**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,](http://www.ica.cz/)
7. ve všech dalších dokumentech, které budou předány Objednateli a jeho pracovníkům Poskytovateli (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.](http://www.ica.cz/)
2. SSL certifikáty jsou dvojího typu:
   1. tzv. Domain validated SSL certifikát (dále jen "DV") obsahující v příslušných položkách plně kvalifikovaná doménová jména.
   2. tzv. Organization validated SSL certifikát (dále jen "OV") obsahující navíc informace o 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 XXXXX 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 XXXXXXXXX. Žadatel může pro generování žádosti použít neveřejné generátory (při zachování důvěrnosti) dostupné na:

* XXXXXXXXXXXXXXXXXX pro DV certifikát
* XXXXXXXXXXXXXXXXXX pro OV certifikát
* V předmětu e-mailu s žádostí musí být uvedeno: *"Žádost o SSL certifikát".*
* V těle emailu musí být uvedeno: *"Já, níže uvedený, tímto prohlašuji, že všechny údaje uvedené v žádosti o SSL certifikát jsou pravdivé".*

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

## 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

## 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,](http://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

## 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,](http://www.ica.cz/) dnsName = mail.ica.cz).

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

1. **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).

## 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/pki- validation/, ve kterém vytvoří soubor ica.html a obsahem souboru bude náhodný řetězec, který poskytne I.CA,
* správce domény pro požadované FQDN vytvoří nový DNS záznam typu CNAME nebo TXT, který bude obsahovat náhodný řetězec, který určí I.CA.

Platnost náhodných řetězců je ve všech případech 30 dní.

## 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.

## 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 Podpis zaměstnance

ČR – Ministerstvo školství, mládeže a tělovýchovy

**Příloha č. 2**

**Rozsah a forma součinnosti při provozování registrační autority**

# I.

## Úvod

**I.CA** (dále jen „provozovatel“) uzavřela s Objednatelem smlouvu, na základě které bude Objednatel provozovat registrační autoritu, vydávající kvalifikované certifikáty, certifikáty pro elektronickou pečeť a komerční certifikáty včetně komerčních technologických (serverových) certifikátů. Objednatel 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 kvalifikované certifikáty pro elektronickou pečeť
  + ověřování totožnosti žadatelů o kvalifikované certifikáty v souladu s platnými certifikačními politikami,
  + vydávání kvalifikovaných a kvalifikovaných certifikátů pro elektronickou pečeť,
  + přijímání žádostí o komerční certifikáty včetně komerčních technologických (serverových) certifikátů,
  + ověřování totožnosti žadatelů o komerční certifikáty včetně komerčních technologických (serverových) certifikátů v souladu s platnými certifikačními politikami,
  + vydávání komerčních certifikátů včetně komerčních technologických (serverových) certifikátů,
  + ostatní s tím související činnosti, tj. vedení dokumentace k vydaným certifikátům.

# II.

## Práva a povinnosti vykonavatele (osoby pověřené příkazcem)

Objednatel 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.

Objednatel je povinen:

1. Dodržovat platnou Certifikační politiku I.CA pro kvalifikované certifikáty (CPQC), platnou Certifikační politiku I.CA pro kvalifikované certifikáty pro elektronickou pečeť (CPEP) 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 technologických (serverových) certifikátů (CPKC) a platnou Provozní směrnici pro pracovníky Registračních autorit I.CA vydávající komerční certifikáty (PSKRA).
3. Řídit se pokyny provozovatele.

# III.

## Práva a povinnosti poskytovatele (I.CA)

Poskytovatel je oprávněn:

1. Požadovat od Objednatele dodržování platné CPQC, CPEP a PSQRA, upozornit jej na

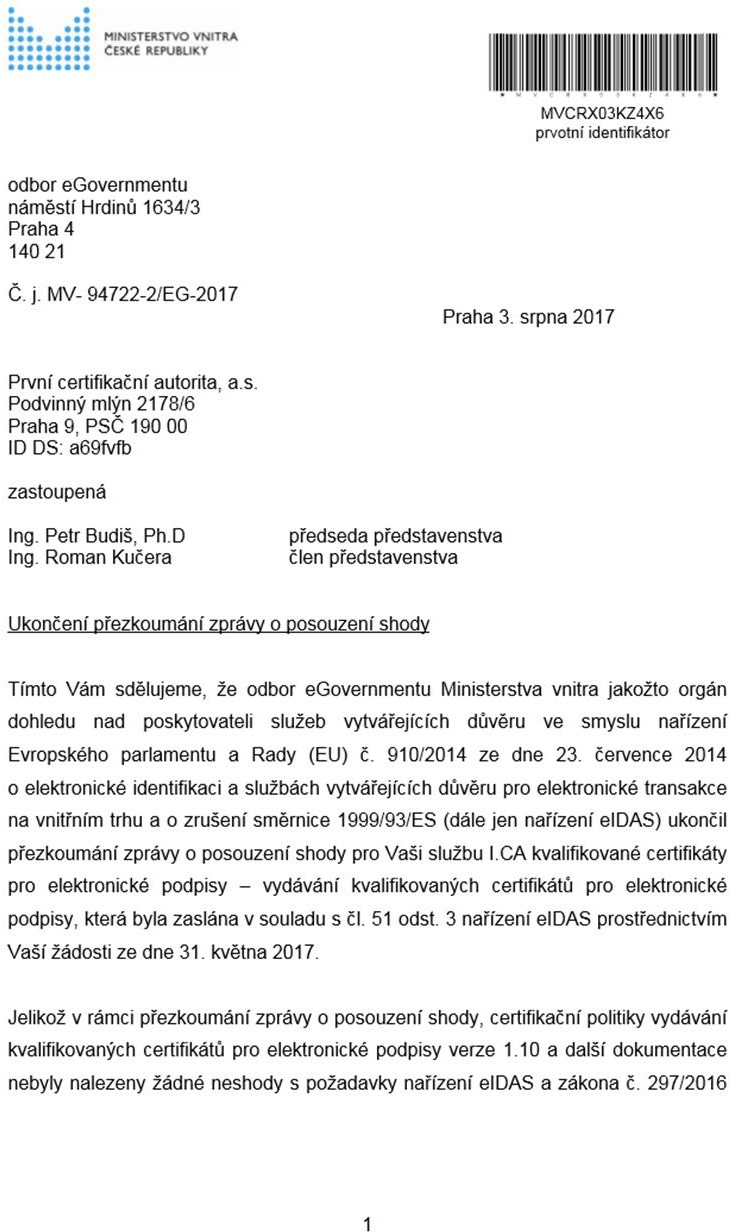
zjištěné nedostatky a požadovat v přiměřené lhůtě nápravu.

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

Provozovatel je povinen:

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

## Příloha č. 3 Doložení statutu kvalifikovaného dodavatele služeb vytvářejících důvěru



Sb., o službách vytvárejícich dúvèru pro elektronické transakce, nadále je První certifikační autoritê, a.s. pïiznán kvalifìkovanÿ status poskytovatele služeb vytváre¡icích dùvéru v souvisìosti s vydáváním kvalifikovanych certifikátù pro elektronické podpisy

Dékuji za spolupráci.

Ing. Roman Vrba

reditel

Vyiizuje: XXXXXX

tel. č.: XXXXXX

e-mail: XXXXXXXXXXX



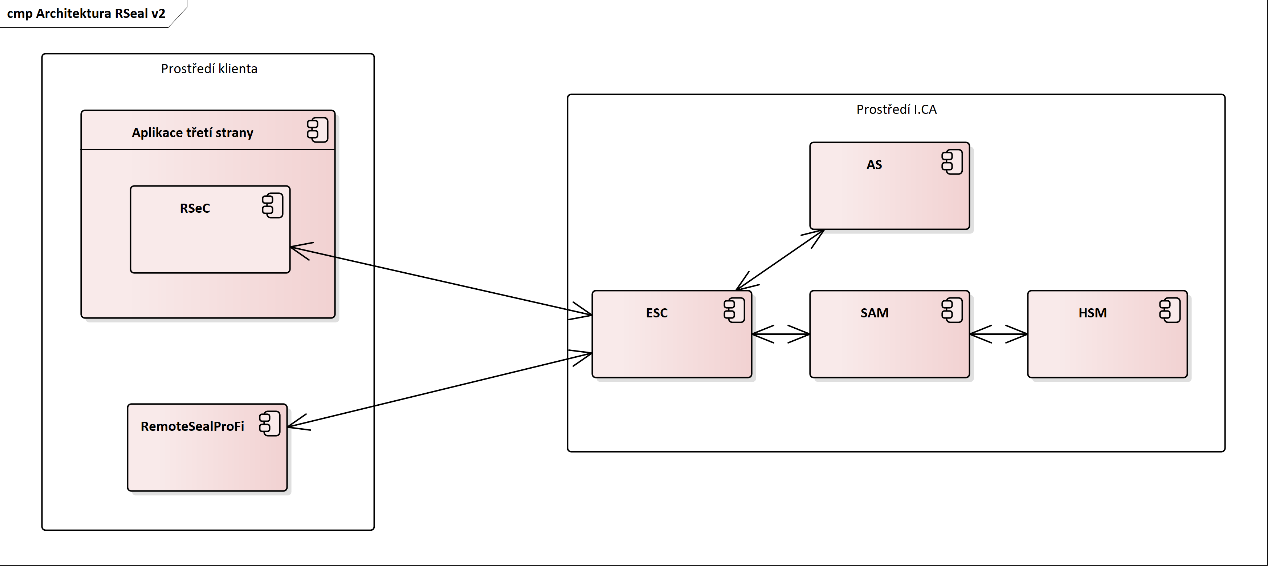
## Příloha č. 4 Popis služby vytváření kvalifikovaných elektronických pečetí na dálku

**Popis služby I.CA RemoteSeal**

## Co je služba I.CA RemoteSeal v2

Služba I.CA RemoteSeal v2 (dále už jen „RemoteSeal“ nebo „služba“) je služba vytváření kvalifikovaných elektronických pečetí na dálku. Služba umožňuje vygenerovat a držet data pro vytváření elektronických pečetí (tj. zejména privátní klíč) v QSealCD certifikovaném HSM zařízení ve správě I.CA a k němu pak zprostředkovat přístup pro účely vytváření kvalifikovaných elektronických pečetí. Klient (tj. právnická osoba) má k dispozici klientskou komponentu a příslušné autentizační markanty, pomocí kterých může dokument opatřit kvalifikovanou elektronickou pečetí. Samotný obsah dokumentu přitom neopouští klientskou komponentu, a tudíž ani prostředí klienta.

