlouvy webovou on-line aplikaci dostupnou příkazníkovi k ověření stavu archivního časového razítka po zadání SN razítka či hash dokumentu.

14.4. Dodavatel se dále zavazuje, že bude v období 10 let od vydání prvního archivního časového razítka vydaného po datu účinnosti této Smlouvy na vyžádání příkazníka poskytovat dokumenty nutné pro ověření platnosti časového razítka dle odstavce 14.2:

- archivní časová razítka a data nutná pro jejich ověření,
- protokol o archivních časových razítkách označený uznávanou elektronickou značkou/pečetí dodavatele, kterou stvrzuje, že archivní časová razítka jsou technicky ověřitelná v době podání žádosti o protokol,
- kompletní strukturu pro potřeby např. soudního znalce.

14.5. Ukončení smluvního vztahu odstoupením, výpovědí nebo jiným způsobem se nedotýká doby trvání závazku dodavatele plynoucího z odstavce 14.4.

14.6. Dodavatel se taktéž zavazuje:

- zajistit, aby časová razítka obsahovala všechny náležitosti stanovené příslušnými obecně závaznými právními předpisy,
- zajistit, aby časový údaj vložený do časového razítka odpovídal hodnotě koordinovaného světového času při vytváření časového razítka,

- zajistit, aby data v elektronické podobě, která jsou předmětem žádosti o vydání časového razítka, jednoznačně odpovídala datům v elektronické podobě obsaženým ve vydaném časovém razítku,
- přijmout odpovídající opatření proti padělání časových razítek,
- poskytovat na vyžádání třetím osobám podstatné informace o podmínkách pro využívání časových razítek, včetně omezení pro jejich použití; tyto informace lze poskytovat elektronicky.

14.7. Dodavatel se zavazuje poskytovat příkazníkovi podporu zaručenou platnou PTSA.

14.8. Dodavatel se zavazuje poskytovat službu vydávání časových razítek s dostupností 98 % za běžný kalendářní rok v nepřetržitém režimu 24 hodin denně 7 dní v týdnu (365 x 24) po celou dobu platnosti a účinnosti Smlouvy.

14.9. Dodavatel prohlašuje, že vydávání časových razítek odpovídá všem požadavkům vyplývajícím z právních předpisů, které se na plnění vztahují.

14.10. Dodavatel se zavazuje poskytovat službu vydávání časových razítek s propustností 2 ks časových razítek za sekundu.

14.11. Dodavatel se zavazuje sledovat stav kryptografických algoritmů používaných pro zajištění služby časových razítek a v případě jejich oslabení neprodleně informovat příkazníka a seznámit jej s riziky z toho vyplývajícími. Současně se dodavatel zavazuje používat vždy kryptografické algoritmy v souladu s právními předpisy, mezinárodními normami a aktuálními bezpečnostními doporučeními.

ČÁST ČTVRTÁ – vytváření kvalifikovaných elektronických pečetí na dálku

15. Úvodní ustanovení

15.1. Dodavatel prohlašuje, že je kvalifikovaným poskytovatelem služeb vytvářejících důvěru podle Nařízení Evropského parlamentu a Rady č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES („eIDAS“) a zákona
č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce pro oblast vydávání kvalifikovaných certifikátů pro elektronické pečetě. Dodavatel dále prohlašuje, že poskytovaná služba vytváření kvalifikovaných elektronických pečetí na dálku byla posouzena orgánem dohledu a používaný kvalifikovaný prostředek pro vytváření elektronických pečetí je spravován kvalifikovaným poskytovatelem služeb vytvářejících důvěru v souladu se všemi požadavky na správu v režimu QCQSCDManagedOnBehalf
(https://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCQSCDManagedOnBehalf/).

16. Předmět Smlouvy

16.1. Předmětem plnění této Smlouvy je zajištění provozu služby vytváření kvalifikovaných elektronických pečetí na dálku v souladu s platnou politikou služby I.C A RemoteSeal, která je vždy v aktuální verzi k dispozici na URL https://www.ica.cz/certifikacnipolitika.

17. Povinnosti dodavatele

17.1. Dodavatel poskytuje odběrateli službu vytváření kvalifikovaných elektronických pečetí na dálku v souladu s bodem 52 recitálu, články 29 a 39, Přílohou II body 3 a 4 a Přílohou III nařízení 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 (eIDAS). Popis služby je uveden v příloze č. 4 této Smlouvy.

17.2. Dodavatel se zavazuje poskytovat službu vytváření kvalifikovaných elektronických pečetí na dálku v režimu 24/7, tedy 24 hodin denně, 7 dní v týdnu, s SLA 98 % a kapacitou až 30 vytvořených pečetí za minutu.

17.3. Dodavatel se zavazuje poskytovat:

a) technickou podporu při provozu služby, řešení nestandardních situací a poradenství související s předmětem této Smlouvy prostřednictvím e-mailové adresy [redacted]
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 [redacted]
c) právní a technickou aktuálnost komponenty pro zajištění komunikace s dodavatelem, jakož i celou službu vytváření kvalifikovaných elektronických pečetí na dálku, s relevantními právními a technickými předpisy a normami v návaznosti na eIDAS.
d) za účelem otestování nových verzí služby vytváření kvalifikovaných elektronických pečetí na dálku před nasazením do ostrého provozu službu vytváření kvalifikovaných elektronických pečetí na dálku v testovacím prostředí s funkcionalitou obdobnou službě vytváření kvalifikovaných elektronických pečetí na dálku v produkčním prostředí, pro testovací prostředí platí SLA 95 % a kapacita 10 vytvořených pečetí za minutu.

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

18. Povinnosti odběratele

18.1. Dodavatel poskytuje službu vytváření kvalifikovaných elektronických pečetí na dálku v souladu se závazným prohlášením uvedeným v článku 15. odst. 15.1. této Smlouvy. Odběratel se zavazuje zabezpečit dodržování platné Politiky služby vytváření kvalifikovaných elektronických pečetí na dálku („Politika“). Veškeré změny a doplňky

této Politiky jsou vůči odběrateli účinné po podpisu dodatku k této Smlouvě podepsaného zástupci obou smluvních stran.

18.2. Odběratel je povinen nahradit újmu na jmění vzniklou v souvislosti s nedodržením Politiky.

18.3. Odběratel se zavazuje neposkytovat plnění poskytnuté dodavatelem dalším osobám bez souhlasu dodavatele a nezneužívat poskytování služeb dodavatele.

19. Smluvní cenové podmínky

19.1. Cena za poskytování služby vytváření kvalifikovaných elektronických pečetí na dálku, 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 připočteno 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	1000	4,00
101 – 300	2000	3,50
301 – 500	3000	3,00
501 – 1.000	5000	2,50
1.001 – 3.000	7000	2,10
3.001 – 5.000	9000	1,70
5.001 – 10.000	11000	1,40
10.001 – 30.000	14000	1,10
30.001 – 50.000	17000	0,80
50.001 – 100.000	21000	0,50
100.001 – 300.000	24000	0,30
300.001 – 500.000	29000	0,20

více než 500.000	35000	0,16

19.2. Ceny uvedené v odst. 1. tohoto článku jsou cenami neměnnými, nejvýše přípustnými a zahrnují veškeré náklady dodavatele související s poskytováním služby vytváření kvalifikovaných elektronických pečetí na dálku. Ceny mohou být změněny pouze v souvislosti se změnou daňových předpisů týkající se DPH, a to nejvýše o částku odpovídající této legislativní změně.

19.3. Úhrada poskytování služby vytváření kvalifikovaných elektronických pečetí na dálku bude prováděna vždy jednou měsíčně zpětně za uplynulý kalendářní měsíc, v němž dodavatel vytvořil 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. 19.1. + paušální poplatek v příslušném pásmu. DPH bude vyjádřeno dle aktuálně platné legislativy.

19.4. Dodavatel je povinen vystavit řádný daňový doklad do 15. dne kalendářního měsíce následujícího po kalendářním měsíci, za který je účtována cena za poskytování služby vytváření kvalifikovaných elektronických pečetí na dálku. Příkazník umožňuje elektronické zasílání faktur na adresu: [redacted]

19.5. Odběratel je povinen uhradit daňové doklady převodem na účet dodavatele do 30 dnů ode dne doručení daňového dokladu, vystaveného dodavatelem, na adresu sídla dodavatele a doručeného písemně na adresu sídla dodavatele podle údajů v této Smlouvě. Daňové doklady doručené mezi 15. prosincem a 15. únorem následujícího kalendářního roku mají splatnost v délce 60 dnů.

20. Sankční ustanovení, odstoupení od Smlouvy

20.1. V případě zaviněného nedodržení parametru SLA dostupnosti služby vytváření kvalifikovaných elektronických pečetí na dálku uvedeného v článku 17. odstavci 17.2. této Smlouvy, tj. pokud dostupnost služby klesne pod 98 % za kalendářní den, je dodavatel povinen uhradit odběrateli smluvní pokutu ve výši 1.000,- Kč bez DPH za každých započatých 0,1 %, o kterých klesne dostupnost poskytované služby pod požadovanou hodnotu. Měsíční výše smluvní pokuty však nepřesáhne výši měsíční ceny za poskytování služby.

20.2. V případě nesplnění povinností uvedených v článku 17. odstavci 17.3. písm. a) a b) této Smlouvy je dodavatel povinen uhradit odběrateli smluvní pokutu ve výši 1.000,- Kč bez DPH za každé takové porušení.

20.3. V případě nesplnění povinností uvedených v článku 17. odstavci 17.3. písm. c) tohoto ujednání je dodavatel povinen uhradit odběrateli smluvní pokutu ve výši 10.000,- Kč bez DPH za každé takové porušení.

ČÁST PÁTÁ – ověřování platnosti kvalifikovaných elektronických podpisů a pečetí

21. Úvodní ustanovení

21.1. Dodavatel prohlašuje, že je kvalifikovaným poskytovatelem služeb vytvářejících důvěru podle Nařízení Evropského parlamentu a Rady č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES („eIDAS“) a zákona
č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, pro oblast vydávání kvalifikovaných certifikátů pro elektronické podpisy, kvalifikovaných elektronických časových razítek, kvalifikovaných certifikátů pro elektronické pečetě a kvalifikované služby ověřování platnosti kvalifikovaných elektronických podpisů a pečetí.

22. Předmět Smlouvy

22.1. Předmětem plnění této Smlouvy je zajištění provozu kvalifikované služby ověřování platnosti kvalifikovaných elektronických podpisů a pečetí v souladu s platnou Politikou kvalifikované služby ověřování platnosti kvalifikovaných elektronických podpisů
a pečetí, která je vždy v aktuální verzi k dispozici na https://www.ica.cz/certifikacni-politika.

23. Povinnosti dodavatele

23.1. Dodavatel poskytuje odběrateli kvalifikovanou službu ověřování platnosti kvalifikovaných elektronických podpisů a pečetí v souladu s články 32, 33 a 40 nařízení 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 (eIDAS). Popis služby je uveden v příloze č. 5 této Smlouvy.

23.2. Dodavatel se zavazuje poskytovat službu ověřování platnosti kvalifikovaných elektronických podpisů a pečetí v režimu 24/7, tedy 24 hodin denně, 7 dní v týdnu, s SLA 98 % a kapacitou až 100 ověření za minutu.

23.3. Dodavatel se zavazuje poskytovat:

a) technickou podporu při provozu služby, řešení nestandardních situací a poradenství související s předmětem této Smlouvy prostřednictvím e-mailové adresy [redacted] a telefonní linky [redacted]
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 [redacted]
c) právní a technickou aktuálnost komponenty pro zajištění komunikace s dodavatelem, jakož i celou službu ověřování platnosti kvalifikovaných elektronických podpisů a pečetí, s relevantními právními a technickými předpisy a normami v návaznosti na eIDAS.
d) za účelem otestování nových verzí služby ověřování platnosti kvalifikovaných elektronických podpisů a pečetí před nasazením do ostrého provozu službu ověřování platnosti kvalifikovaných elektronických podpisů a pečetí v testovacím prostředí

s funkcionalitou obdobnou službě ověřování platnosti kvalifikovaných elektronických podpisů a pečetí v produkčním prostředí, pro testovací prostředí platí SLA 95 % a kapacita 10 ověření za minutu.

23.4. Dodavatel garantuje a nese odpovědnost za výsledek ověření platnosti elektronického podpisu a elektronické pečetě pouze za předpokladu, že data nutná k ověření (odeslána do prostředí dodavatele), generována komponentou dodanou dodavatelem, nebyla jakkoliv pozměněna a nebylo s nimi nijak manipulováno. Pro kontrolu integrity odesílaných dat z prostředí odběratele a dat z prostředí dodavatele využije dodavatel aplikaci, která v případě sporu porovná hashe spočtené z jednotlivých souborů komponentou dodavatele (po kontrole autenticity komponenty pomocí hashe) s hashi přijatými v prostředí dodavatele. Pokud budou hashe totožné, lze konstatovat, že data byla generována originální komponentou dodavatele, jsou správná a nebyla pozměněna.

24. Povinnosti odběratele

24.1. Dodavatel poskytuje službu ověřování platnosti kvalifikovaných elektronických podpisů a pečetí v souladu se závazným prohlášením uvedeným v článku 21., odstavci 21.1. této Smlouvy. Odběratel se zavazuje zabezpečit dodržování platné Politiky kvalifikované služby ověřování platnosti kvalifikovaných elektronických podpisů a pečetí („Politika“). Veškeré změny a doplňky této Politiky jsou vůči odběrateli účinné po podpisu dodatku k této Smlouvě podepsaného zástupci obou smluvních stran.

24.2. Odběratel je povinen nahradit újmu na jmění vzniklou v souvislosti s nedodržením Politiky.

24.3. Odběratel se zavazuje neposkytovat plnění poskytnuté dodavatelem dalším osobám bez souhlasu dodavatele a nezneužívat poskytování služeb dodavatele.

25. Smluvní cenové podmínky

25.1. Cena za poskytování služby ověřování platnosti kvalifikovaných elektronických podpisů a pečetí bude stanovena podle počtu provedených a poskytnutých ověření v daném kalendářním měsíci podle příslušného objemového pásma, a to jako součin „Ceny za 1 ověření Kč bez DPH“ a počtu skutečně provedených a poskytnutých ověření v příslušném pásmu dle přiloženého rozpisu za kalendářní měsíc. K této ceně bude připočteno DPH podle aktuálně platných předpisů.

Počet pečetění od – do za měsíc	Cena za 1 ověření Kč bez DPH
1 – 100	7,00
101 – 500	6,00

501 – 1000	5,10
1001 – 5.000	4,25
5.001 – 10.000	3,40
10.001 – 50.000	1,70
50.001 – 100.000	1,275
100.001 – 300.000	1,02
300.001 – 500.000	0,85
500.001 – 1.000.000	0,68
více než 1.000.000	0,64

25.2. Ceny uvedené v odst. 1. tohoto článku jsou cenami neměnnými, nejvýše přípustnými a zahrnují veškeré náklady dodavatele související s poskytováním služby ověřování platnosti kvalifikovaných elektronických podpisů a pečetí. Ceny mohou být změněny pouze v souvislosti se změnou daňových předpisů týkající se DPH, a to nejvýše o částku odpovídající této legislativní změně.

25.3. Úhrada poskytování služby ověřování platnosti kvalifikovaných elektronických podpisů a pečetí bude prováděna vždy jednou měsíčně zpětně za uplynulý kalendářní měsíc, v němž dodavatel kvalifikované elektronické podpisy a pečetě ověřil, a to podle počtu skutečně provedených a poskytnutých ověření. Daňový doklad bude obsahovat počet skutečně provedených a poskytnutých ověření; cena bude stanovena jako součin „Ceny za 1 ověření Kč bez DPH“ a počtu skutečně provedených a poskytnutých ověření v příslušném pásmu za kalendářní měsíc dle rozpisu uvedeného v odst. 25.1. DPH bude vyjádřeno dle aktuálně platné legislativy.

25.4. Dodavatel je povinen vystavit řádný daňový doklad do 15. dne kalendářního měsíce následujícího po kalendářním měsíci, za který je účtována cena za poskytování služby ověřování platnosti kvalifikovaných elektronických podpisů a pečetí.

25.5. Odběratel je povinen uhradit daňové doklady převodem na účet dodavatele do 30 dnů ode dne doručení daňového dokladu, vystaveného dodavatelem, na adresu sídla dodavatele a doručeného písemně na adresu sídla dodavatele podle údajů v této Smlouvě. Daňové doklady doručené mezi 15. prosincem a 15. únorem následujícího kalendářního roku mají splatnost v délce 60 dnů.

26. Sankční ustanovení, odstoupení od Smlouvy

26.1. V případě zaviněného nedodržení parametru SLA dostupnosti služby ověřování platnosti kvalifikovaných elektronických podpisů a pečetí uvedeného v článku 23.

odstavci 23.2. této Smlouvy, tj. pokud dostupnost služby klesne pod 98 % za kalendářní den, je dodavatel povinen uhradit odběrateli smluvní pokutu ve výši 1.000,- Kč bez DPH za každých započatých 0,1%, o kterých klesne dostupnost poskytované služby pod požadovanou hodnotu. Měsíční výše smluvní pokuty však nepřesáhne dvojnásobek měsíční ceny za poskytované služby.

26.2. V případě nesplnění povinností uvedených v článku 23. odstavci 23.3. písm. a) a b) této Smlouvy je dodavatel povinen uhradit odběrateli smluvní pokutu ve výši 1.000,- Kč bez DPH za každé takové porušení.

26.3. V případě nesplnění povinností uvedených v článku 23. odstavci 23.3. písm. c) tohoto ujednání je dodavatel povinen uhradit odběrateli smluvní pokutu ve výši 10.000,- Kč bez DPH za každé takové porušení.

26.4. V případě nesprávného vyhodnocení platnosti podpisu ze správných vstupních dat je dodavatel povinen uhradit odběrateli smluvní pokutu ve výši 10000,- Kč bez DPH za každé takové porušení, avšak pouze v případě, že data nutná k ověření (která se odesílají do prostředí dodavatele), generována komponentou dodanou dodavatelem, nebyla jakkoliv pozměněna a nebylo s nimi nijak manipulováno. Tím není dotčeno právo odběratele na náhradu případné újmy na jmění.

OBECNÁ ČÁST SMLOUVY

27. Objednávky

27.1. Předmět Smlouvy v rozsahu bodů 28.12. – 28.14 a bodu 28.16. bude plněn na základě dílčích objednávek, které budou dodavateli zasílány vždy s časovým předstihem (nejpozději 3 dny před požadovaným termínem plnění, pokud se strany nedohodnou jinak). Dodavatel je povinen dodržovat odběratelem zadané termíny plnění (dle jednotlivých dílčích objednávek).

27.2. Objednávky musí obsahovat minimálně tyto náležitosti:

a) podrobnou specifikaci požadovaného plnění (jako místo a termín plnění, cenovou kategorii dle ceny uvedené v této Smlouvě a podrobný popis předmětu plnění)
b) identifikační údaje dodavatele a odběratele s odkazem na tuto Smlouvu.

27.3. Dílčí objednávky i jejich potvrzení budou činěny neprodleně a výhradně písemně, přičemž pro účely této Smlouvy se za písemný projev vůle považuje také zaslání na e-mailovou adresu oprávněného zástupce uvedenou v článku 34.1. a 34. 2. Smlouvy.

27.4. Dodavatel bude dostávat pokyny na jednotlivé úkony služby od oprávněného zástupce, určeného odběratelem. Oprávněný zástupce je oprávněn zadávat, konkretizovat a upřesňovat požadovaná zadání na plnění předmětu Smlouvy.

27.5. Dodavatel může objednávku odmítnout pouze v případě závažných objektivních důvodů nespočívajících na jeho straně (např. porušuje-li zaslaná objednávka Smlouvu či právní předpisy nebo v případě vyšší moci). Odmítnutí objednávky je dodavatel povinen zaslat oprávněnému zástupci odběratele neprodleně.

27.6. Odběratel je oprávněn kdykoliv dílčí objednávku zrušit, je však povinen uhradit dodavateli část ceny, která odpovídá již prokazatelně vynaloženým nákladům

dodavatele do okamžiku zrušení objednávky. Dodavatel je povinen tuto výši nákladů prokázat.

27.7. Dodavatel bere na vědomí, že odběratel na základě této Smlouvy není povinen objednat u dodavatele sjednané plnění v plné šíři. Z tohoto titulu si tedy dodavatel nemůže vůči odběrateli vynucovat uzavření jakékoliv dílčí objednávky v souvislosti s touto Smlouvou a požadovat na odběrateli zaplacení jakýchkoli plateb (mimo těch za skutečně objednanou a realizovanou službu).

27.8. Po každém dílčím plnění Smlouvy bude vyhotoven odběratelem akceptační protokol, potvrzující, že dílčí plnění proběhlo bez vad, který bude oboustranně podepsán oprávněnými zástupci smluvních stran, přičemž každá strana si ponechá jedno paré.

28. Cenové a fakturační podmínky

28.1. Cena za vydání jednoho páru prvotních zaměstnaneckých certifikátů dle článku 2.3. na dobu platnosti 1 roku splňujícího naplnění položek elektronické žádosti o vydání tohoto certifikátu pro zaměstnance příkazníka činí:

185 Kč bez DPH.

28.2. Cena za vydání jednoho následného páru následných zaměstnaneckých certifikátů dle článku 2.3 splňujícího naplnění položek elektronické žádosti o vydání tohoto certifikátu s platností 1 rok pro zaměstnance příkazníka činí:

185 Kč bez DPH.

28.3. Cena za vydání jednoho prvotního zaměstnaneckého kvalifikovaného certifikátu na dobu platnosti 1 roku splňujícího naplnění položek elektronické žádosti o vydání kvalifikovaného certifikátu pro zaměstnance příkazníka činí:

185 Kč bez DPH.

28.4.Cena za vydání jednoho následného zaměstnaneckého kvalifikovaného certifikátu splňujícího naplnění položek elektronické žádosti o vydání kvalifikovaného certifikátu s platností 1 rok pro zaměstnance příkazníka činí:

185 Kč bez DPH.

28.5. Cena za vydání jednoho prvotního systémového certifikátu na dobu platnosti 1 roku splňujícího naplnění položek elektronické žádosti o vydání systémového certifikátu pro příkazníka činí:

530 Kč bez DPH.

28.6. Cena za vydání jednoho následného systémového certifikátu splňujícího naplnění položek elektronické žádosti o vydání systémového certifikátu s platností 1 rok pro příkazníka činí:

530 Kč bez DPH.

28.7. Cena za vydání jednoho prvotního zaměstnaneckého komerčního certifikátu na dobu platnosti 1 roku splňujícího naplnění položek elektronické žádosti o vydání komerčního certifikátu pro zaměstnance příkazníka činí:

165 Kč bez DPH.

28.8. Cena za vydání jednoho následného zaměstnaneckého komerčního certifikátu splňujícího naplnění položek elektronické žádosti o vydání komerčního certifikátu s platností 1 rok pro zaměstnance příkazníka činí:

165 Kč bez DPH.

28.9. Cena za vydání jednoho prvotního komerčního certifikátu pro server na dobu platnosti 1 roku splňujícího naplnění položek elektronické žádosti o vydání komerčního certifikátu pro příkazníka činí:

570 Kč bez DPH.

28.10. Cena za vydání jednoho následného komerčního certifikátu pro server splňujícího naplnění položek elektronické žádosti o vydání komerčního certifikátu s platností 1 rok pro příkazníka činí:

570 Kč bez DPH.

28.11. Cena za vydání jednoho prvotního SSL DV/OV certifikátu na dobu platnosti 1 roku splňujícího naplnění položek elektronické žádosti o vydání SSL certifikátu pro příkazníka činí:

967 Kč bez DPH.

28.12. Cena za jeden výjezd pracoviště mobilní registrační autority příkazce určené pro vydávání kvalifikovaných certifikátů a komerčních certifikátů (výjezd se uskuteční pouze v případě požadavku a na základě objednávky příkazníka) činí:

100 Kč bez DPH.

28.13. Cena za USB čtečku čipových karet (není-li nedílnou součástí kvalifikovaného prostředku pro vytváření elektronických podpisů) činí:

165 Kč bez DPH.

28.14. Cena za kvalifikovaný prostředek pro vytváření elektronických podpisů ve formě čipové karty činí:

325 Kč bez DPH.

28.15. Cena za roční provoz aplikace pro správu certifikátů splňující podmínky vyhlášky č. 259/2012 Sb. činí:

0 Kč bez DPH.

28.16. Cena za poskytnutí licence aplikace pro hromadné podepisování dokumentů s možností vkládání časových razítek po dobu trvání této Smlouvy činí:

1150 Kč bez DPH.

28.17. Cena za archivní časová razítka je počítána jako počet skutečně odebraných archivních časových razítek vynásobený cenou za jedno časové razítko. Cena za jedno časové

razítko se odvíjí od počtu odebraných časových razítek v daném měsíci a je stanovena následovně:

Odebrané množství razítek ks/měsíc	Cena v Kč za 1 ks razítka bez DPH
Do 500	1,80
501 - 1000	1,50
1001 - 5000	1,30
5001 – 10000	0,99
Nad 10000	0,72

Např. při odběru 150 ks časových razítek tedy cena činí 150 x 1,80 Kč, tj. 270 Kč bez DPH.

28.18. Cena archivního časového razítka uvedená v odst. 17. tohoto článku Smlouvy zahrnuje i cenu služby poskytování archivních časových razítek a výstupů dle článků 14.2. a 14.4. Smlouvy. Pro odstranění jakýchkoli pochybností smluvní strany sjednávají, že jakékoli požadavky příkazníka na výstupy v souladu s 14.4. této Smlouvy jsou vyřizovány ze strany zdarma, resp. cena těchto výstupů je již zahrnuta do celkové ceny služby poskytování archivních časových razítek vyjádřené jednotkovou cenou archivního časového razítka.

28.19. Vyúčtování ceny za vydání všech prvotních a všech následných certifikátů dle článku 2.3. Smlouvy, všech prvotních a všech následných kvalifikovaných a komerčních certifikátů či objednaných a uskutečněných výjezdů mobilní registrační autority příkazce, čteček čipových karet, kvalifikovaných prostředků pro vytváření elektronických podpisů a časových razítek pro příkazníka bude prováděno hromadně, vždy jednou měsíčně zpětně za poslední uplynulý kalendářní měsíc, v němž příkazce certifikáty či časová razítka vydal, uskutečnil výjezd pracoviště mobilní registrační autority příkazce nebo dodal čtečky čipových karet a kvalifikované prostředky pro vytváření elektronických podpisů.

28.20 Faktury za poskytnuté kvalifikované certifikáty a odebraná archivní časová razítka dle bodů 28.1 – 4, 28.7 – 8 a 28.17 budou vystaveny zvlášť pro OP EU v gesci MŠMT a zvlášť pro úřad MŠMT. Faktury hrazené z OP EU budou vždy označeny názvem příslušného operačního programu a registračním číslem projektu, z něhož jsou hrazeny. Registrační číslo projektu a název operačního programu bude dodavateli písemně sděleno příkazníkem. V případě změny registračního čísla projektu/operačního programu bude ze strany příkazníka vždy takováto změna dodavateli včas sdělena.