## Architektura



* **RSeC** (RemoteSeal Client) - klientská komponenta určená pro strojové pečetění dokumentů a pro integraci do spisové služby nebo jiného systému, který potřebuje autonomně vytvářet kvalifikované pečeti. Existuje ve vícero variantách pro snadnou integraci do různých systémů.
* **RemoteSealProFi** - klientská desktop aplikace pro Windows, která slouží ke správě pečetění dané organizace a ručnímu vytváření kvalifikovaných pečetí.
* **ESC** (Evolved Signature Core) - základní aplikační server provozovaný I.CA, přes který jdou veškeré komunikace týkající se pečetění z klientských komponent.
* **SAM** (Signature Activation Module) - povinná součást QSCD pro vzdálený podpis/pečeť, který zajišťuje kontrolu přístupu ke klíčům uloženým na HSM modulu
* **HSM** (Hardware Security Module) - povinná součást QSCD pro vzdálený

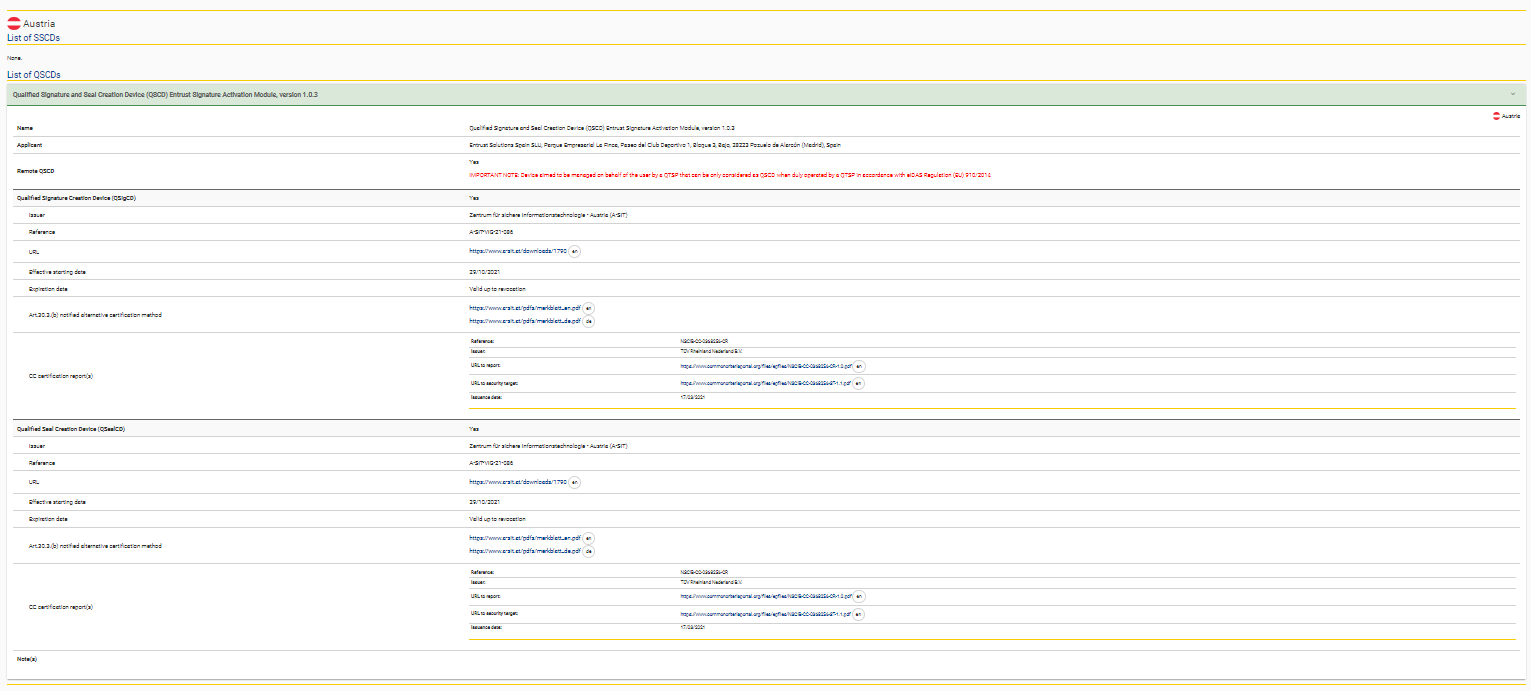
podpis/pečeť, která zajišťuje samotné bezpečné generování, uchovávání a používání privátních klíčů.

* **AS** (Authorization Server) - aplikační server, který zajišťuje ověření autentizace koncového uživatele (držitele klíče) a vytváření SAD (Signature Activation Data) tj. datové struktury autorizující použití příslušného privátního klíče pro podpis příslušných dat pro SAM.

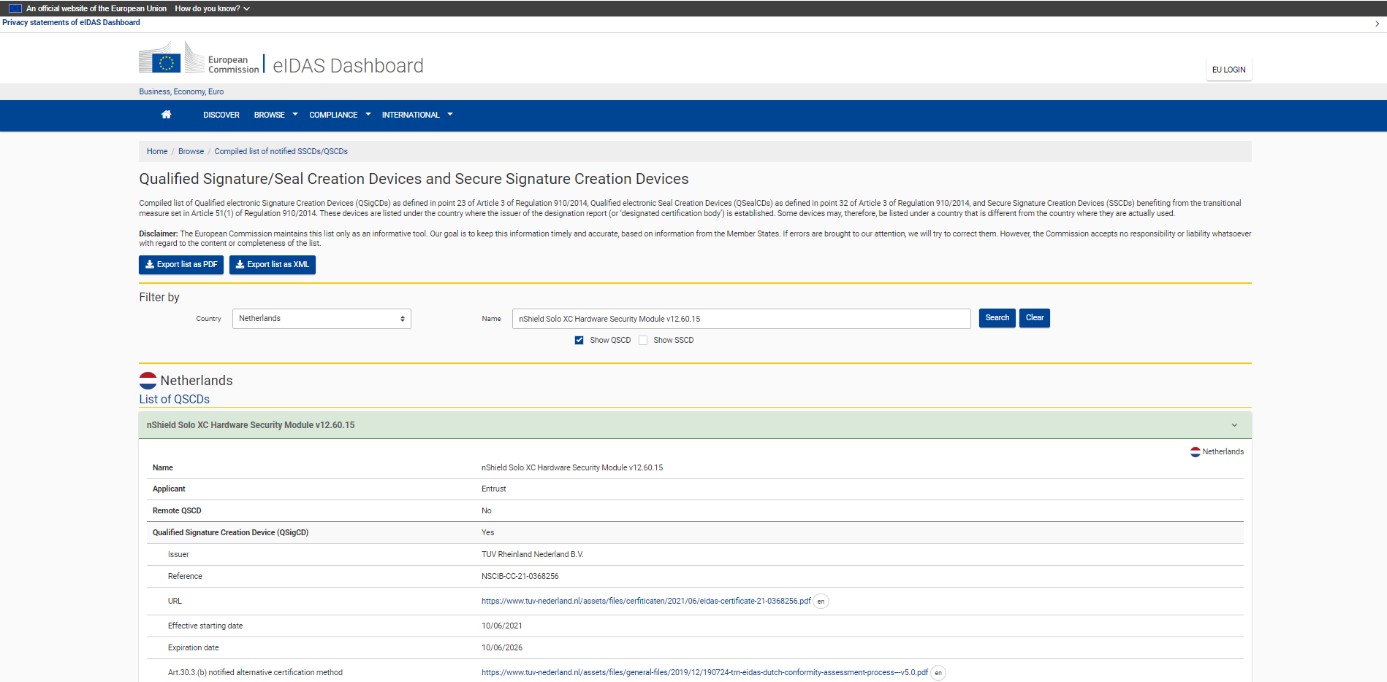
## Použité QSCD

Služba využívá certifikované Remote QSealCD skládající se ze:

* SAM modulu Entrust SAM https://eidas.ec.europa.eu/efda/browse/notification/qscd-sscd



* HSM modulu Entrust nShield Connect XC



Certificate eIDAS

Standard



Certificate

number Certificate holder TOE developer

Product and assurance level

Project number

REGULATION (EU) NO 910/2014 OF THE EUROPEAN PARLIAMENT AND OF

THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

CC-21-0368256•eIDAS

TÜV Rheinland Nederland B.V. certifies:

**Entrust**

Minneapolis1187 Park Place, Shakopee, MN 55379, USA

nCipher Security Limited (an Entrust company)

One Station Square, Cambridge CB1 2GA, UK

**nshield Solo XC Hardware Security Module** v12.60.15 Assurance Package:

* EAL4 augmented with AVA\_VAN.5 and ALC\_FLR.2

Protection Profite Conformance:

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

0368256

Evaluation faci!'+Y Brightsight BV located in Delft, the Netherlands

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

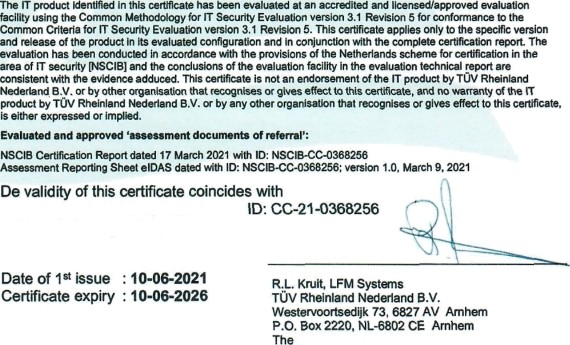


The Deslgnatad Body from The +,<.,a.»\* under Artlde 30{2) and 39(2) al Regulaùon 010/Z014 w.o> that:



slgnaturefseui v•«i'aata is hetd ln'an emmett but not aecesserily azcJus ety'user-munayö «imini«æm."‘“”"'

- The IT pfoduct meets tbe requlrements laid down in Annex ll of REGULATiON (EU) No 810/2014 of THE



the published NSClB-certificate with with the following validity-dates:

Netherlands

TÜVRheinland”

Precisely R ight.

## Varianty klientských komponent

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

dvou skupin:

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

## Klientské komponenty pro ruční pečetění uživatelem, tedy člověkem

Pro ruční pečetění člověkem - tj. zaměstnanci dané organizace existuje desktopová GUI aplikace pro Windows RemoteSealProFi, která umožňuje ručně vybrat

dokument/dokumenty a opatřit je kvalifikovanou elektronickou pečetí.

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

## Klientské komponenty pro automatizované/strojové pečetění

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

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

platformu:

* **jRSeC** (Linux i Windows) - nadstavba nad RSeC určená pro integraci do aplikací v

jazyce Java formou Java class library.

* **RSeC.NET** (Linux i Windows) - nadstavba nad RSeC určená pro integrací do aplikací v

jazyce .NET

* **RSeProxy** (Windows) - serverová aplikace určená pro instalaci do sítě klienta, která do vnitřní sítě klienta poskytuje SOAP webové služby pro funkcionalitu pečetění, přičemž vůči systému RemoteSeal vystupuje jako klientská komponenta RSeC.

## Zřízení služby

1. Prvním krokem je uzavření smlouvy mezi organizací a I.CA.
2. Oprávněná osoba žadatele (tj. organizace) dohodne se zástupcem I.CA způsob vydání osobního autentizačního komerčního certifikátu – obvykle navštíví pobočku RA v sídle společnosti I.CA s potřebnými doklady ke zřízení služby I.CA RemoteSeal na danou organizaci.
3. Operátor RA vydá oprávněné osobě osobní autentizační komerční certifikát na čipovou kartu Starcos 3.5 nebo 3.7. Tato osoba se tímto automaticky stává prvním (a v tento okamžik prozatím také jediným) správcem služby pečetění pro danou organizaci.
4. Operátor RA provede zřízení služby I.CA RemoteSeal vč. vydání kvalifikovaného pečetícího certifikátu (kvalifikovaný certifikát pro elektronickou pečeť) pro danou

organizaci, přičemž privátní klíč pro tento certifikát je generován a spravován QSCD zařízením služby I.CA RemoteSeal.

1. V rámci vydání pečetícího certifikátu oprávněná osoba žadatele podepisuje dokumentaci k vydání certifikátu, přičemž tyto mohou být podepsány:
   * klasicky vlastnoručním podpisem na papír, nebo
   * bezpapírově/elektronicky pomocí osobního autentizačního komerčního certifikátu oprávněné osoby (v tom případě žadatel podepisuje pouze smlouvu)
2. Oprávněná osoba žadatele odchází z RA s čipovou kartou s autentizačním komerčním certifikátem.

## Uživatelské účty RemoteSealProFi

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

Uživatelské účty jsou dvojího druhu:

* Přenosný uživatelský účet
* Fixní uživatelský účet

## Přenosný uživatelský účet

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

Pro autentizaci uživatele slouží:

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

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

*Aktivace přenosného uživatelského účtu*

Pro aktivaci přenosného uživatelského účtu je potřeba mít čipovou kartu s komerčním

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

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

aplikace.

Poznámka

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

## Fixní uživatelský účet

Fixní uživatelský účet je oproti tomu vázán na konkrétní PC, resp. na konkrétní uživatelský profil v OS Windows, na kterém proběhla aktivace a jinde se k němu není možné přihlásit. K přihlášení však nejsou potřeba žádné fyzické markanty, postačuje:

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

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

*Aktivace fixního uživatelského účtu*

Po zřízení nového fixního uživatelského účtu (správcem pečetění) obdrží uživatel tzv.

aktivační mail, který v příloze obsahuje tzv. aktivační soubor. Tento slouží pro provedení aktivace následovně:

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

aplikace.

## Uživatelské role RemoteSealProFi

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

## správce pečetění

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

## běžný uživatel

* + - Nemá přístup do administrátorské sekce RemoteSealProFi.
    - Může libovolně vytvářet kvalifikované elektronické pečetě.

## Aktivace RSeC

Komponenta RSeC pro autentizaci vůči systému RemoteSeal vyžaduje:

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

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

dvojici přístupový soubor + heslo.

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

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

Do komponenty RSeC se pak přístupový soubor a heslo předávají přes API příslušné knihovny

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

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

přístupového souboru ani hesla.

## Opečetění dokumentu

**Opečetění dokumentu přes RSeC**

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

## Opečetění dokumentu přes RemoteSealProFi

1. Uživatel se přihlásí do aplikace RemoteSealProFi
2. Uživatel vybere "profil pečetě" podle kterého chce pečetit

– profil pečetě jsou de-facto uložené parametry vytvářené pečetě (viditelný podpis, vložení časového razítka, atp), které mohou sloužit jako fixně

předepsané parametry pro druh dokumentu (např.: všechna potvrzení o

studiu mají stejné parametry) - jako základní nastavení parametrů, které jsou pro daný případ uživatele následně upraveny a je možné je sdílet s dalšími uživateli pod stejným pečetícím accountem.

1. Volitelně uživatel upraví parametry pečetě
2. Následně uživatel vybere dokumenty, které se mají opečetit a potvrdí
3. RemoteSealProFi postupně opečetí všechny vybrané dokumenty

## Obnova pečetícího certifikátu

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

pečetícího certifikátu. Správce pečetění:

1. Se přihlásí do aplikace RemoteSealProFi a otevře administrátorskou část aplikace => správa pečetícího certifikátu
2. Stiskne tlačítko obnovit certifikát
3. Aplikace zajistí vytvoření žádosti o následný certifikát a zobrazí uživateli detail servisní transakce k podpisu žádosti o vydání následného certifikátu
4. Uživatel stiskne tlačítko podepsat a zadá své heslo k uživatelskému účtu ke službě

RemoteSeal

1. Služba následně zajistí vydání následného pečetícího certifikátu a po jeho vydání naplánuje odložené nasazení nově vydaného pečetícího certifikátu (za + 15 dní)
2. Správce pečetění si může po vydání certifikátu v aplikaci zobrazit informace o novém certifikátu, uložit si nový certifikát do souboru, vidět přesný čas plánovaného nasazení nového certifikátu a tento čas může v aplikace také změnit.

## Podporované formáty podpisu

* + **CAdES**
    - CAdES-B-B, CAdES-B-T
    - Dle normy EN 319 122, ve variantách:
      * Interní
      * Externí

## PAdES

* + - PAdES-B-B, PAdES-B-T
    - Dle normy EN 319 142, ve variantách:
      * Neviditelný
      * Viditelný – Text/Obrázek/Text+Obrázek + volitelně obrázek na pozadí

## XAdES

* + - XAdES-B a XAdES-T
    - XAdES Enveloping podle TS 103 171
    - XAdES Detached podle TS 103 171
    - XAdES DetachedExtern podle TS 103 171
    - XAdES Enveloped podle EN 319 132
    - XAdES Enveloping podle EN 319 132
    - XAdES Detached podle EN 319 132
    - XAdES DetachedExtern podle EN 319 132

## ASiC-E XAdES

* + - ASiC-E XAdES-B a ASiC-E XAdES-T
    - Dle normy ETSI TS 103 174, přičemž:
      * Je možné opečetit právě jeden datový objekt právě jednou kvalifikovanou pečetí
      * Není podporováno rozšíření stávajícího ASiC-E souboru o další pečeť/podpis, ani několik podpisů/pečetí v rámci jednoho ASiC-E souboru.
      * Pro soubory typu .txt, .pdf, .xml, .png je implicitně doplněn příslušný mimetype odpovídající dané příponě. Tuto implicitní volbu je možné v rozhraní explicitně přenastavit na jiný mimetype, popř. lze explicitní

cestou nastavit mimetype pro ostatní (implicitně nepodporované) typy datových objektů.

* + - * Samotná XAdES pečeť uvnitř ASiC-E kontejneru obsahuje pouze minimální nezbytně nutnou množinu podepisovaných a nepodepisovaných properties vyžadovanou danou ETSI normou.

## Doplňkové zabezpečení zdroje komunikace

Pro jednotlivé pečetící accounty je možné nastavit doplňkové zabezpečení zdroje

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

## 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:

* 1. 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;
  2. stanoví pravidla pro služby vytvářející důvěru;
  3. 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 Digitální a informační agenturou jako gesčním orgánem pro oblast eIDAS v ČR.

Příslušný certifikát I.CA:

Certifikát č.: PCEB 23/05/05

**tayIIorcox.com**

ensure your certification

**Certifikát**

Certifikační orgán TAYLLORCOX PCEB,

zčízenÿ společností TAYLLORCOX s.r.o., institutem pro auditování, kontrolu a testování, udèluje tento certifikát společnosti

První certifikační autorita, a.s.

IČ: 264 39 395

Podvinnÿ mlÿn 2178/6

CZ 190 00, Praha 9 - Libeñ, Czech Republic

potvrzující, že kvalifikovaná sluźba vyNáčejîcí duvéru

QVerify, verze 1.1

pro ovéfování platnosti kvalifikovanÿch elektronickÿch podpisu a kvalifikovanÿch elektronickÿch pečetí je v souladu s:

Načízením Evropského Parlamentu a Rady (EU) č. 910/2014, článkem 5, článkem 13, článkem 15, článkem

19, článkem 24, článkem 32, článkem 33 a ćlánkem 40.

Tento certifikát je vydáván v souladu s požadavky certifikačního schématu definovaného normou ČSN ETSI EN 319 403-1 v2.3.1 ve spojení s DKP verze 4.

Datum certifikace:

Certifikát platí do:

I - • ‘ ! ’ ”

Ing. Radek Nedvèd

Reditel certifikačního orgänu

26.05.2023

25.05.2025



V 3239

Podle eIDAS zveřejňuje Digitální a informační agentura seznam kvalifikovaných poskytovatelů a kvalifikovaných služeb vytvářejících důvěru na webové stránce:

https://[www.dia.gov.cz/egovernment/eidas-sluzby-vytvarejici-duveru-a-elektronicka-](http://www.dia.gov.cz/egovernment/eidas-sluzby-vytvarejici-duveru-a-elektronicka-) identifikace/povinne-zverejnovane-informace/seznam-kvalifikovanych-poskytovatelu-sluzeb- vytvarejicich-duveru-a-poskytovanych-kvalifikovanych-sluzeb-vytvarejicich-duveru/



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-LT1. 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.