28.21 Příkazce je povinen zajistit na své straně pro účely fakturace evidenci vydaných zaměstnaneckých kvalifikovaných certifikátů, zaměstnaneckých komerčních certifikátů, případně jejich párů a archivních časových razítek (body 28.1 – 4, 28.7 – 8 a 28.17) tak, aby se prokazatelně daly vyúčtovat a fakturovat zvlášť pro OP EU a zvlášť pro úřad MŠMT.

28.22. Příkazce je povinen vystavit řádný daňový doklad do 15. dne kalendářního měsíce následujícího po kalendářním měsíci, za který je účtována cena za vydání všech prvotních a za vydání všech následných certifikátů dle článku 2.3, za vydání všech prvotních a za vydání všech následných kvalifikovaných a komerčních certifikátů, za objednané a uskutečněné výjezdy pracoviště mobilní registrační autority příkazce

a dodávku čteček čipových karet a kvalifikovaných prostředků pro vytváření elektronických podpisů pro příkazníka.

28.23. Příkazník je povinen uhradit cenu za všechny prvotní certifikáty, za všechny následné certifikáty, výjezdy mobilní registrační autority příkazce a čtečky čipových karet a kvalifikované prostředky pro vytváření elektronických podpisů převodem na účet příkazce do 30 dnů ode dne prokazatelného doručení daňového dokladu, vystaveného příkazcem na adresu Příkazníka. Daňové doklady doručené mezi 15. prosincem a 15. únorem následujícího kalendářního roku mají splatnost v délce 60 dnů. Příkazník umožňuje zasílání faktur na email [redacted]

28.24. Daňový doklad musí mít náležitosti daňových a účetních dokladů, stanovených platnými právními předpisy. Příkazník je oprávněn daňový doklad, který nebude splňovat náležitosti podle platných právních předpisů, a nebo jehož věcný obsah nebude
v souladu s počtem a druhem vydaných prvotních a následných certifikátů dle článku 2.3, vydaných prvotních a následných kvalifikovaných certifikátů a komerčních certifikátů, počtem výjezdů pracoviště mobilní registrační autority příkazce a čteček čipových karet a kvalifikovaných prostředků pro vytváření elektronických podpisů, vrátit příkazci.

28.25. Příkazce je povinen nedostatky daňového dokladu odstranit a vystavit nový daňový doklad. Na základě vadně vystaveného daňového dokladu ve smyslu tohoto odstavce se příkazník neocitá v prodlení. Doba splatnosti počíná běžet znovu od opětovného zaslání náležitě doplněných či opravených dokladů.

28.26. Příkazce tímto bere na vědomí, že příkazník je organizační složkou státu a jeho stav účtu závisí na převodu finančních prostředků ze státního rozpočtu. Příkazce souhlasí s tím, že v případě nedostatku finančních prostředků na účtu příkazníka, dojde k zaplacení faktury po obdržení potřebných finančních prostředků a že časová prodleva z těchto důvodů nebude započítána do doby splatnosti uvedené na faktuře a nelze z těchto důvodů vůči příkazníkovi uplatňovat žádné sankce. Příkazník se zavazuje, že v případě, že tato skutečnost nastane, oznámí ji neprodleně a to písemně dodavateli nejpozději do doby splatnosti faktury vystavené příkazcem.

28.27. Příkazce je podle ustanovení § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů, osobou povinnou spolupůsobit při výkonu finanční kontroly prováděné v souvislosti s úhradou služeb z veřejných výdajů.

28.28. Příkazce je povinen zajistit archivaci dokumentů o plnění předmětu této Smlouvy po dobu stanovenou právními předpisy, zejména uchování účetních záznamů a dalších relevantních podkladů, souvisejících s dodávkou služeb. Příkazce je navíc povinen umožnit osobám oprávněným k výkonu kontroly projektu, z něhož je předmět této Smlouvy hrazen, provést kontrolu dokladů souvisejících s plněním Smlouvy, a to až do 31. 12. 2033.

28.29. Odběratel si vyhrazuje právo závazné pokyny k fakturaci dále upřesnit.

28.30. Platba bude uskutečněna bezhotovostním převodem z účtu odběratele na účet dodavatele, a to v české měně. Za datum úhrady se považuje den odepsání příslušné částky z účtu odběratele.

28.31. Odběratel nebude poskytovat dodavateli žádné zálohové platby.

29. Poskytování informací třetím osobám

29.1. Smluvní strany se zavazují, že obchodní a technické informace, které jim byly svěřeny druhou stranou, nezpřístupní třetím osobám bez písemného souhlasu druhé strany a nepoužijí tyto informace k jiným účelům, než je k plnění podmínek této Smlouvy.

30. Ochrana osobních údajů

30.1. 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 č. 110/2019 Sb.“) a ve smyslu zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce.

30.2. Příkazník má pro účely ochrany osobních údajů postavení zpracovatele ve smyslu Obecného nařízení a zákona č. 110/2019 Sb. Příkazce má pro účely ochrany osobních údajů postavení správce ve smyslu Obecného nařízení a zákona č. 110/2019 Sb.

30.3. Podrobné podmínky zpracování osobních údajů jsou uvedeny v příloze č. 6.

31. Mlčenlivost

31.1. Všechny informace, ať už v písemné, ústní, vizuální, elektronické, nebo jiné podobě, které byly či budou poskytnuty druhé ze smluvních stran, nebo jejím jménem v souvislosti s plněním této Smlouvy, nebo informace se kterými se smluvní strany při výkonu smluvních povinností náhodně setkají, vyjma informací veřejných (viz následující článek této Smlouvy), budou smluvní strany pokládat za neveřejné, a budou s nimi takto nakládat. Tyto informace budou mít smluvní režim vztahující se na informace důvěrné, především ohledně obchodního tajemství ve smyslu § 504 a důvěrných informací ve smyslu § 1730 zákona č. 89/2012 Sb., občanského zákoníku a musí s nimi být nakládáno v souladu s Obecným nařízením a se zákonem č. 110/2019 Sb.

31.2. Veřejnými informacemi jsou:

a) Informace, které se staly obecně dostupnými veřejnosti jinak než následkem jejich zpřístupnění přímo či nepřímo smluvními stranami, nebo
b) Informace, které smluvní strany získají jako informace nikoliv neveřejného charakteru z jiného zdroje, avšak pouze v případě, že smluvní strany veřejnost takové informace nejprve ověřily u druhé smluvní strany, jinak jde o informaci neveřejnou.

31.3. Smluvní strany se zavazují použít neveřejné informace výhradně v souvislosti s plněním této Smlouvy. Smluvní strany se dále zavazují, že ony ani osoby, které jsou s nimi přímo či nepřímo majetkově propojeny, ani jejich zástupci, zaměstnanci, zmocněnci,

mandatáři nebo jiné osoby, které byly smluvními stranami seznámeny s neveřejnými informacemi, je nezpřístupní žádné třetí osobě s výjimkou případů, kdy:

a) Je zveřejnění neveřejné informace vyžadováno zákonem nebo jinými platnými právními předpisy nebo;
b) Kdy zveřejnění těchto neveřejných informací je vysloveně touto Smlouvou povoleno nebo;
c) V případě, kdy zveřejnění těchto neveřejných informací bude předem písemně odsouhlaseno smluvními stranami.

31.4. Smluvní strany se zavazují, že její zaměstnanci, konzultanti, zástupci a mandatáři (dále jen „zaměstnanci“) budou s neveřejnými informacemi zacházet náležitým způsobem a v souladu s touto Smlouvou. Smluvní strany se zavazují, že pokud přijdou její zaměstnanci do styku s osobními nebo citlivými údaji ve smyslu Obecného nařízení a zákona č. 110/2019 Sb., učiní veškerá opatření, aby nedošlo k neoprávněnému nebo nahodilému přístupu k těmto údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož aby i jinak neporušili tento zákon. Smluvní strany nesou plnou odpovědnost a právní důsledky za případné porušení zákona z jejich strany.

31.5. Závazky smluvních stran dle výše uvedených ustanovení trvají i po skončení účinnosti této Smlouvy.

32. Sankce

32.1. Za prokazatelné porušení povinností uvedených v této Smlouvě mají smluvní strany nárok na náhradu újmy na jmění, která jim v důsledku tohoto porušení vznikla.

32.2. Náhradu újmy na jmění podle tohoto článku nelze uplatnit, došlo-li k závadě v důsledku vyšší moci.

32.3. Za každý den prodlení příkazníka s uhrazením daňového dokladu, vystaveného příkazci, je příkazce oprávněn účtovat příkazníkovi úrok z prodlení, a to ve výši 0,01 % z dlužné částky za každý den prodlení. Jiné sankce jsou vůči příkazníkovi nepřípustné.

32.4. V případě porušení povinnosti mlčenlivosti dle této Smlouvy je dodavatel povinen zaplatit smluvní pokutu ve výši 100 000,- Kč, a to za každý jednotlivý případ.

33. Doba trvání Smlouvy

33.1. Tato Smlouva se uzavírá na dobu 4 let ode dne nabytí účinnosti Smlouvy nebo do vyčerpání maximální předpokládané hodnoty za předmět plnění ve výši 1 900 000,- Kč (jeden milion devět set tisíc korun českých) bez DPH.

33.2. Platnost Smlouvy lze ukončit písemnou dohodou podepsanou oprávněnými zástupci obou smluvních stran.

33.3. Každá ze smluvních stran má právo odstoupit od této Smlouvy v případě, poruší-li jedna ze smluvních stran své závazky a povinnosti stanovené touto 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 jinak řídí ust. § 2001 a násl. občanského zákoníku

33.4. Kterákoliv ze smluvních stran je oprávněna Smlouvu vypovědět, a to i bez udání důvodu. Výpovědní doba činí 30 kalendářních dnů a začíná běžet první den následující po dni, v němž výpověď byla doručena.

33.5. Zánikem Smlouvy nejsou smluvní strany, kdy bylo písemné vyhotovení výpovědi prokazatelně doručeno druhé smluvní straně, zbaveny povinnosti vyrovnat veškeré své závazky vzniklé v důsledku provozu registračních autorit a jsou povinny učinit veškeré úkony, které nesnesou odkladu a které jsou nutné k zabránění vzniku újmy na jmění druhé smluvní strany.

34. Další ujednání

34.1. Kontaktní osoby odběratele

	Příjmení jméno, titul	Telefon	GSM	e-mail
[redacted]				

34.2. Kontaktní osoby dodavatele:

[redacted]

35. Závěrečná ustanovení

35.1. Tato Smlouva může být měněna jen formou písemných, vzestupně číslovaných dodatků podepsaných oprávněnými zástupci obou smluvních stran. V případě změny v označení smluvních stran, změn pověřených osob, statutárních orgánů a dalších údajů uvedených v označení smluvních stran a osob oprávněných k jednání z této Smlouvy, nepoužije se ustanovení v první větě tohoto článku. Ke změně těchto údajů, postačuje oznámení druhé smluvní straně ve písemným oznámením kontaktní osobě odběratele. K tomuto dopisu musí být přiložena ověřená listina nebo plná moc, dokládající oznamovanou změnu údajů. Ustanovení tohoto článku se použije i v případě změny právní formy některé ze smluvních stran, zániku smluvní strany s likvidací nebo bez likvidace, kdy práva a povinnosti podle obecně závazných právních předpisů přechází na právního nástupce smluvní strany.

35.2. Právní vztahy smluvních stran výslovně touto Smlouvou neupravené a z ní vyplývající nebo s ní související se řídí obecně závaznými právními předpisy, zejména nařízením Evropského parlamentu a Rady (EU) č. 910/2014, o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES, a příslušnými ustanoveními občanského zákoníku.

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

35.4. Smluvní strany se zavazují, že jakékoli případné spory, vzniklé z této Smlouvy nebo v souvislosti s ní, budou řešeny mimosoudním jednáním na úrovni zplnomocněných zástupců obou smluvních stran, s cílem zachování dobrých vztahů. Teprve nepovede-li takové smírčí jednání k vyřešení sporu, bude soudní spor veden u příslušného soudu ČR.

35.5. Příkazce tímto prohlašuje, že vůči němu není vedeno řízení dle zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), ve znění pozdějších předpisů, a zavazuje se bezodkladně informovat příkazníka zejména nikoliv však jen výlučně o tom, že je v úpadku, či hrozícím úpadku, nebo i o skutečnosti, že je proti němu, jako osobě povinné, vedena exekuce dle zákona č. 120/2001 Sb., o soudních exekutorech a exekuční činnosti (exekuční řád), ve znění pozdějších předpisů, nebo dle zákona č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů.

35.6. Smluvní strany se dohodly, že ve vztazích mezi příkazcem a příkazníkem vyplývajících z této Smlouvy se neuplatní ustanovení §§ 1895 až 1900 a § 2436 občanského zákoníku.

35.7. Smlouva a jednotlivé dílčí objednávky nabývají platnosti dnem jejich podpisu druhou ze smluvních a účinnosti dnem jejich zveřejnění v registru smluv, nejdříve však 8. 3. 2021.

35.8. V souladu se zákonem o registru smluv zajistí příkazník uveřejnění celého textu Smlouvy a dílčích objednávek splňujících zákonné podmínky, vyjma osobních údajů a metadat Smlouvy, v registru smluv včetně případných oprav uveřejnění s tím, že nezajistí-li příkazník uveřejnění Smlouvy nebo metadat Smlouvy v registru smluv do 30 dnů od uzavření Smlouvy, pak je oprávněn zajistit jejich uveřejnění příkazce ve lhůtě tří měsíců od uzavření Smlouvy.