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

Podrobný popis:

Služba podporuje ověření dokumentu ve standardních a legislativně podporovaných formátech:

* XAdES dle ETSI TS 103 171 v úrovni shody B, T a LT,
* PAdES dle ETSI TS 103 172 v úrovni shody B, T, LT **a LTA**,
* CAdES dle ETSI TS 103 173 v úrovni shody B, T a LT,
* CAdES dle ETSI EN 319 122-1 v úrovni shody B-B, B-T, B-LT a B-LTA,
* XAdES dle ETSI EN 319 132-1 v úrovni shody B-B, B-T a B-LT,
* PAdES dle ETSI EN 319 142-1 v úrovni shody B-B, B-T, B-LT a B-LTA,
* ASiC-E CAdES dle ETSI TS 103 174 v úrovni shody B, T a LT,
* ASiC-E XAdES dle ETSI TS 103 174 v úrovni shody B, T a LT,
* ASiC-S with CAdES dle ETSI TS 103 174 v úrovni shody B, T a LT,
* ASiC-S with XAdES dle ETSI TS 103 174 v úrovni shody B, T a LT,
* ASiC-S with CAdES dle ETSI EN 319 162 v úrovni shody B-B, B-T a B-LT,
* ASiC-S with XAdES dle ETSI EN 319 162 v úrovni shody 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 vybrat2, 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.

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

2 Lze ponechat jako parametrické či definovat jednu z možností.

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.

1. Provedení vstupních kontrol
2. Provedení ověření jednotlivých podpisů (tj. dvojic podpisová struktura + hash)
3. Sestavení odpovědi s výsledkem ověření - XML elektronicky podepsaná datová struktura (zasílaná on-line)
4. Uložení dat pro následné generování PDF protokolu s výsledkem ověření v prostředí

I.CA

1. Předání výsledku ověření v XML struktuře aplikaci klienta
2. Zalogování procesu ověření
3. Záznam do STAT o využití služby
4. 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:

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

## Omezující podmínky:

* 1. 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.
  2. Ověřovány jsou podpisy založené na certifikátech vydaných všemi důvěryhodnými poskytovateli zemí EU (EUTL, LoTL).
  3. 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.
  4. Časová razítka jsou vydávána časovou autoritou I.CA.

4 Viz příklad v příloze.

Podporované platformy - klientská komponenta.

Klientská komponenta jde 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.

Dostupnost:

* Služba je poskytována v režimu 24/7 s SLA až 99,95% a kapacitou až 500 ověření za

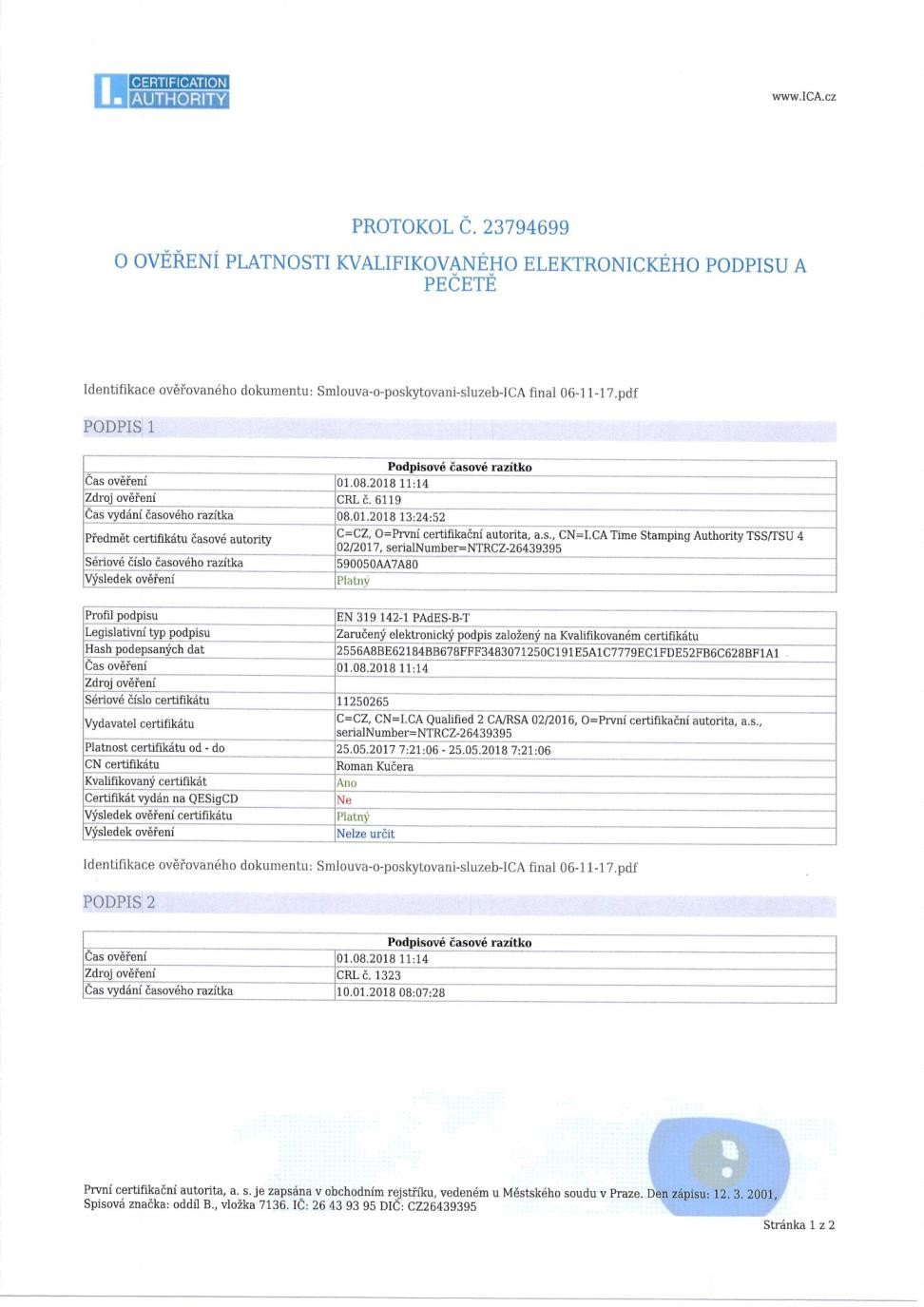
minutu.

Příklad xml protokolu:



protocol.xml

Příklad PDF protokolu:



**Příloha č. 6**

**Podmínky zpracování osobních údajů**

# ZPŮSOB, ROZSAH A DOBA ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

* + - 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:
         1. jméno nebo jména,
         2. příjmení,
         3. titul (před i za jménem),
         4. údaje o adrese trvalého pobytu
         5. datum narození,
         6. rodné číslo,
         7. e-mailová adresa,
         8. číslo primárního a sekundárního osobního dokladu,
         9. název zaměstnavatele,
         10. identifikátor klienta Ministerstva práce a sociálních věcí.
      2. Osobní údaje uvedené výše v odst. 1.1 je Zpracovatel oprávněn zpracovávat zejména za účelem:
         1. obsluhy Subjektu údajů jako zákazníka/klienta Správce při provozu Registrační autority sloužící k vydávání kvalifikovaných a komerčních certifikátů,
         2. uzavírání smluvních vztahů o vydání a používání certifikátu se zákazníky/klienty,
         3. vyřizování návrhů na změnu a zánik smluvních vztahů uvedených v písm. b)

tohoto odst.

* + - 1. 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. Osobní údaje Subjektů údajů je Zpracovatel oprávněn zpracovávat nejdéle po dobu trvání této smlouvy.

# PRÁVA A POVINNOSTI STRAN

* + - 1. Zpracovatel se zavazuje zpracovávat Osobní údaje poskytnuté Subjektem údajů

v souladu s touto smlouvou a výlučně k výše uvedenému Účelu.

* + - 1. 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. 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.
      3. 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.
      4. 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.
      5. 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.
      6. Správce je oprávněn uveřejnit nebo jinak sdělit svým klientům, a to formou dle uvážení Správce, že se Zpracovatel podílí na zpracování Osobních údajů, s nimiž Správce nakládá, a za jakým účelem.
      7. Zpracování Osobních údajů Zpracovatelem a jejich ochrana podle této smlouvy probíhá bez nároku Zpracovatele na zvláštní odměnu.
      8. 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.
      9. 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: XXXXXXXXXX

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.

* + - 1. 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. 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.
      3. 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.

# ZÁRUKY TECHNICKÉHO A ORGANIZAČNÍHO ZABEZPEČENÍ OCHRANY OSOBNÍCH ÚDAJŮ

* + - 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.
      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. 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.
      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.
      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.
      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.
      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.

* + - 1. 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.
      2. 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. 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.

# NÁHRADA ŠKODY

* + - 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.

# TRVÁNÍ SMLOUVY A LIKVIDACE DAT

* + - 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.
      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.
      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.
      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.