35.9. Příkazce bere na vědomí, že příkazník jako povinný subjekt musí na žádost poskytnout informace podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, a to zejména informace týkající se identifikace smluvních stran, informace o ceně plnění a rámcovou informaci o předmětu plnění Smlouvy. Informace poskytnuté v souladu s citovaným zákonem nelze považovat za porušení závazku mlčenlivosti o důvěrných informacích dle § 1730 odst. 2 občanského zákoníku.

35.10. Příkazce bere na vědomí povinnost příkazníka uveřejnit tuto Smlouvu také v souladu s ust. § 219 zákona č. 134/2016 Sb., o zadávání veřejných zakázek.

35.11. Tato Smlouva se uzavírá elektronicky.

35.12. Smluvní strany prohlašují, že si Smlouvu přečetly, že tato byla sepsána na základě jejich pravé a svobodné vůle, a že souhlasí s celým jejím obsahem, a na důkaz toho připojují své podpisy.

35.13. Příkazník prohlašuje, že jím dodávané plnění má všechny vlastnosti požadované příkazcem coby zadavatelem veřejné zakázky, ze které plnění z této Smlouvy vzešlo.

35.14. V případě interpretačních různic smluvních stran vyplývajících z této Smlouvy se smluvní strany dohodly, že bude při interpretaci Smlouvy užito zadávací dokumentace veřejné zakázky s názvem „Zajištění služeb certifikační autority“.

35.15. Nedílnou součástí této Smlouvy jsou:

- Příloha 1: Technické, procesní a bezpečnostní požadavky.
- Příloha 2: Rozsah a forma součinnosti při provozování registrační autority.
- Příloha 3: Doložení statutu kvalifikovaného dodavatele služeb vytvářejících důvěru.
- Příloha 4: Popis služby vytváření kvalifikovaných elektronických pečetí na dálku
- Příloha 5: Popis služby ověřování platnosti kvalifikovaných elektronických podpisů a pečetí
- Příloha 6: Podmínky zpracování osobních údajů

Příkazník:

V Praze dne (dle el. podpisu)

Ing. Václav Jelen
Digitálně podepsal Ing. Václav Jelen
Datum: 2021.03.04 16:48:24 +01'00'

Ing. Václav Jelen

Ředitel odboru informatiky a statistiky

Ing. Michal Macháček
Digitálně podepsal Ing. Michal Macháček
Datum: 2021.03.04 16:25:47 +01'00'

Bc. Jan Frisch

Ředitel odboru technické pomoci

Příkazce:

V Praze dne (dle el. podpisu)

Petr Budiš
Digitálně podepsal Petr Budiš
Datum: 2021.03.04 11:07:42 +01'00'

Ing. Petr Budiš, Ph.D., MBA

Předseda představenstva

Ing. Roman Kučera
Digitálně podepsal Ing. Roman Kučera
Datum: 2021.03.04 11:02:34 +01'00'

Ing. Roman Kučera

Člen představenstva

Příloha č. 1

Technické, procesní a bezpečnostní požadavky

Technické, procesní a bezpečnostní požadavky pro provozování registrační autority

Technické, procesní a bezpečnostní požadavky pro provozování registrační autority jsou uvedeny zejména v následujících dokumentech:

1. V celostátně platné legislativě, která souvisí s činností registračních autorit a na kterou se tato smlouva odvolává,
2. v podmínkách této smlouvy,
3. v certifikačních politikách společnosti První certifikační autorita, a.s., pro vydávání kvalifikovaných certifikátů,
4. v provozních směrnicích společnosti První certifikační autorita, a.s., pro pracovníky registračních autorit I.CA pro vydávání kvalifikovaných certifikátů,
5. v metodických pokynech, zpracovaných pro vydávání certifikátů, které jsou dostupné pro operátory registračních autorit na https://rainfo.ica.cz,
6. na webu společnosti První certifikační autorita, a.s., tj. na: www.ica.cz,
7. ve všech dalších dokumentech, které budou předány příkazníkovi a jeho pracovníkům příkazcem (společností První certifikační autorita, a.s.).

Technické požadavky pro vydávání SSL certifikátů

1. SSL certifikáty budou vydávány v souladu s Certifikační politikou pro SSL certifikáty (dále jen "CP SSL"), 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 organizaci, které je certifikát vydáván.

3. Uvedené SSL certifikáty budou vydávány na základě elektronické žádosti o SSL certifikáty, která musí být předem zaslána na e-mailovou adresu [redacted] a která musí dále splňovat níže popsané a definované požadavky dle CP SSL. Elektronická žádost musí být prokazatelně odeslána ve formě přílohy e-mailové zprávy zmocněnou osobou na straně MŠMT uvedenou v Plné moci, jejíž vzor je uveden níže, 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 níže uvedeném Postupu pro získání SSL certifikátu (dále též „Postup“).

6. Žadatel je povinen vytvářet žádosti o SSL certifikáty v souladu s platnou CP SSL a podle postupů uvedených v Postupu.

7. Pokud zaslaná žádost nebude v souladu s CP SSL anebo požadavky uvedenými v Postupu, 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 držitel nesplnil povinnosti požadované CP SSL (např. poskytnutí nesprávných údajů apod.), dle kterých mohlo dojít k vydání SSL certifikátu.

Postup pro získání SSL certifikátu

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

- [redacted]

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

1. Rozlišují se dva typy certifikátů:

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

2. Požadavky na doménu:

Jsou vydávány certifikáty pro všechny typy domén kromě nových gTLD (.company, .bike, .movie, .club apod.).
V žádosti může být pouze jedna doména druhého řádu (ica.cz) a až devět dalších názvů dnsName (subdomén – www.ica.cz, neco1.ica.cz, neco2.ica.cz).
V položkách žádosti dále nesmí být IP adresa a doména se zástupnými znaky, tzv. wildcard doména, např. *.ica.cz

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

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

Rozšíření subjectAlternativeName:

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

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

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

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

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

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

6. Ověření vlastnictví domény

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

- na e-mail uvedený u doménového kontaktu dle WHOIS zašle e-mail žádající schválení vydání SSL certifikátu pro DNS jména obsažená v předložené žádosti, který obsahuje náhodný řetězec, doménový kontakt pošle schválení žádosti obsahující tento řetězec zpět do I.CA,

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

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

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

Platnost náhodných řetězců je ve všech případech 30 dní.

7. Kontrola CAA záznamů

I.CA provede první kontrolu a:

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

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

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

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

V opačných případech je žádost odmítnuta.

8. Obnovení – následný certifikát

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.

Plná moc pro vydání SSL certifikátu – vzor

Tímto potvrzujeme, že pan/paní

……..……,

R.Č. ……..……..……..… bytem ……..…….

Č. OP …….

je k dnešnímu dni naším zaměstnancem.

Název: **Česká republika – Ministerstvo školství, mládeže a tělovýchovy**
Adresa: Karmelitská 529/5, 118 12 Praha 1
IČO: 00022985

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 školství, mládeže a tělovýchovy**
Adresa: Karmelitská 529/5, 118 12 Praha 1
IČO: 00022985

E-mailová adresa žadatele:…….

V Praze dne ...…….....

…… ……..……
Podpis statutárního zástupce ČR – Ministerstvo školství, mládeže a tělovýchovy

Podpis zaměstnance

Příloha č. 2

Rozsah a forma součinnosti při provozování registrační autority

I.
Úvod

I.CA (dále jen „provozovatel“) uzavřela s příkazníkem smlouvu, na základě které bude příkazník provozovat registrační autoritu, vydávající kvalifikované certifikáty, systémové certifikáty a komerční certifikáty včetně komerčních certifikátů pro servery. Příkazník pověřil osoby odpovědné za provoz registrační autority (dále jen „vykonatel“), které budou v rámci služeb První certifikační autority, a.s., zajišťovat fungování této registrační autority, a to vykonáváním následujících činností:

- přijímání žádostí o kvalifikované a systémové certifikáty,
- ověřování totožnosti žadatelů o kvalifikované a systémové certifikáty v souladu s platnými certifikačními politikami,
- vydávání kvalifikovaných a systémových certifikátů,
- přijímání žádostí o komerční certifikáty včetně komerčních certifikátů pro servery,
- ověřování totožnosti žadatelů o komerční certifikáty včetně komerčních certifikátů pro servery v souladu s platnými certifikačními politikami,
- vydávání komerčních certifikátů včetně komerčních certifikátů pro servery,
- ostatní s tím související činnosti, tj. vedení dokumentace k vydaným certifikátům.

II.
Práva a povinnosti vykonavatele (osoby pověřené příkazcem)

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 Certifikační politiku I.CA pro kvalifikované certifikáty (CPQC), platnou Certifikační politiku I.CA pro systémové certifikáty (CPSC) a platnou Provozní směrnici pro pracovníky Registračních autorit I.CA vydávající kvalifikované a systémové certifikáty (PSQRA).

2. Dodržovat platnou Certifikační politiku I.CA pro komerční certifikáty včetně komerčních certifikátů pro servery (CPKC) a platnou Provozní směrnici pro pracovníky Registračních autorit I.CA vydávající komerční certifikáty (PSKRA).
3. Řídit se pokyny provozovatele.

III.
Práva a povinnosti provozovatele (I.CA)

Provozovatel je oprávněn:

1. Požadovat od vykonavatele dodržování platné CPQC, CPSC a PSQRA, upozornit jej na zjištěné nedostatky a požadovat v přiměřené lhůtě nápravu.
2. Požadovat od vykonavatele dodržování platné CPKC a PSKRA, upozornit jej na zjištěné nedostatky a požadovat v přiměřené lhůtě nápravu
3. Provádět u vykonavatele kontrolu a nezbytná zjišťování.

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.

Příloha č. 3

Doložení statutu kvalifikovaného dodavatele služeb vytvářejících důvěru

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

MVCRX03KZ4X6
prvotní identifikátor

odbor eGovernmentu
náměstí Hrdinů 1634/3
Praha 4
140 21

Č. j. MV- 94722-2/EG-2017

Praha 3. srpna 2017

První certifikační autorita, a.s.
Podvinný mlýn 2178/6
Praha 9, PSČ 190 00
ID DS: a69fvfb

zastoupená

Ing. Petr Budiš, Ph.D — předseda představenstva
Ing. Roman Kučera — člen představenstva

Ukončení přezkoumání zprávy o posouzení shody

Tímto Vám sdělujeme, že odbor eGovernmentu Ministerstva vnitra jakožto orgán dohledu nad poskytovateli služeb vytvářejících důvěru 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 jen nařízení eIDAS) ukončil přezkoumání zprávy o posouzení shody pro Vaši službu I.CA kvalifikované certifikáty pro elektronické podpisy – vydávání kvalifikovaných certifikátů pro elektronické podpisy, která byla zaslána v souladu s čl. 51 odst. 3 nařízení eIDAS prostřednictvím Vaší žádosti ze dne 31. května 2017.

Jelikož v rámci přezkoumání zprávy o posouzení shody, certifikační politiky vydávání kvalifikovaných certifikátů pro elektronické podpisy verze 1.10 a další dokumentace nebyly nalezeny žádné neshody s požadavky nařízení eIDAS a zákona č. 297/2016

Sb., o službách vytvářejících důvěru pro elektronické transakce, nadále je První certifikační autoritě, a.s. přiznán kvalifikovaný status poskytovatele služeb vytvářejících důvěru v souvislosti s vydáváním kvalifikovaných certifikátů pro elektronické podpisy.

Děkuji za spolupráci.

Ing. Roman Vrba
ředitel

Elektronický podpis - 4.8.2017

Certifikát autora podpisu :
Jméno : Ing. Roman Vrba
Vydal : PostSignum Qualified C...
Platnost do : 2.7.2018

MVCRX03LDQR7
prvotní identifikátor

odbor eGovernmentu
náměstí Hrdinů 1634/3
Praha 4
140 21

Č. j. MV- 74361-5/EG-2017

Praha 14. srpna 2017
Počet listů: 3

První certifikační autorita, a.s.
Podvinný mlýn 2178/6
Praha 9, PSČ 190 00
ID DS: a69fvfb

zastoupená

Aleš Kapusta člen představenstva
Ing. Roman Kučera člen představenstva

ROZHODNUTÍ

Ministerstvo vnitra České republiky, odbor eGovernmentu, jako správní orgán příslušný podle ustanovení § 13 odst. 1 zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce (dále jen „zák. č. 297/2016 Sb.) a čl. 21 odst. 2 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 jen „nařízení EU č. 910/2014), ve správním řízení o žádosti o udělení statusu kvalifikované služby vytvářející důvěru, kterou podali dne 5. června 2017 pan Aleš Kapusta a pan Ing. Roman Kučera, členové představenstva spol. První certifikační autorita, a.s., rozhodlo takto:

uděluje se kvalifikovaný status poskytovatele služeb vytvářejících důvěru v souvislosti se službami

- I.CA kvalifikované certifikáty pro elektronické pečetě
- I.CA kvalifikovaná elektronická časová razítka

poskytovateli

První certifikační autorita, a.s.
se sídlem Praha 9 – Libeň
Podvinný mlýn 2178/6, PSČ 19000
IČ 26439395

a uděluje se kvalifikovaný status služby vytvářející důvěru službám

I.CA kvalifikované certifikáty pro elektronické pečetě
a
I.CA kvalifikovaná elektronická časová razítka

Žadatel může začít dané služby poskytovat jako kvalifikované služby vytvářející důvěru poté, co byl status kvalifikovaného poskytovatele a kvalifikovaných služeb vyznačen v důvěryhodném seznamu České republiky, který je zveřejněn na internetové adrese https://tsl.gov.cz/publ/TSL_CZ.xtsl.

Odůvodnění:

Dne 5. června 2017 podali pan Aleš Kapusta a pan Ing. Roman Kučera, členové představenstva spol. První certifikační autorita, a.s. (dále jen „žadatel“) žádost o udělení statusu kvalifikované služby vytvářející důvěru pro služby:

- I.CA kvalifikované certifikáty pro elektronické pečetě (vydávání kvalifikovaných certifikátů pro elektronické pečetě),
- I.CA kvalifikovaná elektronická časová razítka (vydávání kvalifikovaných elektronických časových razítek).

Ministerstvo vnitra České republiky udělí v souladu s ustanovením § 13 odst. 1 zák. č. 297/2016 Sb. a čl. 21 odst. 2 nařízení EU č. 910/2014 status kvalifikovaného poskytovatele služeb vytvářejících důvěru a status kvalifikované služby vytvářející důvěru, pokud

a) žadatel předloží oznámení o svém úmyslu začít poskytovat kvalifikovanou službu vytvářející důvěru společně se zprávou o posouzení shody vydanou subjektem posuzování shody a
b) Ministerstvo vnitra České republiky, jakožto orgán dohledu ve smyslu čl. 17 nařízení EU č. 910/2014, dojde k závěru, že poskytovatel služeb vytvářejících důvěru a jím poskytovaná služba vytvářející důvěru splňuje požadavky na kvalifikovaného poskytovatele služeb vytvářejících důvěru a požadavky na kvalifikovanou službu vytvářejících důvěru.

Žadatel předložil veškeré zákonné náležitosti a splnil tak požadavky pro udělení kvalifikovaného statusu poskytovatele služeb vytvářejících důvěru v souvislosti se službami I.CA kvalifikované certifikáty pro elektronické pečetě a I.CA kvalifikovaná elektronická časová razítka a požadavky pro udělení kvalifikovaného statusu služby vytvářející důvěru službám I.CA kvalifikované certifikáty pro elektronické pečetě a I.CA kvalifikovaná elektronická časová razítka.

P o u č e n í :

Proti tomuto rozhodnutí lze podle ustanovení § 152 odst. 1 zákona č. 500/2004 Sb., správní řád, podat rozklad k ministru vnitra. Podle ustanovení § 86 odst. 1 správního řádu se rozklad podává u odboru eGovernmentu Ministerstva vnitra České republiky, a to podle ustanovení § 83 odst. 1 správního řádu ve lhůtě do 15 dnů ode dne jeho oznámení.

Ing. Roman Vrba
ředitel

otisk úředního razítka

Elektronický podpis - 15.8.2017

Certifikát autora podpisu :
Jméno : Ing. Roman Vrba
Vydal : PostSignum Qualified C...
Platnost do : 2.7.2018

MVCRX040AMF4
prvotní identifikátor

odbor eGovernmentu
náměstí Hrdinů 1634/3
140 21 Praha 4

Č. j.: MV- 68158-6/EG-2018

Praha 21. června 2018
Počet listů: 4

První certifikační autorita, a.s.
Podvinný mlýn 2178/6
Praha 9, PSČ 190 00
ID DS: a69fvfb

zastoupená

Ing. Petr Budiš, Ph.D., MBA (dat. nar. 24. února 1970)
předseda představenstva

Ing. Roman Kučera (dat. nar. 6. února 1963)
člen představenstva

ROZHODNUTÍ

Ministerstvo vnitra České republiky, odbor eGovernmentu, jako správní orgán příslušný podle ustanovení § 13 odst. 1 a § 13 odst. 3 zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů (dále jen „zák. č. 297/2016 Sb.“), ve věci posouzení služby vytváření kvalifikovaných elektronických pečetí na dálku I.CA RemoteSeal, kterou podali dne 22. května 2018 pan Ing. Petr Budiš, Ph.D., MBA, předseda představenstva, a pan Ing. Roman Kučera, člen představenstva, spol. První certifikační autorita, rozhodlo takto:

povoluje se kvalifikovanému poskytovateli služeb vytvářejících důvěru

První certifikační autorita, a.s.
se sídlem Praha 9 – Libeň
Podvinný mlýn 2178/6, PSČ 19000
IČ 26439395

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

a

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 nové certifikační politiky pro vydávání kvalifikovaných certifikátů pro elektronické pečetě na dálku s identifikátorem 1.3.6.1.4.1.23624.10.1.38.1.0 bude zveřejněn odborem eGovernmentu v důvěryhodném seznamu České republiky u služby „(78) I.CA - vydávání kvalifikovaných certifikátů“ společně s kvalifikátorem „QCQSCDManagedOnBehalf“ podle kap. 5.5.9.2.3 technických specifikací ETSI TS 119 612 v2.1.1. Důvěryhodný seznam České republiky je veden na základě čl. 22 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 jen „nařízení EU č. 910/2014“), a zveřejněn na internetové adrese https://tsl.gov.cz/publ/TSL_CZ.xtsl.

Odůvodnění:

Dne 22. května 2018 podali pan Ing. Petr Budiš, Ph.D., MBA, předseda představenstva, a pan Ing. Roman Kučera, člen představenstva, spol. První certifikační autorita žádost o posouzení služby vytváření kvalifikovaných elektronických pečetí na dálku I.CA RemoteSeal. Z obsahu žádosti je patrné, že kvalifikovaný poskytovatel služeb vytvářejících důvěru První certifikační autorita, a.s. touto žádostí oznamuje odboru eGovernmentu Ministerstva vnitra jakožto orgánu dohledu změny v poskytování své kvalifikované služby vytvářející důvěru ve smyslu čl. 24 odst. 2 písm. a) nařízení EU č. 910/2014. Změny se dotýkají služby vydávání kvalifikovaných certifikátů pro elektronické pečetě a spočívají:

- v poskytování služby vytváření kvalifikovaných elektronických pečetí na dálku, tj. ve vytváření a správě dat pro vytváření elektronických pečetí jménem pečetící osoby a dále ve správě kvalifikovaného prostředku pro vytváření elektronických pečetí jménem pečetící osoby,
- ve vydávání kvalifikovaných certifikátů pro elektronické pečetě podle nové 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).

Ministerstvo vnitra České republiky neshledalo v předložených dokumentech (certifikační politika vydávání kvalifikovaných certifikátů pro elektronické pečetě na dálku [algoritmus RSA] - verze 1.00, politika služby vytváření kvalifikovaných elektronických pečetí na dálku - verze 1.00 a prováděcí směrnice služby vytváření kvalifikovaných elektronických pečetí na dálku - verze 1.00) žádné nedostatky, které by byly v rozporu s platnou právní úpravou regulující poskytování služeb vytvářejících důvěru, tzn. nařízením EU č. 910/2014 a také zák. č. 297/2016 Sb.

Zařízení ARX CoSign v8.2 a DocuSign Signature Appliance v8.4, které hodlá První certifikační autorita, a.s. použít pro poskytování služby vytváření kvalifikovaných elektronických pečetí na dálku I.CA RemoteSeal, jsou certifikovány jako kvalifikované prostředky pro vytváření elektronických pečetí. Informace o certifikaci výše uvedených zařízení je uvedena v unijním seznamu kvalifikovaných prostředků pro vytváření elektronických podpisů a kvalifikovaných prostředků pro vytváření elektronických pečetí, který je dostupný na adrese: https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds s poznámkou, že se zařízení považují za kvalifikované prostředky pro vytváření elektronických pečetí, pouze pokud jsou spravovány kvalifikovaným poskytovatelem služeb vytvářejících důvěru jménem pečetící osoby.

P o u č e n í :

Proti tomuto rozhodnutí lze podle ustanovení § 152 odst. 1 zákona č. 500/2004 Sb., správní řád, podat rozklad k ministru vnitra. Podle ustanovení § 86 odst. 1 správního řádu se rozklad podává u odboru eGovernmentu Ministerstva vnitra České republiky, a to podle ustanovení § 83 odst. 1 správního řádu ve lhůtě do 15 dnů ode dne jeho oznámení.

Ing. Roman Vrba
ředitel
v zastoupení
Mgr. Jiří Klein

otisk úředního razítka

Elektronický podpis - 25.6.2018
Certifikát autora podpisu :
Jméno : Mgr. Jiří Klein
Vydal : PostSignum Qualified C...
Platnost do : 15.1.2019

MVCRX03G2IOI
prvotní identifikátor

odbor eGovernmentu
náměstí Hrdinů 1634/3
Praha 4
140 21

Č. j. MV- 22860-7/EG-2017

Praha 24. dubna 2017
Počet listů: 3

První certifikační autorita, a.s.
Podvinný mlýn 2178/6
Praha 9, PSČ 190 00
ID DS: a69fvfb

zastoupená

Aleš Kapusta člen představenstva
Ing. Roman Kučera člen představenstva

R O Z H O D N U T Í

Ministerstvo vnitra České republiky, odbor eGovernmentu, jako správní orgán příslušný podle ustanovení § 13 odst. 1 zákona č. 297/2016 Sb. o službách vytvářejících důvěru pro elektronické transakce (dále jen „zák. č. 297/2016 Sb.) a čl. 21 odst. 2 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 jen „nařízení EU č. 910/1014), ve správním řízení o žádosti o udělení statusu kvalifikované služby vytvářející důvěru pro službu ověřování platnosti kvalifikovaných elektronických podpisů a pečetí - I.CA QVerify, kterou podali dne 15. února 2017 pan Aleš Kapusta a pan Ing. Roman Kučera, členové představenstva spol. První certifikační autorita, a.s., rozhodlo takto:

uděluje se kvalifikovaný status poskytovatele služeb vytvářejících důvěru v souvislosti se službou I.CA QVerify poskytovateli

První certifikační autorita, a.s.
se sídlem Praha 9 – Libeň
Podvinný mlýn 2178/6, PSČ 19000
IČ 26439395

a uděluje se kvalifikovaný status služby vytvářející důvěru službě

I.CA QVerify

Odůvodnění:

Dne 15. února 2017 podali pan Aleš Kapusta a pan Ing. Roman Kučera, členové představenstva spol. První certifikační autorita, a.s. (dále jen „žadatel") žádost o udělení statusu kvalifikované služby vytvářející důvěru pro službu ověřování platnosti kvalifikovaných elektronických podpisů a pečetí - I.CA QVerify.

Ministerstvo vnitra České republiky udělí v souladu s ustanovením § 13 odst. 1 zák. č. 297/2016 Sb. a čl. 21 odst. 2 nařízení EU č. 910/1014 status kvalifikovaného poskytovatele služeb vytvářejících důvěru a status kvalifikované služby vytvářející důvěru, pokud

a) žadatel předloží oznámení o svém úmyslu začít poskytovat kvalifikovanou službu vytvářející důvěru společně se zprávou o posouzení shody vydanou subjektem posuzování shody,
b) Ministerstvo vnitra České republiky, jakožto orgán dohledu ve smyslu čl. 17 nařízení EU č. 910/1014, dojde k závěru, že poskytovatel služeb vytvářejících důvěru a jím poskytovaná služba vytvářející důvěru splňuje požadavky na kvalifikovaného poskytovatele služeb vytvářejících důvěru a požadavky na kvalifikovanou službu vytvářejících důvěru.

Žadatel předložil výše uvedené zákonné náležitosti. Vzhledem k tomu, že žadatel splnil požadavky pro udělení kvalifikovaného statusu poskytovatele služeb vytvářejících důvěru v souvislosti se službou I.CA QVerify a požadavky pro udělení kvalifikovaného statusu služby vytvářející důvěru službě I.CA QVerify, se žadateli uděluje status kvalifikovaného poskytovatele služeb vytvářejících důvěru

v souvislosti se službou I.CA QVerify a službě I.CA QVerify se uděluje kvalifikovaný status služby vytvářející důvěru.

P o u č e n í :

Proti tomuto rozhodnutí lze podle ustanovení § 152 odst. 1 zákona č. 500/2004 Sb., správní řád, podat rozklad k ministru vnitra. Podle ustanovení § 86 odst. 1 správního řádu se rozklad podává u odboru eGovernmentu Ministerstva vnitra České republiky, a to podle ustanovení § 83 odst. 1 správního řádu ve lhůtě do 15 dnů ode dne jeho oznámení.

Žadatel může začít danou službu I.CA QVerify poskytovat jako kvalifikovanou službu vytvářející důvěru poté, co byl status kvalifikovaného poskytovatele a kvalifikované služby vyznačen v důvěryhodném seznamu České republiky, který je zveřejněn na internetové adrese https://tsl.gov.cz/publ/TSL_CZ.xtsl.

Ing. Roman Vrba
ředitel
(podepsáno elektronicky)

otisk úředního razítka

Elektronický podpis - 26.4.2017

Certifikát autora podpisu :
Jméno : Ing. Roman Vrba
Vydal : PostSignum Qualified C...
Platnost do : 19.6.2017

Příloha č. 4

Popis služby vytváření kvalifikovaných elektronických pečetí na dálku

Východisko služby

Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (dále jen „nařízení eIDAS“), konkrétně bod 52 recitálu, články 29 a 39, body 3 a 4 Přílohy II a Příloha III.

Právní základ

Povinnost používat kvalifikované elektronické pečetě orgány veřejné moci počínaje 20.9.2018 je dána § 8 zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce:

„Nestanoví-li jiný právní předpis jako náležitost právního jednání obsaženého v dokumentu podpis nebo tato náležitost nevyplývá z povahy právního jednání, veřejnoprávní podepisující a jiná právnická osoba, jedná-li při výkonu své působnosti, zapečetí dokument v elektronické podobě kvalifikovanou elektronickou pečetí.“

Kvalifikovaná elektronická pečeť dle bodu 27) článku 3 nařízení eIDAS:

„Zaručená elektronická pečeť, která je vytvořena pomocí kvalifikovaného prostředku pro vytváření elektronických pečetí a která je založena na kvalifikovaném certifikátu pro elektronickou pečeť.“

Požadavky na kvalifikované prostředky pro vytváření elektronických pečetí (QSealCD):

- prostřednictvím „mutatis mutandis“ stanoveny v Příloze II. nařízení eIDAS
- jedná se o stejné požadavky jako na kvalifikované prostředky pro vytváření elektronických podpisů
- stejné funkční požadavky jako pro SSCD prostředky dle směrnice 1999/93/ES pro ty prostředky, které jsou v držení osoby
- v případě prostředků pro vytváření kvalifikovaných elektronických pečetí na dálku dodatečné požadavky na kvalifikované poskytovatele (odst. 3 a 4 Přílohy II. nařízení eIDAS).