**Příloha č. 7 Popis služby vytváření kvalifikovaných elektronických podpisů na dálku**

# LEGISLATIVNÍ PODKLADY KE SLUŽBĚ

Využívání tzv. elektronického podepisování na dálku má oporu v legislativě EU Nařízení

910/2014 eIDAS:

1. *Podepisující osoba by měla mít možnost svěřit kvalifikované prostředky pro vytváření elektronických podpisů do péče třetí straně, pokud jsou zavedeny odpovídající mechanismy a postupy, které zajišťují, že podepisující osoba má výhradní kontrolu nad používáním svých dat pro vytváření elektronických podpisů, a použitím tohoto prostředku jsou splněny požadavky na kvalifikovaný elektronický podpis.*
2. *Vytváření elektronického podpisu na dálku, jehož prostředí spravuje poskytovatel služeb vytvářejících důvěru jménem podepisující osoby, přináší mnohé ekonomické výhody, a bude tedy pravděpodobně stále častější. Aby však bylo zajištěno, že tyto elektronické podpisy budou z právního hlediska uznávány stejně jako elektronické podpisy, které jsou vytvářeny v prostředí spravovaném výlučně uživatelem, měli by poskytovatelé nabízející služby elektronického podpisu na dálku uplatňovat zvláštní postupy pro zajištění bezpečnosti v oblasti řízení a správy a používat důvěryhodné systémy a produkty zahrnující zabezpečené kanály pro elektronickou komunikaci, a zajistit tak spolehlivost prostředí, v němž jsou elektronické podpisy vytvářeny, a zaručit, že je toto prostředí používáno pod výlučnou kontrolou podepisující osoby. V případě kvalifikovaného elektronického podpisu vytvořeného pomocí prostředku pro vytváření elektronických podpisů na dálku by se měly použít požadavky stanovené v tomto nařízení, které jsou použitelné na kvalifikované poskytovatele služeb vytvářejících důvěru.*

# VÝCHODISKO SLUŽBY

V současnosti se objevuje stále více požadavků na opatřování dokumentů a dat kvalifikovaným elektronickým podpisem, který je jako jediný ekvivalentem vlastnoručního podpisu. Pro jeho vytváření je nezbytné, aby měl uživatel, podepisující osoba, k dispozici bezpečné zařízení, tzv. kvalifikovaný prostředek pro vytváření elektronického podpisu (QESCD). Standardně je tento požadavek zajištěn prostřednictvím certifikované čipové karty nebo USB tokenu.

Dnes se často využívají zařízení, která neumožňují připojení čipové karty (mobilní zařízení, ultrabooky apod.) Pro takové případy, kde využití čipové karty není vhodné nebo možné, nabízí I.CA řešení pomocí elektronického podepisování na dálku.

V rámci tohoto řešení uživatel nevlastní kvalifikovaný prostředek pro vytváření elektronického podpisu, ale využívá vzdálený přístup k certifikovanému bezpečnému zařízení, které je spravováno poskytovatelem služeb vytvářejících důvěru v souladu s požadavky Nařízení EU 910/2014 - eIDAS.Služba

# STRUČNÝ POPIS SLUŽBY

Služba I.CA RemoteSign umožňuje vytváření kvalifikovaného elektronického podpisu na mobilních zařízeních (mobilní telefony, tablety) nebo prostřednictví PC aplikace instalované

na počítači uživatele služby.

Uživatel má k dispozici aktivovanou mobilní nebo PC aplikaci, kterou využívá pro přijímání požadavků a vytváření kvalifikovaného elektronického podpisu. V současnosti jsou v rámci služby podporována mobilní zařízení s operačním systémem Android nebo iOS a pro PC aplikaci je to operační systém Windows.

## Uzavření smlouvy na obchodním místě I.CA

Uzavření smlouvy probíhá na obchodním místě I.CA nebo u poskytovatelů služeb, kteří provozují registrační autority pro službu I.CA RemoteSign. Zde je provedeno ověření totožnosti uživatele a jeho registrace. Při zřizování služby je na registrační autoritě potřeba určit, zda bude využita mobilní či PC varianta aplikace. Podle toho obdrží uživatel buď aktivační obálku, nebo mu I.CA odešle na email aktivační soubor pro PC aplikaci. Aktivační obálka obsahuje aktivační kód pro mobilní aplikaci, aktivační email obsahuje aktivační kód pro PC aplikaci.

## Aktivace mobilní aplikace I.CA RemoteSign

Dle používané platformy si uživatel z AppStore/AndroidMarket stáhne aplikaci I.CA RemoteSign, která je zde volně k dispozici. Po jejím prvním spuštění je vyžadována její aktivace a nastavení hesla ke klíči. K tomu uživatel použije získanou aktivační obálku a po zvolení vlastního hesla ke klíči je služba okamžitě aktivní.

## Aktivace další mobilní aplikace

Přístup k certifikátu nemusí být omezen na jedno zařízení. Aplikace umožňuje přidání dalšího zařízení prostřednictvím volby „Přidat nové zařízení“. Nové zařízení aktivuje pomocí QR kódu, který se zobrazí v procesu přidání nového zařízení. Obě aktivní zařízení v systému I.CA RemoteSign mají vždy stejná oprávnění a využívají shodný podpisový certifikát. Požadavky k podpisu jsou vždy k dispozici na obou aktivních zařízeních.

Aktivovaná zařízení může uživatel také zablokovat, popř. trvale zrušit.

## Aktivace PC aplikace I.CA RemoteSign

Uživatel spustí nainstalovanou PC aplikaci a spustí proces aktivace. V průběhu procesu

uživatel vloží aktivační kód, který obdrží emailem, zvolí si heslo, kterým se bude do aplikace přihlašovat a zároveň tímto heslem bude potvrzovat podepsání jednotlivých transakcí.

Aktivaci potvrdí přepsáním kódu z obdržené SMS zprávy.

## Vztah mobilní a PC aplikace

Z aktivované PC aplikace lze přidat, aktivovat aplikaci na mobilním zařízení. Opačný postup nyní není možný. Jeden uživatel může mít aktivovanou jen jednu PC aplikaci

Při zřizování služby je na registrační autoritě potřeba určit, zda bude využita mobilní či

desktopová varianta aplikace, podle toho dostane uživatel buď aktivační obálku, nebo mu na email přijde aktivační soubor.

## Vlastnosti PC aplikace

Aplikace podporuje operační systémy Windows 7 a novější, využívá .Net Framework 4.8, který je součástí Windows 10 od verze 1903. Na starších verzích operačního systému je

potřeba jej doinstalovat. Uživatelská data, která aplikace používá, jsou bezpečně uložena v souboru, který je zašifrován privátním klíčem, jenž je uložen na serverech I.CA. Přístup k

tomuto klíči je umožněn pouze skrze privátní klíč, který je vygenerován při aktivaci aplikace

na straně klienta. Přístupový privátní klíč se generuje do úložiště certifikátů ve Windows a je

označen jako neexportovatelný, tj. nedá se zálohovat. Data aplikace tedy není možné nijak zálohovat či přesunout na jiné PC. Každý uživatel může mít aktivovanou pouze jednu verzi PC aplikace.



## Podepisování dokumentů

Podepsání dokumentu proběhne tak, že Poskytovatel služeb vytvoří nový požadavek k podpisu a vloží ho do systému I.CA RemoteSign. I.CA následně odešle notifikaci o novém požadavku k podpisu příslušnému uživateli do mobilní aplikace. Poté je postup pro podpis shodný jak pro mobilní, tak pro PC aplikaci. Uživatel se jednoduše do aplikace přihlásí, zkontroluje dokument k podpisu a podepíše jej zadáním hesla ke klíči.

Podepsaný požadavek je předán zpět poskytovateli služeb, který požadavek do systému vložil. Poskytovatel služeb si podepsaný požadavek převezme k dalšímu zpracování. Může jej například opatřit svým vlastním elektronickým podpisem nebo pečetí. Také může do dokumentu vložit časové razítko, a tak vznikne elektronicky podepsaný dokument, který je roven písemně podepsanému dokumentu.

# TECHNICKÉ ŘEŠENÍ SLUŽBY

Poskytovatel služeb vkládá požadavky do služby I.CA RemoteSign prostřednictvím komponenty RSiCon, která je integrována v jeho interním systému. Takto je založen nový požadavek k podpisu. Na jeho základě dojde v komponentě RSiCon k realizaci procesů nutných pro realizaci podpisu (výpočet hash, vytvoření náhledu dokumentu atd.)

Komponenta RSiCon zašle požadavek, obsahující potřebné informace, serveru I.CA

RemoteSign. Server vrací informaci o úspěšném založení požadavku spolu s daty, které je nutné uchovat do okamžiku ukončení podepisovací transakce. Data předávaná do systému I.CA RemoteSign neobsahují obsah podepisovaného dokumentu. Stejně tak vygenerovaný náhled dokumentu v PDF formátu nebo odkaz na stažení podepisovaných dat jsou předávány v zašifrované podobě. K jejich dešifrování může dojít vždy pouze na koncovém zařízení podepisujícího uživatele.

Po úspěšném založení požadavku k podpisu, I.CA kontaktuje jednotlivá aktivní zařízení daného uživatele formou push notifikace. Po otevření push notifikace dojde k otevření mobilní aplikace I.CA RemoteSign.

Po autentizaci uživatele (heslem případně biometricky) se zobrazí seznam čekajících požadavků k podpisu. Uživatel si může u jednotlivých dokumentů zobrazit detailní informace. Každý dokument je možné podepsat či odmítnout.

Každý požadavek má definovanou platnost, což je časový údaj definovaný providerem služeb. Po jeho uplynutí požadavek k podpisu expiruje a uživatel jej nemá možnost podepsat.

Pokud se uživatel rozhodne požadavek podepsat, je vyzván k zadání hesla pro podpis na dálku. Tím se zahájí kryptografická komunikace mezi mobilní aplikací a systémem I.CA RemoteSign. Je-li heslo správné, vytvoří se kvalifikovaný elektronický podpis hash podepisovaných dat. Služba I.CA RemoteSign podporuje vytváření elektronických podpisů typů PAdES-B-B a PAdES- B-T dle EN 319 142-1 nebo CAdES-B-B a CAdES-B-T dle EN 319 122-1.

Po vytvoření podpisu dochází k tzv. notifikaci systému Poskytovatele služeb, který je touto cestou informován o změně stavu podpisové transakce. Na základě této notifikace systém providera služeb zavolá prostřednictvím komponenty RSiCon systém I.CA RemoteSign. Dojde ke stažení „jádra podpisu“ do systému providera služeb a následnému sestavení kompletního podepsaného dokumentu. Podepsaný dokument je následně vrácen volajícímu systému providera služeb a je možné s ním nakládat jako s jakýmkoliv jiným elektronicky podepsaným dokumentem.

## Komponenta RSiCon

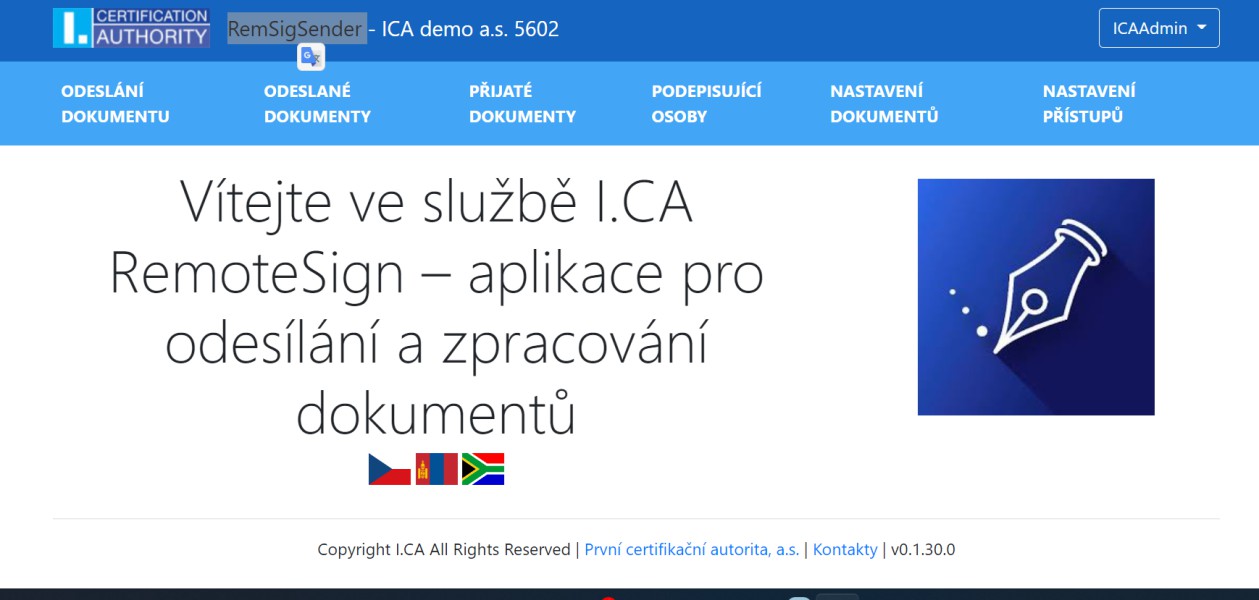
Komponenta RSiCon je určena pro komunikaci Poskytovatele služeb se systémem I.CA RemoteSign. Je realizována formou nativní knihovny pro Windows nebo Linux, nad níž poskytujeme wrapper ve formě .NET assembly nebo JAR knihovny pro snazší integraci do systémů service providera.

Možná je také realizace samostatné serverové aplikace, která bude umístěna v prostředí providera služeb. Tato aplikace bude obsahovat nativní jádro RSiCon, jeho funkcionality bude poskytovat dalším systémům prostřednictvím SOAP, popř. REST rozhraní.

## Aplikace RemSigSender

Pro Poskytovatele služeb, kteří nemohou nebo nechtějí integrovat Komponentu RSiCon do svého systému je určena intranetová aplikace pro snadné zasílání dokumentů vybraným Uživatelům k podpisu. Je provozovaná v síti Poskytovatele služeb, jednotliví operátoři do ní přistupují prostřednictvím internetového prohlížeče. Doporučená verze serveru je MS Windows Server 2019 Standard. Hardwarové požadavky jsou závislé na předpokládaném objemu dokumentů, minimálně x64 procesor, 4GB RAM, diskový prostor pro databázi 200GB na SSD disku. Aplikace používá databázi, pro běžný objem dokumentů stačí bezplatná verze MS SQL Express nainstalovaná přímo na serveru společně s aplikací. Pro provoz je nutný

přístup do internetu (ke službě I.CA RemoteSign) s nastavenými prostupy pro notifikace. Pro autentizaci operátorů je možno použít prostředky operačního systému (ActiveDirectory) nebo udržovat seznam operátorů přímo v aplikaci. Aplikace je k dispozici v české, anglické a slovenské jazykové verzi.



## RemoteSign Server – správa identit, prodloužení služby

Jeden uživatel představuje vždy jednu identitu v rámci systému, kterému odpovídá příslušná aktivační obálka. Během procesu aktivace dochází k vygenerování prvního párů klíčů pro danou identitu a vydání prvotního kvalifikovaného certifikátu.

Žadatel odchází z kontaktního místa s aktivační obálkou, která (jako jediná) obsahuje potřebné

„tajemství“ pro zpřístupnění práce s privátním klíčem k němuž byl vydán příslušný kvalifikovaný certifikát.

Prodloužení služby, tj. vydání následného kvalifikovaného certifikátu je autonomní proces systému I.CA RemoteSign, který (vyjma potvrzení servisního požadavku prodloužení služby) nevyžaduje žádnou akci od providera služeb ani koncového uživatele.

I.CA RemoteSign zajistí vytvoření žádosti o vydání následného certifikátu, která je zaslána do zařízení uživatele formou servisní transakce – prodloužení služby. Podpis této transakce probíhá de-facto standardním způsobem, přičemž výsledkem je žádost o následný kvalifikovaný certifikát. Vydaný následný certifikát je vložen do systému RemoteSign a od tohoto okamžiku I.CA RemoteSign zahájí jeho využívání.

# HLAVNÍ VÝHODY SLUŽBY

Mezi hlavní výhody této služby patří:

* Uživatel nepotřebuje žádný dodatečný hardware pro vytváření elektronického podpisu (čtečku, či čipovou kartu), stačí mu mobilní telefon případně počítač.
* Výsledkem podepisování je elektronický podpis s nejvyšší mírou záruky, tzv. kvalifikovaný elektronický podpis.
* Uživatel může vytvářet elektronický podpis pomocí více mobilních zařízení
* Obnovu certifikátu zařídí I.CA. Uživatel pouze odsouhlasí požadavek dalšího využívání služby.

**Příloha 8: Bližší specifikace plnění**

**Druhy vydávaných certifikátů**

**Kvalifikovaný certifikát pro elektronický podpis**

Kvalifikovaný certifikát pro elektronický podpis splňuje všechny požadavky stanovené legislativou, zejména nařízením Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (dále též „eIDAS“).

Kvalifikovaný certifikát pro elektronický podpis a s ním svázaný soukromý klíč (data pro vytváření elektronického podpisu) lze použít k vytváření a ověřování elektronických podpisů. Použití kvalifikovaného certifikátu pro elektronický podpis pro další úkony, jako například šifrování přenášených zpráv, je omezeno legislativou. Proto První certifikační autorita, a.s., nabízí i produkt TWINS (pár kvalifikovaného a komerčního certifikátu), jehož součástí je i komerční certifikát.

## Komerční certifikát

Komerční certifikáty mají svou významnou úlohu především tam, kde nelze s ohledem na platnou legislativu využít kvalifikované certifikáty. V současné době mají komerční certifikáty použití zejména pro šifrování a autentizaci. Jedná se především o neanonymní přístup na webové servery, autentizaci do informačních systémů a předávání šifrovaných dat.

## Twins

Tento produkt je kombinací kvalifikovaného a komerčního certifikátu. Jeho cílem je poskytnout zákazníkovi možnost využít jak služby elektronického podpisu, tak i služby autentizace a šifrování v souladu s platnou legislativou a technickými standardy. Oba certifikáty jsou vydány v rámci jednoho procesu a spravovány jako pár certifikátů, čímž se zjednodušuje jak prvotní vydání, tak následná správa certifikátů uživatelem.

## Systémový certifikát, kvalifikovaný certifikát pro elektronickou pečeť

Systémové certifikáty I.CA jsou certifikáty, které byly vydávány v souladu se zákonem č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů. Tyto certifikáty a s nimi svázané klíče jsou určeny k bezpečnému vytváření a ověřování elektronických značek. Vzhledem ke změně legislativy (zákon č. 297/2016 Sb.) jsou tyto certifikáty nahrazovány kvalifikovanými certifikáty pro elektronickou pečeť vydávanými v souladu s eIDAS.

## Komerční (technologický) serverový certifikát, SSL certifikát

Pro zajištění bezpečnosti především webových serverů, ale též např. vzájemné komunikace serverů, vydává I.CA komerční (technologické) serverové certifikáty. Tyto certifikáty jsou vydávány jak fyzickým, tak i právnickým osobám.

Zvláštní skupinou serverových certifikátů jsou SSL/TLS certifikáty pro důvěryhodné ověření domény.

## Vydání nových prvotních certifikátů

Nové prvotní certifikáty bude možné vydávat buď na klientské registrační autoritě (stacionární v sídle zadavatele či mobilní na notebooku) obsluhované zaměstnanci zadavatele, nebo v případech, kdy nebude využití klientské registrační autority praktické, je možné prvotní certifikáty získat na registračních autoritách I.CA, případně je možné zajistit výjezd operátora I.CA na smluvené místo.

## Obnova certifikátů u stávajících uživatelů

Navrhované řešení předpokládá u stávajících držitelů certifikátů plně elektronické vydání následných certifikátů bez nutnosti dostavovat se na registrační autoritu či realizovat výjezd. Pro uložení certifikátů a příslušných soukromých klíčů bude možné využít stávající hardware v majetku zadavatele.

## Kvalifikované prostředky pro vytváření elektronických podpisů



K uložení certifikátů a příslušných soukromých klíčů nabízí I.CA dlouhodobě ověřené a spolehlivě fungující čipové karty (v textu též „karty“) Starcos renomované firmy Giesecke&Devrient ve spojení s USB čtečkami ve formě tokenů ACR40T-A6. Jedná se o stejný hardware, který je v SPÚ v současné době již využíván a nehrozí tedy problémy s kompatibilitou ve stávajících řešeních.

Dodávaná čipová karta Starcos 3.7 splňuje požadavky na kvalifikované prostředky pro vytváření elektronických podpisů definované nařízením 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 (eIDAS).

Oddělení čipu od čtečky (tokenu) má výhodu, že v případě nutnosti výměny čipu (např. z důvodu blokace karty při opakovaném zadaní špatného PIN) je možné vyměnit pouze kartu a token nadále využívat.

Certifikát uložený na čipové kartě je možné používat na jakémkoli PC v síti úřadu, kde je nainstalován ovládací SW SecureStore (viz níže). Po vložení čipové karty proběhne automatická instalace ovladače a registrace certifikátu do operačního systému, a po cca 15 s je možné certifikát používat.

Při vydávání certifikátu je soukromý klíč generován přímo čipem karty a nelze jej exportovat. Přístup k soukromému klíči (datům pro vytváření elektronického podpisu) je chráněn PINem.