Existují dva typy QSealCD:

1. QSealCD v držení pečetící osoby (pokud jsou data pro vytváření elektronických pečetí uchovávána v prostředí spravovaném zcela, nikoli však nutně výhradně uživatelem).
2. QSealCD na dálku (pokud data pro vytváření elektronických pečetí spravuje kvalifikovaný poskytovatel služeb vytvářejících důvěru jménem pečetící osoby).

Služba I.CA RemoteSeal představuje variantu 2 s tím, že certifikace na základě alternativního procesu – musí používat srovnatelnou úroveň bezpečnosti a zároveň certifikační orgán daný postup oznámil Komisi. Alternativní postup může být použit pouze v případě, že příslušné normy neexistují.

Seznam EU pro QSealCD

„Compilation of Member States notification on SSCDs and QSCDs“
https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds

- Seznam je spravován Komisí.
- Komise pouze v roli editora seznamu.
- Mohou přispívat pouze ty členské státy, které měly nebo mají nahlášeny certifikační orgány.
- Je na zodpovědnosti členských států nahlašovat prostředky Komisi a případné změny jejich certifikace.
- Seznam nemá konstitutivní hodnotu, jedná se pouze o informativní seznam.

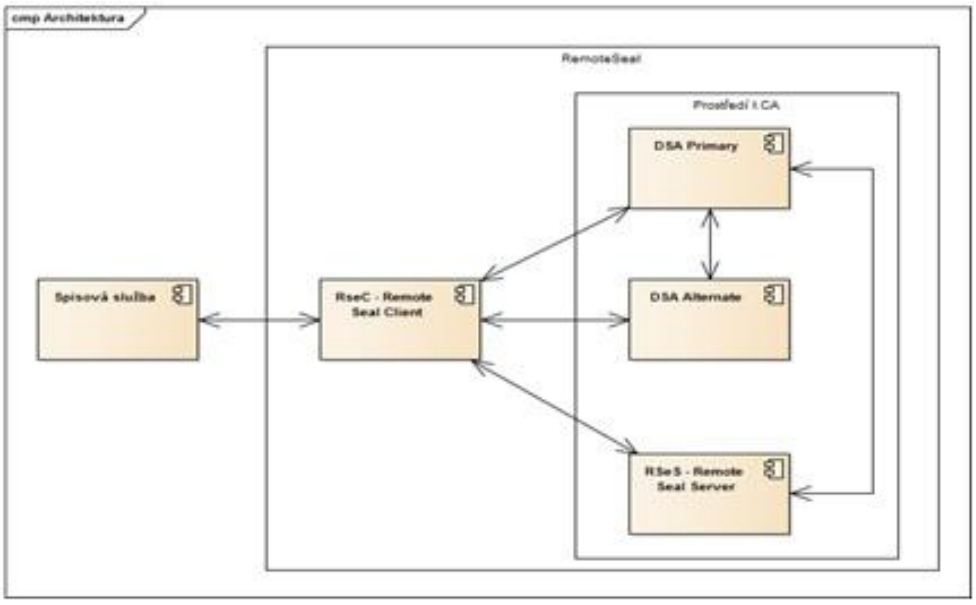
Výběr QSealCD pro službu I.CA RemoteSeal

- ARX (Algorithmic Research) CoSign v8.2
- Společnost ARX koupena v roce 2015 společností DocuSign
- Produkt nadále prodáván pod názvem DocuSign Signature Appliance v8.2

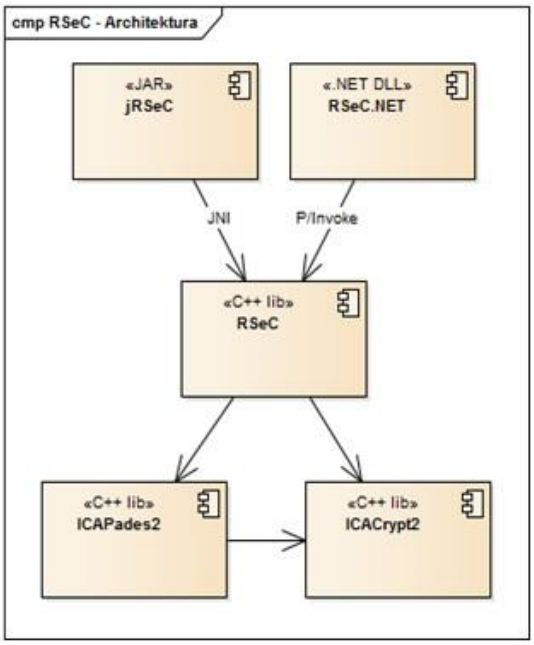
List of QSCDs

Name:	-
Name:	**ARX CoSign v8.2**
Applicant	ARX (Algorithmic Research, Ltd.)
Qualified Signature Creation Device (QSigCD)	yes IMPORTANT NOTE: Device aimed to be managed on behalf of the user (signatory) by a QTSP that can be only considered as QSigCD when duly operated by a QTSP in accordance with eIDAS Regulation (EU) 910/2014.
QSigCD designation by	OCSI
QSigCD designation date	07.02.2017
QSigCD designation expiry	-
QSigCD designation report reference	OCSI/ACC/ARX/01/2017/RA
QSigCD designation report	http://www.ocsi.isticom.it/documenti/accertamenti/arx/ac_rda_eidas_cosign_82_v1.0.pdf
Art.30.3.(b) notified alternative certification method	http://www.ocsi.isticom.it/index.php/dispositivi-di-firma/procedura-di-accertamento
CC certification report reference	OCSI/CERT/IMQ/05/2016/RC
CC certification body	-
CC certification date	12.09.2016
CC certification report	http://www.ocsi.isticom.it/documenti/certificazioni/arx/rc_arx_cosign_82_v1.0.pdf
Security Target	http://www.ocsi.isticom.it/documenti/certificazioni/arx/st_arx_cosign_82_v2.6.pdf
Conformity Protection Profile	-
Evaluation criteria and version	-
Evaluation level	-
Developers	-
Qualified Seal Creation Device (QSealCD)	yes IMPORTANT NOTE: Device aimed to be managed on behalf of the user (seal creator) by a QTSP that can be only considered as QSealCD when duly operated by a QTSP in accordance with eIDAS Regulation (EU) 910/2014.
QSealCD designation by	OCSI
QSealCD designation date	07.02.2017
QSealCD designation expiry	-
QSealCD designation report reference	OCSI/ACC/ARX/01/2017/RA
QSealCD designation report	http://www.ocsi.isticom.it/documenti/accertamenti/arx/ac_rda_eidas_cosign_82_v1.0.pdf
Art.30.3.(b) notified alternative certification method	http://www.ocsi.isticom.it/index.php/dispositivi-di-firma/procedura-di-accertamento
CC certification report reference	OCSI/CERT/IMQ/05/2016/RC
CC certification body	-
CC certification date	12.09.2016
CC certification report	http://www.ocsi.isticom.it/documenti/certificazioni/arx/rc_arx_cosign_82_v1.0.pdf
Security Target	http://www.ocsi.isticom.it/documenti/certificazioni/arx/st_arx_cosign_82_v2.6.pdf

Architektura služby



- **RSeC** – RemoteSeal Client – klientská komponenta určená pro integraci do volající aplikace, typicky do spisové služby.
- **RSeS** – RemoteSeal Server – základní aplikační server provozovaný I.CA, který realizuje první vrstvu autentizace volající aplikace a udržuje evidenci provedených transakcí (opečetění).
- DSA Primary - DocuSign Signature Appliance Primary - primární HSM modul, který drží privátní klíče uživatelů a podepisuje
- DSA Alternate - DocuSign Signature Appliance Alternate - záložní HSM modul, který udržuje repliku databáze privátních klíčů a v případě výpadku primárního HSM zastoupí primární HSM pro podepisování
- **RSeActivationUtil** – Aktivační utilita sloužící k aktivaci RSeC pomocí tzv. aktivační karty.



- RemoteSeal Client
- Klientská komponenta sloužící k zadávání transakcí (požadavků na opečetění dat) do systému RemoteSeal.
- Nativní C++ jádro
- Distribuováno ve formě:
- JAR pro Java
- .NET assembly pro .NET
- V případě zájmu možno volat přímo nativní jádro.

Zřízení služby

Zřízení služby bude probíhat na vybraných pobočkách RA následujícím způsobem:

- Klient navštíví pobočku RA.
- Operátor RA vydá klientovi prvotní autentizační komerční certifikát (**FAC** - First Authentication Certificate) na aktivační kartu/token (viz názvosloví). FAC je nutné zavést do AUTHu jako autentizační certifkát pro RemoteSeal pro daného uživatele (budou provádět ručně obchodníci na základě SN certifikátu, které jim zašle klient).
- Operátor RA připraví žádost o pečetící certifikát pro uživatele.
- Operátor RA vygeneruje párová data pro pečetící certifikát (z pohledu operátora atomická operace) což obnáší:
    - ICARA pomocí **RSeS** (RemoteSealServer) založí pro klienta uživatele na DSA včetně prvotního hesla **FP** (First Password).
    - ICARA náhodně vygeneruje nové heslo **PP** (Production Password) (drženo pouze v RAM)
    - ICARA náhodně vygeneruje 256b AES šifrovací klíč **SK** (Secret Key)
    - ICARA zašifruje pomocí AES-KW (kde **K** je **SK** a **PP** je **W**) do výsledku **CPP** (Ciphered Production Password)
    - ICARA zašifruje pomocí RSAES_PKCS#1 v1.5 klíč **SK** veřejným klíčem **FAC** do výsledku $\mathbf{CSK_{FAC}}$ (Ciphered Secret Key)

  - ICARA následně uloží do RSeS kryptogramy **CSK_{FAC}** a **CPP**
  - ICARA provede aktivaci uživatelského účtu v DSA pomocí FP (a tudíž i změnu hesla na PP).
  - ICARA provede pod účtem uživatele (s heslem PP) generování párových dat pro vydání prvotního pečetícího certifikátu.
- Operátor RA pomocí ICARA podepíše žádost o vydání pečetícího certifikátu privátním klíče párových dat na DSA (zde můžeme teoreticky zapojit uživatele aby zadal PIN na pinpadové čtečce (pro rozšifrování **CPP** pomocí privátního klíče **FAC**)
- Na základě žádosti proběhne na CA vydání pečetícího certifikátu.
- Pečetící certifikát:
- CA pošle na mailovou adresu uživatele.
- ICARA uloží na čipovou kartu uživatele.
- ICARA uloží na DSA (díky přihlášení jako uživatel)
- Klient odchází z RA s aktivační(m) kartou/tokenem.

Aktivace RSeC

- Pro aktivaci RSeC spustí uživatel (např.: oprávněná osoba úřadu) dodávanou GUI utilitu RSeActivationUtil (dále jen utilita)
- Utilita vyzve uživatele k vložení aktivační karty (potažmo aktivačního tokenu), načež utilita:
  - Naváže spojení s RSeS pomocí oboustranně autentizovaného HTTPS za pomoci **FAC** (uživatel bude vyzván k zadání PINu)
  - Automaticky vytvoří žádost o vydání následného certifikátu **SACi** (Secondary Authentication Certificate číslo i), která bude podepsána **FAC** a privátní klíč k **SACi** se bude generovat v SW (nikoliv na kartě)
  - Žádost se odešle ke zpracování na CA, kde se obratem vydá následný certitifikát **SACi** a ten se stáhne zpět do utility
  - Utilita si z RSeS stáhne **CSK_{FAC}** (drží se pouze v RAM)
  - Pomocí privátního klíče **FAC** na aktivační kartě dešifruje **CSK_{FAC}** na **SK** (drží se pouze v RAM)
  - Zašifruje pomocí RSAES_PKCS#1 v1.5 klíč **SK** veřejným klíčem **SACi** do výsledku **CSK_{SACi}**
  - Utilita následně uloží do RSeS kryptogram **CSK_{SACi}**

- Utilita může případně uživatele vyzvat k dalším nastavením RSeC, pokud nějaká budou (např.: přidávání TS, viditelný podpis, reason, location pokud se tyto nebudou nastavovat pomocí RSeCAPI)
- Následně utilita vytvoří aktivační soubor, kde bude uložen certifikát **SACi** včetně privátního klíče.
- Uživatel tento aktivační soubor následně načte do spisové služby (obecně do aplikace volající RSeC), která jej bude pro použití RemoteSeal předávat do RSeC.

Technické parametry RSeActivationUtil

- Jednoduchá Windows GUI utilita.
- Nemusí být spouštěna na stejném PC, na kterém je provozován RSeC.
- Vyžaduje: .NET 4.0

Opečetění dokumentu

- Proces opečetění dokumentu inicializuje spisová služba (obecně volající aplikace), která má integrovanou knihovnu RSeC.
- Spisová služba předá do RSeC dokument k opečetění spolu s nastavením pečetění (viditelný/neviditelný podpis, formát, přidání TS, atp.) + aktivační soubor vzniklý při aktivaci RSeC
- RSeC připraví dokument k podpisu a sestaví žádost o opečetění (obsahující číslo jednací dokumentu (obecně jednoznačný textový identifikátor), parametry podpisu, hash původního dokumentu a hash který bude vstupem pro výpočet kryptogramu)
- Tato žádost bude podepsána pomocí **SACi**
- Následně RSeC naváže oboustraně autentizovaný TLS kanál pro komunikaci s RSeS pomocí **SACi**
- Navázaným kanálem předá podepsanou žádost o opečetění na RSeS
- RSeS obratem vrátí do RSeC kryptogramy $\mathbf{CSK_{SACi}}$ a **CPP**, které budou v RSeC drženy pouze v RAM
- RSeC pomocí **SACi** rozšifruje $\mathbf{CSK_{SACi}}$ na **SK** a pomocí něj rozšifruje **CPP** na **PP** (vše pouze v RAM, po dešifrování **PP** možno ostatní z RAM uvolnit)
- RSeC následně naváže anonymní HTTPS na DSA s aplikováním certificate pinningu na ověření autenticity DSA
- Následně tímto kanálem po autentizaci pomocí **PP** vytvoří na DSA kryptogram pomocí privátního klíče pečetícího certifikátu
- Po vytvoření kryptogramu se z RAM odstraní **PP**
- RSeC využije kryptogram pro kompletaci podepsaného dokumentu
- Pokud je vyžadován podpis s časovým razítkem, je TS do dokumentu přidáno nyní, přičemž RSeC se vůči TSA autentizuje pomocí **SACi**
- Hotový opečetěný dokument je vrácen spisové službě

Automatické prodloužení služby

- Součástí RSeC bude funkcionalita automatické obnovy **SACi** (obdobné řešení jako v QVerify)
- Nejprve se z RSeS stáhne $\mathbf{CSK_{SACi}}$
- Pomocí nově vygenerované veřejného klíče se vygeneruje $\mathbf{CSK_{SACj}}$ a spolu s veřejným klíčem se nahraje na RSeS.
- Následně je možné provést standardní obnovu a nahrát nově vydaný certifikát SACj na RSeS

Obnova pečetícího certifikátu

- V rámci automatického prodloužení služby (zakotveného ve Smlově) bude také probíhat automatická obnova pečetícího certifikátu
- RSeC s určitým předstihem před vypršením certifikátu vygerenuje na DSA nový pár klíčů a vytvoří žádost o vydání následného certifikátu, kterou opečetí původním certifikátem
- Žádost o následný certifikát se zpracuje na CA standardní cestou
- RSeC následně uloží do DSA následný certifikát a od toho okamžiku jej začne pro pečetění využívat

Podporované formáty podpisu:

- CAdES-B-B, CAdES-B-T
  - Dle normy EN 319 122, ve variantách:
  - Interní
  - Externí
- PAdES-B-B, PAdES-B-T
  - Dle normy EN 319 142, ve variantách:
  - Neviditelný
  - Viditelný – Text/Obrázek/Text+Obrázek + volitelně obrázek na pozadí
- XAdES-B a XAdES-T
  - dle normy ETSI TS 103 171, a to ve variantě enveloped, přičemž:
    • Na vstupu bude XML dokument, který bude kompletně použit jakožto vstup podepisovaných data.
    • Na vstupu bude určeno ID elementu, do nějž bude jakožto poslední child element přidán element Signature obsahující nově vytvořenou kvalifikovanou elektronickou pečeť.
    • Na vstupu bude definice požadovaných transformací , digest metody a mime-type referencovaných dat pro element Reference s id="xadesReference".
    • Na vstupu bude volba hash algoritmu podpisu (SHA256/SHA384/SHA512)
    • Na vstupu bude možnost volby podpisu typu XAdES-B/XAdES-T tedy bez nebo s časovým razítkem.

Dostupnost

Pro službu vytváření kvalifikovaných elektronických pečetí na dálku v režimu 365 x 24 je stanovena min. dostupnost služby (SLA) 98 %. Do této doby nebudou započítány plánované odstávky nahlášené minimálně 7 dní předem oprávněným zástupcům zadavatele. Jakékoli plánované odstávky systému budou realizovány mimo pracovní dny. Minimální garantovaná propustnost činí 30 ks vytvořených pečetí/min.

Příloha č. 5

Popis služby ověřování platnosti kvalifikovaných elektronických podpisů a pečetí

Východisko služby:

Nařízení 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 (eIDAS), konkrétně články 32, 33 a 40.

Nařízení:

a) stanoví podmínky, za nichž členské státy uznávají prostředky pro elektronickou identifikaci fyzických a právnických osob, které spadají do oznámeného systému schématu elektronické identifikace jiného členského státu;

b) stanoví pravidla pro služby vytvářející důvěru;

c) stanoví právní rámec pro elektronické podpisy, elektronické značky, elektronická časová razítka, elektronické dokumenty, služby registrovaného elektronického doručování a certifikační služby pro autentizaci internetových stránek.

Jednou ze služeb vytvářejících důvěru, která může být poskytována pouze kvalifikovaným poskytovatelem služeb vytvářejících důvěru (dle minulé terminologie akreditovaným poskytovatelem certifikačních služeb, I.CA), je kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů a pečetí I.CA QVerifyTL (také „I.CA QVerify“) (čl. 32, 33 a 40 eIDAS).

Povinnost subjektů ověřovat podpisy přijatých elektronických dokumentů je dána článkem 32 eIDAS a §12 zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce.

Veřejnoprávní původci mají povinnost ověřování definovanou § 4 odst. 4-7 vyhlášky č. 259/2012 Sb., o podrobnostech výkonu spisové služby.

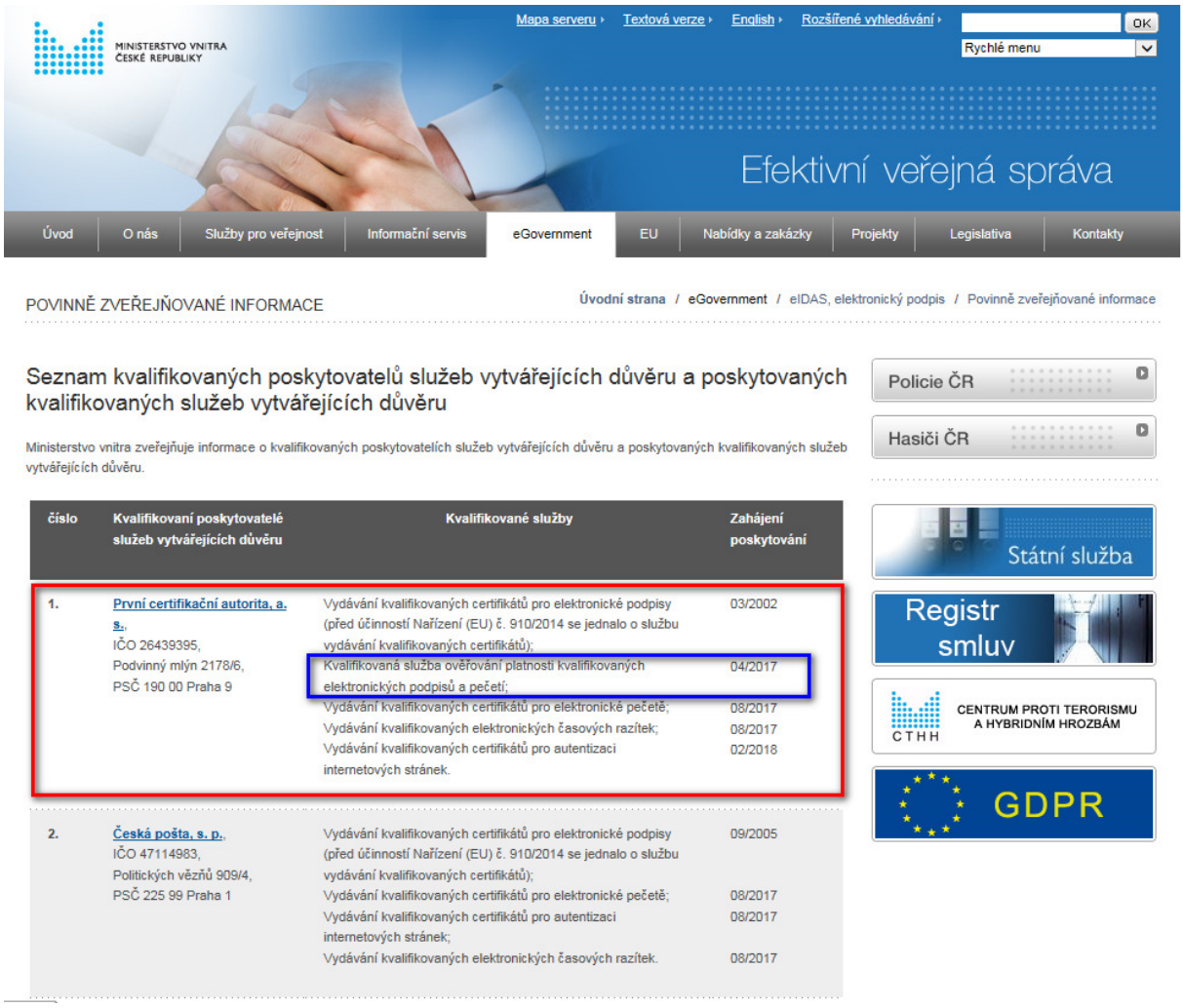
PDF či XML protokoly, jež jsou výstupem procesu ověření platnosti elektronických podpisů, představují závazný výstup služby provozované I.CA – kvalifikovaným poskytovatelem služeb vytvářejících důvěru dle eIDAS. Za správnost tohoto výstupu je I.CA právně zodpovědná. PDF protokol a XML data jsou označena jednoznačným identifikátorem jedinečným v rámci výstupů kvalifikované služby. Odpovědnost za případnou škodu způsobenou klientovi nesprávným vyhodnocením platnosti podpisu a důkazní břemeno jsou definovány v čl. 13 odst. 1 eIDAS:

„V případě kvalifikovaného poskytovatele služeb vytvářejících důvěru se úmysl nebo nedbalost předpokládá, pokud daný kvalifikovaný poskytovatel služeb vytvářejících důvěru neprokáže, že škoda podle prvního pododstavce nastala bez jeho úmyslu nebo nedbalosti.“

Znamená to, že ověření elektronického podpisu poskytované jako služba kvalifikovaného poskytovatele služeb vytvářejících důvěru představuje maximální právní i věcnou odpovědnost za případnou škodu současně s přenesením odpovědnosti za správné ověření elektronického podpisu na třetí stranu – kvalifikovaného poskytovatele služeb vytvářejících důvěru. Ten totiž proto, aby mohl kvalifikovanou službu nabízet a provozovat, musel projít auditem ze strany subjektu k tomu oprávněného Českým institutem pro akreditaci, tj. musel splnit celou řadu povinností daným technickými normami, na něž se eIDAS odkazuje. Postupy a vlastní fungování služby ověřování elektronického podpisu tak bylo prověřeno nezávislými experty subjektu posuzování shody, Českým institutem pro akreditaci (nejvyšší orgán v ČR pro tuto oblast) a ministerstvem vnitra jako gesčním orgánem pro oblast eIDAS v ČR.

Podle eIDAS zveřejňuje Ministerstvo vnitra ČR seznam kvalifikovaných poskytovatelů a kvalifikovaných služeb vytvářejících důvěru na webové stránce:

http://www.mvcr.cz/clanek/seznam-kvalifikovanych-poskytovatelu-sluzeb-vytvarejicich-duveru-a-poskytovanych-kvalifikovanych-sluzeb-vytvarejicich-duveru.aspx



Vzhledem k tomu, že zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, (tzv. Adaptační zákon) zavedl 2-leté přechodné období, během kterého může být ze strany veřejnoprávního podepisujícího použit při podepisování dokumentu, kterým právně jedná, místo kvalifikovaného elektronického podpisu uznávaný elektronický podpis (zaručený elektronický podpis založený na kvalifikovaném certifikátu pro elektronický podpis) a současně (bez přechodného období) může být při úkonu, kterým se právně jedná vůči veřejnoprávnímu podepisujícímu použit uznávaný elektronický podpis nebo kvalifikovaný elektronický podpis, je nutné, aby byla služba I.CA QVerify rozšířena oproti požadavkům eIDAS i o ověřování platnosti uznávaného elektronického podpisu.

Pozn: vzhledem k přechodnému období daného pro ČR zákonem č. 297/2016 Sb. budou ověřovány a rozlišovány jak kvalifikovaný podpis, tak i uznávaný podpis.

Je třeba nezaměňovat pojem „uznávaný“ elektronický podpis dle zákona č. 297/2016 se stejným pojmem dle zrušeného zákona č. 227/2000 Sb., o elektronickém podpisu („ZoEP“).

Dle ZoEP: uznávaným elektronickým podpisem se rozumí zaručený elektronický podpis založený na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb a obsahujícím údaje, které umožňují jednoznačnou identifikaci podepisující osoby (§11 odst. 3).

Dle zákona č. 297/2016 Sb.: uznávaným elektronickým podpisem se rozumí zaručený elektronický podpis založený na kvalifikovaném certifikátu pro elektronický podpis nebo kvalifikovaný elektronický podpis (§6 odst. 2).

Přičemž zaručeným elektronickým podpisem se rozumí elektronický podpis, který splňuje následující požadavky:

1. je jednoznačně spojen s podepisující osobou,

2. umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě,

3. byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou,

4. je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat (§2 odst. b) ZoEP).

V dalším textu je pro ověření platnosti kvalifikovaných a uznávaných elektronických podpisů a kvalifikovaných elektronických pečetí použita zkratka „ověření platnosti podpisu".