Při vydávání certifikátu detekuje software registrační autority, zda byla žádost a s ní i příslušný soukromý klíč generován čipovou kartou Starcos 3.7 a pokud ano, zajistí, aby byl do rozšiřujících položek certifikátu vložen QCStatement s naplněním id-tsi-qcs-QcSSCD (OID 0.4.0.1862.1.4).

Dále je I.CA schopna zajistit mazání certifikátů uložených na kartě po uplynutí smluvené doby. Na základě specifikace ve výzvě bude tato doba nastavena na 400 dní.

U čipů i tokenů garantuje I.CA životnost po dobu 4 let s garanci bezplatné výměny a splnění všech zákonných požadavků pro kvalifikovaný prostředek pro vytváření elektronických podpisů minimálně po dobu platnosti smlouvy.

## Technologická specifikace čipové karty/čipu Starcos 3.7

* Paměťová kapacita karty je využívána dynamicky, což umožňuje na kartu uložit variabilní počet klíčů, certifikátů a ostatních dat ve volné části. V části určené pro kvalifikované certifikáty je prostor pro následující počet klíčů uvedených parametrů:
  + **4x RSA 2048bit**
  + **2x RSA 4096bit**
  + **4x ECC NIST P-384**
* Na kartě je možné zvolit podporované (důvěryhodné) Certifikační autority, jejichž klientské certifikáty může klient využívat. Jiné klientské certifikáty pak není možné na kartu umístit, čímž se významně omezuje možnost použití karty k nepovoleným operacím. Pro kartu Starcos 3.7 je použita nová koncepce ukládání ROOT certifikátů CA – na kartě bude realizováno tzv. rozšířené úložiště CA certifikátů.
* Bezpečnostně citlivé operace je na kartě možné vždy realizovat pouze po zadání PIN, jehož délka je **6 – 8 míst**. Po zadání PUK, který má 8 míst, získá klient další pokusy pro zadání PIN. Karta není po personalizaci vybavena PIN a PUK a klient je při prvním použití karty požádán o zvolení PIN a PUK. Variantně lze dodat čipové karty inicializované, kde je PIN a PUK již vytvořen a klient je obdrží v zabezpečené podobě.
* Auditní log na kartě – v rámci práce s kartou se budou do auditního logu zaznamenávat poslední provedené bezpečnostně citlivé operace jako je mazání klíčů, generování klíčů apod.

## Základní technické parametry

* Velikost privátního klíče generovaného na kartě: RSA 2048 a 4096, ECC NIST P-384
* Kryptografické funkce: AES až 256bit, RSA až 4096 bits, elliptic curves až 521bit
* Podpora Hashes: SHA1, SHA-2 až SHA-512
* Podporované standardy: ISO 7815-4/-8/-9, ISO 14443-1/-2/-3/-4
* Podporované protokoly: ISO 7816-3 T=0 a T=1
* Privátní klíč se generuje přímo v kartě a nikdy neopustí kartu¨
* Kapacita karty: 126,9 kB

## Kompatibilita se standardy

* ISO/IEC, DIN, EMV

## Podporované OS:

* OS: Windows 7 x64, 8 či 10, MacOS, Linux (ve vývoji)
* pro čipové karty je k dispozici pro komunikaci v prostředí Windows minidriver. Čipová karta I.CA je v systému dostupná prostřednictvím providera Microsoft Smart Card Base CSP (CAPI1) a KSP (CAPI2 KeyStorageProvider.) Výhodou KSP providera je, že umožňuje použití RSASSA-PSS a ECC.

## SecureStore I.CA

Aplikace SecureStore je samostatně běžícím programem na platformě MS Windows/MAC OS

s následujícími základními funkcemi:

* generování páru klíčů o velikosti 1024 nebo 2048 bit na kartě současně s vytvořením příslušné žádosti o certifikát vybraného typu (komerční, kvalifikovaný). Pro pár klíčů je vždy možné zvolit, zda se jedná o pár určený pro šifrování (pár se při tvorbě zálohuje) nebo pár určený pro elektronický podpis (pár se nezálohuje),
* import vydaného certifikátu na kartu - vydaný certifikát ve formátu DER uloží na kartu do příslušného úložiště k páru klíčů,
* práce s certifikáty uloženými na čipové kartě a správa úložišť na kartě - včetně mazání a importu certifikátu,
* označení úložiště používaného pro Windows SmartCard Logon,
* PIN management - změna PIN – se znalostí starého PINu lze nastavit nový, odblokování

PIN - pomocí zadání PUK získá uživatel nové pokusy pro zadání PIN,

* registrace certifikátu do Windows - provede instalaci certifikátu do úložišť Windows tak, aby byl dostupný pomocí služeb pracujících s certifikáty v prostředí Windows,
* sledování využití prostoru karty,
* nativní podpora pro TWINS
* využití volného prostoru karty pro ukládání libovolných souborů. Úložiště pro volný prostor je možné zvolit ve dvou variantách:

1. nezabezpečené, které je volně přístupné
2. zabezpečené, které je přístupné pouze po zadání PINu k tomuto úložišti. Toto úložiště je vhodné např. pro správu hesel.

* Aplikace umožňuje automatický upgrade dle definovaných parametrů pro klienty s Win 10 x64.

## Zřízení klientské registrační autority

I.CA bezplatně zřídí a zajistí provoz registrační autority (RA) v sídle zadavatele včetně dodání potřebného hardwarového a softwarového vybavení a potřebného školení – resp. využije v současnosti zřízených dvou pracovišť registrační autority. V případě potřeby I.CA na žádost zadavatele bezplatně zřídí a vybaví další pracoviště registrační autority, případně proškolí nové operátory.

RA je místo kde operátoři RA (zaměstnanci zadavatele) mohou vydávat všechny druhy certifikátů I.CA (s výjimkou SSL certifikátů, které se vydávají elektronicky bez návštěvy RA) bezpečným a přitom rychlým a pohodlným způsobem.

Aplikace RA přijímá žádosti o služby podle Certifikačních politik I.CA a pomáhá plnit úkoly I.CA vyplývající z jejího vztahu ke klientům, zejména přijímá žádosti o vydání certifikátů a zprostředkovává předání vydaných certifikátů a dokumentace s procesem vydání certifikátů spojené. Jedná se o univerzální řešení, které je přizpůsobitelné pro prostředí kteréhokoli klienta. Instalace aplikace i její obsluha je jednoduchá a intuitivní.

Dodávka každé RA zahrnuje SW RA a speciální HW RA (součástí dodávky RA není PC, notebook tiskárna či kopírka).

RA musí být v průběhu procesu přijetí žádosti a vydání certifikátu připojena k internetu.

## Vlastní zřízení Registrační autority I.CA

* RA může být zřízena ve formě stacionární (instalace na PC + podpůrný bezpečný HW + tiskárna), nebo ve formě mobilní (instalace na notebook + podpůrný bezpečný HW + tiskárna)
* na RA bývají vyškoleni zpravidla dva pracovníci = dva operátoři RA (tj. dva zaměstnanci provozovatele Registrační autority, dále též provozovatele RA), lze však vyškolit libovolný počet operátorů
* dodávku RA, kterou tvoří licence SW RA, čtečka, operátorské čipové karty a razítko

provede I.CA po podpisu smlouvy s provozovatelem RA

* vlastní instalaci RA provede I.CA na pracovišti provozovatele RA nebo na jím určeném místě a současně vyškolí budoucí operátory RA
* na školení jsou předány všechny HW komponenty, ověřena totožnost operátorů podle předložených OP, vydány operátorské certifikáty na speciální čipové karty (pokud je klientem požadována plná provozuschopnost aplikace RA hned po provedení proškolení nových operátorů, je nutno vytvořit tyto certifikáty cca 2 dny před školením a zaregistrovat je v databázi I.CA), je podepsán předávací protokol
* dále jsou novými operátory podepsána „Prohlášení o proškolení“ a na jejich základě obdrží operátoři „Plnou moc k vydávání certifikátů I.CA“.

Na odbornost operátorů nejsou kladeny žádné zvláštní nároky, aplikace vydávání certifikátů je intuitivní a návodná.

## Školení administrátorů a uživatelů RA

I.CA zajistí pro pracovníky provozovatele RA (operátory) školení, týkající se vydávání certifikátů v souladu se zákonem č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce.

## Hlavními body školení jsou:

* úvod do problematiky infrastruktury veřejných klíčů (PKI),
* seznámení s legislativou upravující problematiku certifikačních služeb a elektronického podpisu a certifikačními politikami I.CA,
* vydávání certifikátů:
  + požadované doklady pro vydání certifikátu,
  + vytvoření žádosti o certifikát, povinné, nepovinné položky, kontrola naplnění,
  + předání vydaného certifikátu,
  + vytváření a uchovávání dokumentace a její následné předání do archivu I.CA,
* podepsání patřičných protokolů a prohlášení operátory RA,
* vydání operátorských certifikátů.

## Součásti dodávky RA je:

* bezpečná operátorská čtečka čipových karet
* operátorské čipové karty
* razítko I.CA
* SW RA pro komunikaci s I.CA ICARA
* SW pro správu čipové karty SecureStore
* školení operátorů v potřebném rozsahu (cca 4 hodiny)
* support pro operátory (e-mail, telefon)
* přístup operátora na web RAINFO, kde jsou umístěny všechny relevantní informace potřebné pro vydávání certifikátů.

HW a SW komponenty RA, které nejsou součástí dodávky I.CA

1. PC (ve verzi stacionární RA) nebo notebook (ve verzi mobilní RA), schopné provozovat Win7, 8, či 10 – není součástí dodávky RA
2. tiskárna – není součástí dodávky RA

## Výjezd mobilní registrační autority

Vydání certifikátů je možné v případě zájmu a požadavku zadavatele zajistit výjezdem mobilní registrační autority I.CA. Za jeden den, tj. 8 hodin, je možné vydat cca 20-25 prvotních certifikátů.

## Správa certifikátů

Pro splnění povinnosti dané veřejnoprávním původcům (orgánům veřejné moci) vyhláškou č. 259/2012 Sb., o podrobnostech výkonu spisové služby, nabízí I.CA aplikaci Správa certifikátů.

Aplikaci Správa certifikátů nabízí I.CA těm klientům, kteří využívají služeb I.CA a používají certifikáty vydané I.CA. Služba je dostupná přes webové rozhraní po autentizaci komerčním certifikátem vydaným I.CA k tomuto účelu zdarma.