Stručný popis (manažerské shrnutí):

Služba je koncipována jako komponenta pro ověření platnosti podpisu instalovaná v prostředí klienta a volaná obvykle spisovou službou. Služba ověření podpisu pracuje s dokumenty ve standardních a legislativně podporovaných formátech PAdES a CAdES B-B, B-T a B-LT (CAdES v interní i externí verzi) a XAdES B-B, B-T a B-LT[1]. Výstupem je stav ověření (platný/neplatný podpis, nelze ověřit, důvod, proč nelze ověřit nebo proč je podpis neplatný), čas, ke kterému se ověřovalo, zdroj času (čas obdržení požadavku, časové razítko, parametr zadaný uživatelem, data, na základě kterých bylo ověření provedeno, legislativní typ podpisu, zda je certifikát na QESigCD). Ověření má charakter elektronicky podepsané XML odpovědi v definované struktuře, vhodné pro automatizované zpracování. Současně jsou ukládána data pro následné generování PDF protokolu v případě požadavku klienta (generuje I.CA). Jeho účelem je potvrdit výsledek ověření elektronického podpisu i v lidsky čitelné formě v případě požadavku klienta např. před soudem.

Podrobný popis:

Služba podporuje ověření dokumentu ve standardních a legislativně podporovaných formátech:

- XAdES v úrovni shody B, T a LT
- PAdES v úrovni shody B, T a LT
- CAdES v úrovni shody B, T a LT (v interní i externí verzi)
- ASiC-E XAdES-B-B, ASiC-E XAdES-B-T, ASiC-E XAdES-B-LT
- ASiC-E CAdES-B-B, ASiC-E CAdES-B-T, ASiC-E CAdES-B-LT
- ASiC-S with CAdES B, T a LT

[1] Prováděcí rozhodnutí Komise (EU) č. 2015/1506.

- ASiC-S with XAdES B, T a LT
- ASiC-S with CAdES B-B,B-T a B-LT
- ASiC-S with XAdES B-B, B-T a B-LT.

Služba též umožňuje ověřit platnost podpisu/pečetě obálky datové zprávy Informačního systému datových schránek formátu ZFO. Služba však nepodporuje ověření podpisů/pečetí obsahujících atribut specifikující použitou podpisovou politiku (PP). Z tohoto důvodu nebude výsledkem ověření indikace TOTAL-PASSED.

Služba je dále doplněna o nekvalifikovanou nadstavbu pro ověřování platnosti uznávaných elektronických podpisů e-mailových zpráv formátů S/MIME a PAdES - Basic. V tomto případě služba ověří platnost certifikátu, na němž je uznávaný elektronický podpis založen včetně kryptografické správnosti podpisu a hashe podepsaných dat a vrátí elektronicky podepsanou XML odpověď, která bude obsahovat informace o typu podpisového certifikátu, vydavateli, době jeho platnosti, zda je certifikát na QESCD, revokaci, atd. a případné info o problémech s ověřením kryptografické platnosti podpisu ve struktuře shodné s ověřením podpisu u kvalifikované služby. Výsledek ověření je však informativní a vzhledem k praktické nekonformnosti S/MIME a PAdES - Basic podpisů se standardy dle eIDAS prakticky nikdy neskončí výsledkem TOTAL-PASSED.

Při ověřování platnosti podpisu/pečetě obálky datové zprávy formátu ZFO, e-mailové zprávy formátu S/MIME a formátu PAdES - Basic neověří služba platnost časového razítka. Důvodem je skutečnost, že dle normy EN 319 102-1, definující postup ověřování, se při ověřování podpisu s razítkem nejdříve provede Basic validační proces a pouze pokud skončí s jedním z výsledků:

- PASSED,
- INDETERMINATE/CRYPTO_CONSTRAINS_FAILURE_NO_POE,
- INDETERMINATE/REVOKED_NO_POE,
- INDETERMINATE/REVOKED_CA_NO_POE,
- INDETERMINATE/TRY_LATER nebo INDETERMINATE/OUT_OF_BOUNDS_NO_POE,

lze pokračovat na ověřování razítek.

Protože ale ověření formátu ZFO kvůli přítomnosti atributu PP (podpisová politika) skončí s indikací INDETERMINATE/POLICY_PROCESSING_ERROR a ověření S/MIME kvůli chybějícímu atributu SigningCertificate, stejně jako ověření PAdES – Basic kvůli nepodporovanému formátu dle eIDAS skončí s indikací INDETERMINATE/SIG_CONSTRAINTS_FAILURE, proces ověřování musí být ukončen a k ověření časového razítka nedojde.

Časový okamžik, ke kterému je možné platnost podpisu ověřit:

Služba umožní vybrat[2], k jakému času má ověřování proběhnout (v sestupném pořadí):

1. ověřovat k času uvedenému v časovém razítku (pokud je v dokumentu či podpisu přítomno)
2. ověřovat k okamžiku podpisu, rozhodnému okamžiku nebo jinému času zadanému klientem (parametr předávaný klientem)
3. ověřovat k času přijetí požadavku na ověření v systému I.CA (pokud z nějakého důvodu požadavek na ověření parametr času neobsahuje).

Služba ověření podpisu je poskytována jako rozdělená mezi klienta a server.

[2] Lze ponechat jako parametrické či definovat jednu z možností.

Kompletní ověření je prováděno na serveru v prostředí I.CA. Pomocí komponenty I.CA[3] umístěné a volané z prostředí klienta dojde k výpočtu hashe z podepsaných dat a získání podpisové struktury. Tato data jsou zaslána na server, kde proběhne vlastní ověření. **Znamená to, že podepsaný dokument (tj. data v dokumentu = obsah dokumentu), jehož podpis se ověřuje, nikdy neopustí prostředí klienta**.

Základní postup ověření:

1. Volání komponenty (např. spisovou službou)
2. Autentizace uživatele ke službě (komerční/technologický (komerční serverový) certifikát I.CA)
3. Výpočet hashe z podepsaných dat, získání podpisové struktury
4. Zaslání dat k ověření ze strany klienta na server I.CA
5. Provedení vstupních kontrol
6. Provedení ověření jednotlivých podpisů (tj. dvojic podpisová struktura + hash)
7. Sestavení odpovědi s výsledkem ověření - XML elektronicky podepsaná datová struktura (zasílaná on-line)
8. Uložení dat pro následné generování PDF protokolu s výsledkem ověření v prostředí I.CA
9. Předání výsledku ověření v XML struktuře aplikaci klienta
10. Zalogování procesu ověření
11. Záznam do STAT o využití služby
12. Konec zpracování.

Výstupem služby je:

Stav ověření:

- platný/neplatný podpis/nelze ověřit + důvod, proč nelze ověřit nebo proč byl podpis neplatný
- čas, ke kterému se ověřovalo
- zdroj času (časové razítko, parametr zadaný uživatelem, čas obdržení požadavku)
- data, na základě kterých bylo ověření provedeno (OCSP, CRL)
- legislativní typ podpisu (kvalifikovaný/uznávaný)
- zda byl kvalifikovaný certifikát (resp. privátní klíč) generován a uložen na QESigCD
- výsledek ověření certifikátu
- zda je časové razítko vydáno kvalifikovaným poskytovatelem
- hash ověřovaných dat a další informace.

Stav ověření má charakter:

Odpovědi v definované struktuře (xml data), vhodné pro automatizované zpracování. Odpověď je elektronicky podepsána externím CAdES podpisem a zasílána automaticky on-line.

Omezující podmínky:

[3] Komponenta mimo parsování podpisu a zajištění potřebných dat pro ověření zajišťuje komunikaci s interním systémem I.CA; za její aktuálnost (právní i technickou) a integritu odpovídá I.CA. Komponenta neumožňuje komunikaci s jiným poskytovatelem než I.CA.

a) Ověřuje se platnost podpisu či podpisů v daném dokumentu. PDF protokol i XML data budou obsahovat tabulkovou strukturu vážící se k jednomu podpisu a struktur bude tolik, kolik bude v dokumentu podpisů (PDF/XML protokol je vždy jeden pro jeden dokument)[4].
b) Ověřovány jsou podpisy založené na certifikátech vydaných všemi důvěryhodnými poskytovateli zemí EU (EUTL, LoTL).
c) Ověřovány budou i podpisy založené na již expirovaných certifikátech, a to i tehdy, pokud je v dokumentu již expirované razítko. To znamená, že ověření takového podpisu nebude odmítnuto, ale ověření proběhne s výsledkem, že podpis je neplatný a bude standardně vystaven protokol o ověření.
d) Časová razítka jsou vydávána časovou autoritou I.CA.

Dostupnost

Pro službu ověřování platnosti podpisů v režimu 365 x 24 je stanovena min. dostupnost služby (SLA) 98 %. Do této doby nebudou započítány plánované odstávky nahlášené minimálně 7 dní předem oprávněným zástupcům zadavatele. Maximální garantovaná doba nepřetržité nedostupnosti činí 30 min. Jakékoli plánované odstávky systému budou realizovány mimo pracovní dny. Minimální garantovaná propustnost činí 100 ks ověření/min.

Podporované platformy - klientská komponenta.

Klientská komponenta je realizována v Javě 32b a 64b a .NET.

Bezpečnostní požadavky a jejich splnění:

Důvěrnost:

- Ověřovaná data nejsou v systému ukládána
- Důvěrnost dat je řešena:
  - Při přenosu dat: prostřednictvím SSL protokolu.
  - Při zpracování požadavku na ověření na serveru: s ověřovanými daty se pracuje pouze v paměti a nejsou v žádném kroku fyzicky uložena do souboru (ani dočasného) nebo databáze. Po procesu ověření jsou data z paměti vymazána.
  - Celý proces ověření je logován.

Integrita:

- Ověřovaná data nejsou v systému ukládána. Integrita vstupních dat při přenosu je řešena na úrovni datové struktury webové služby (vstupem je hash ověřovaných dat a hash z podpisu) a jejich kontrolou na serveru.

[4] Viz příklad v příloze.

Příklad PDF protokolu:

CERTIFICATION AUTHORITY

www.ICA.cz

PROTOKOL Č. 23794699

O OVĚŘENÍ PLATNOSTI KVALIFIKOVANÉHO ELEKTRONICKÉHO PODPISU A PEČETĚ

Identifikace ověřovaného dokumentu: Smlouva-o-poskytovani-sluzeb-ICA final 06-11-17.pdf

PODPIS 1

Podpisové časové razítko	
Čas ověření	01.08.2018 11:14
Zdroj ověření	CRL č. 6119
Čas vydání časového razítka	08.01.2018 13:24:52
Předmět certifikátu časové autority	C=CZ, O=První certifikační autorita, a.s., CN=I.CA Time Stamping Authority TSS/TSU 4 02/2017, serialNumber=NTRCZ-26439395
Sériové číslo časového razítka	590050AA7A80
Výsledek ověření	Platný

Profil podpisu	EN 319 142-1 PAdES-B-T
Legislativní typ podpisu	Zaručený elektronický podpis založený na Kvalifikovaném certifikátu
Hash podepsaných dat	2556A8BE62184BB678FFF3483071250C191E5A1C7779EC1FDE52FB6C628BF1A1
Čas ověření	01.08.2018 11:14
Zdroj ověření	
Sériové číslo certifikátu	11250265
Vydavatel certifikátu	C=CZ, CN=I.CA Qualified 2 CA/RSA 02/2016, O=První certifikační autorita, a.s., serialNumber=NTRCZ-26439395
Platnost certifikátu od - do	25.05.2017 7:21:06 - 25.05.2018 7:21:06
CN certifikátu	Roman Kučera
Kvalifikovaný certifikát	Ano
Certifikát vydán na QESigCD	Ne
Výsledek ověření certifikátu	Platný
Výsledek ověření	Nelze určit

Identifikace ověřovaného dokumentu: Smlouva-o-poskytovani-sluzeb-ICA final 06-11-17.pdf

PODPIS 2

Podpisové časové razítko	
Čas ověření	01.08.2018 11:14
Zdroj ověření	CRL č. 1323
Čas vydání časového razítka	10.01.2018 08:07:28

Příloha č. 6

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 předávané Subjektem údajů za výše uvedeným Účelem smlouvy v podobě elektronických a/nebo tištěných dokumentů, které mohou obsahovat níže uvedené kategorie Osobních údajů:

a) jméno nebo jména,

b) příjmení,

c) titul (před i za jménem),

d) údaje o adrese trvalého pobytu

e) datum narození,

f) rodné číslo,

g) e-mailová adresa,

h) číslo primárního a sekundárního osobního dokladu,

i) název zaměstnavatele,

j) identifikátor klienta Ministerstva práce a sociálních věcí.

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 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 Zpracovatel je povinen mít sjednané a po celou dobu platnosti této smlouvy udržovat v platnosti pojištění proti rizikům, ve formě a ve výši, které jsou obvyklé v oblasti činnosti Zpracovatele, zejména pojištění odpovědnosti za škodu způsobenou při výkonu činnosti Zpracovatele.

2.7 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: 

Česká republika - Ministerstvo školství, mládeže a tělovýchovy, Karmelitská 529/5, 118 12 Praha 1

e-mail:

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 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 o skutečnostech, které Správce 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 pří 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 důvěryhodných zaměstnanců; důvěryhodným zaměstnancem se rozumí osoba bez záznamu v trestním rejstříku a s důvěryhodnými referencemi o předchozím profesním působení.

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 vybavení Registrační autority u Správce, který zajišťuje přístup pouze pověřených osob na základě přístupových kódů či hesel, a Osobní údaje pravidelně zálohuje. 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.
- pravidelné 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 ochraně OÚ, Nařízením a jinými právními předpisy.

4. NÁHRADA ŠKODY

4.1 V případě, že Zpracovatel poruší jakoukoli povinnost stanovenou touto smlouvou nebo právními předpisy, které se v souvislosti s touto smlouvou aplikují, bude Správce oprávněn požadovat po Zpracovateli náhradu způsobené újmy, a to včetně sankcí uložených Správci příslušnými orgány.

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.