Její největší předností je možnost zneplatnění certifikátu i tehdy, pokud není známo heslo pro zneplatnění.

Prostřednictvím aplikace Správa certifikátů mají po autentizaci komerčním certifikátem pověřené osoby klienta přístup ke všem údajům požadovaným výše uvedenou vyhláškou a zároveň mají možnost prostřednictvím aplikace zneplatnit libovolný certifikát vydaný pro danou organizaci, a to i bez znalosti hesla pro zneplatnění certifikátu. Jednotlivým pověřeným osobám lze nastavit různé úrovně oprávnění (nižší – pouze prohlížení údajů o certifikátech, vyšší – prohlížení + zneplatňování certifikátů).

Přístup do aplikace Správa certifikátů je zahrnut v ceně certifikátů spravovaných aplikací.

## Dodávka licencí ICA Secom2

Aplikace *I.CA Secom 2®* umožňuje vytváření a ověřování elektronických podpisů. Pomocí aplikace je možné podepsat všechny typy souborů: textové soubory, obrázky v libovolných formátech, scanované obrázky, různé texty či binární soubory apod. K vytváření elektronického podpisu je třeba vlastnit soukromý klíč a certifikát. Soukromý klíč může být uložen v úložišti na PC nebo v bezpečném zařízení jako je např. čipová karta nebo token.

Režimy aplikace jsou koncipovány pro snadné používaní s jednoduchými ovládacími prvky. Aplikace ověřuje dokumenty s časovými razítky až po dobu jejich platnosti a umožňuje uživatelům vytvářet elektronické podpisy prostřednictvím více kvalifikovaných certifikátů I.CA díky uživatelským profilům. Zároveň disponuje níže uvedenými funkcemi a vyhovuje požadavkům aktuálních technických standardů a norem ETSI.

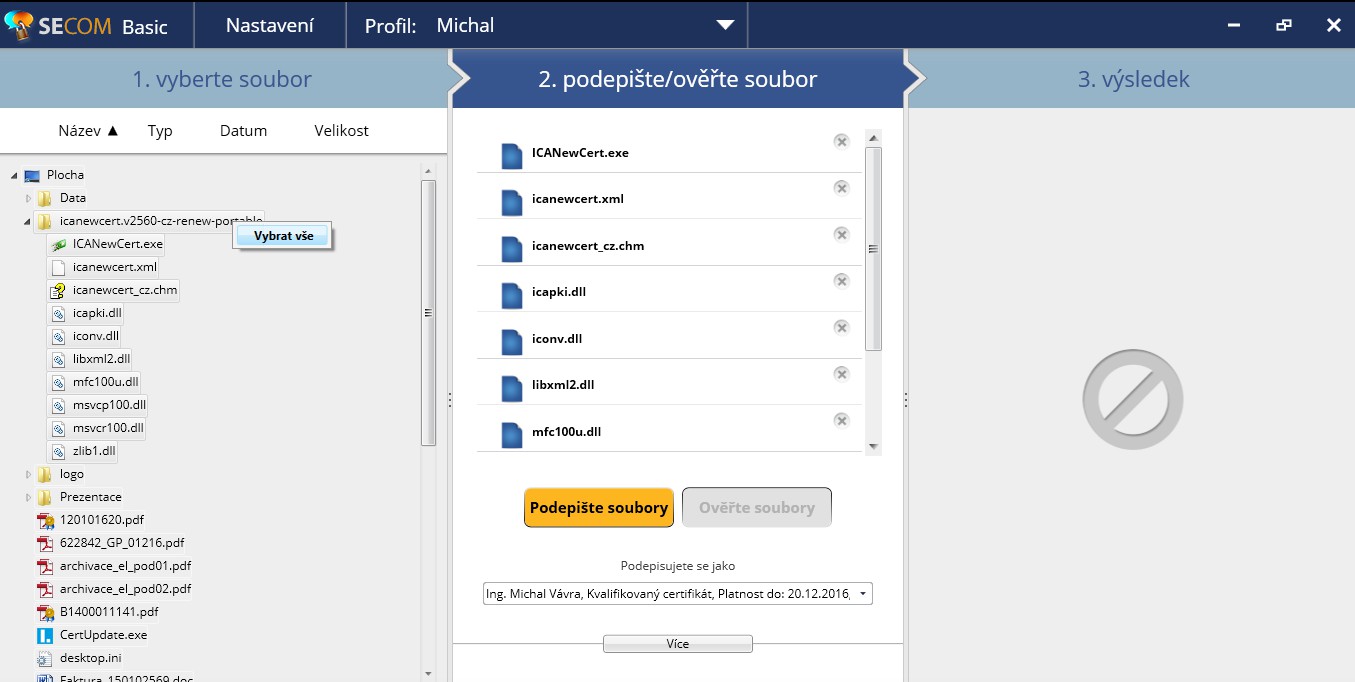
## Základní přehled funkcí aplikace

1. Vytváření podpisů PAdES (podpis souborů typu PDF)
2. Vytváření podpisů CAdES (podpis ostatních libovolných souborů)
3. Možnost přidání kvalifikovaných časových razítek I.CA k elektronickému podpisu
4. Viditelná prezentace podpisu PAdES v PDF dokumentech s variabilními texty a položkami převzatými z certifikátu
5. Možnost podepisování a razítkování přímo z MS Word
6. Hromadné podepisování dokumentů - složkové podepisování
7. Vícenásobné podepisování dokumentů - podepsání již podepsaných dokumentů
8. Hromadné ověřování dokumentů s elektronickým podpisem a časovým razítkem
9. Ověřování expirovaných elektronických podpisů s časovými razítky vůči starším seznamům zneplatněných certifikátů (CRL).
10. Uživatelské profily - v jedné aplikaci lze podepisovat více certifikáty I.CA
11. Možnost nastavení historie podepisování
12. Automatické online aktualizace formou neplacených updatů
13. Možnost napojení na proxy server pro odběr časových razítek
14. Uživatelská podpora - hotline
15. Možnost automatického zálohování podepsaných dokumentů

## Hlavní okno aplikace a hromadné podepisování dokumentů - složkové podepisování

Hlavní okno aplikace se skládá z horního panelu - menu, dolního panelu a ze tří sloupců, přičemž v prvním sloupci se vybírají ze stromové struktury dokumenty k podpisu nebo k ověření, ve druhém sloupci jsou zobrazeny vybrané dokumenty a funkce podepsat nebo ověřit a ve třetím sloupci jsou indikovány výsledky zvolených akcí s dokumenty.

Aplikace umožňuje hromadné podepisování vybraných dokumentů. Uživatel může jednotlivé dokumenty ručně zvolit nebo může jednoduše vybrat příslušnou složku a podepsat všechny dokumenty z této složky.



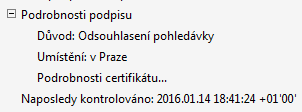
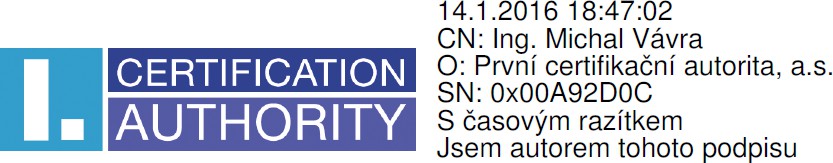
## Výběr typu podpisu

Před vytvořením podpisu aplikace sama detekuje typ dokumentu, který chce uživatel podepsat a nabídne příslušné podepisovací menu.

* + U non PDF dokumentů je možné vytvořit externí nebo interní podpis s možností přidání časového razítka. Jedná se o podpisové formáty typu CAdES, které jsou vytvářeny v souladu se standardem ETSI 101 733 Electronic Signatures and Infrastructures (modré ikony).
  + U PDF dokumentů je pak možné vytvořit samotný podpis spolu s časovým razítkem nebo vytvořit i tzv. viditelný podpis, který bude zobrazen na definovaném místě v PDF dokumentu. Jedná se o podpisové formáty typu PAdES, které jsou vytvářeny v souladu se standardem ETSI 102 778 Electronic Signatures and Infrastructures (červené ikony).

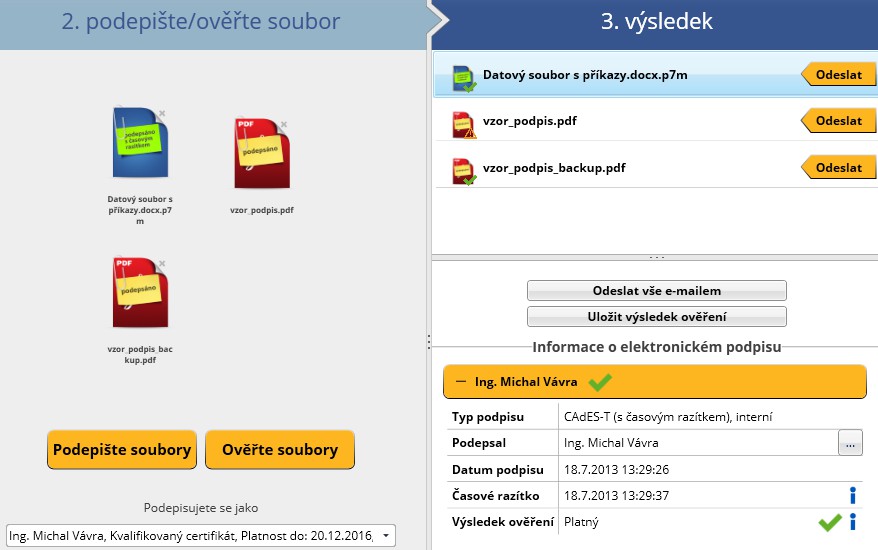


Viditelný podpis v PDF dokumentu zobrazuje dodatečné informace o podpisu s možností definování variabilního textu nebo loga společnosti podepisovatele. Zobrazuje se i na tištěné verzi dokumentu. Pokud by viditelný podpis zasahoval do textu, je možné dodatečné informace o podpisu zadat přímo do jeho struktury.



## Možnosti ověřování elektronických podpisů

Aplikace umožňuje hromadné ověřování vybraných dokumentů. Ověřují se dokumenty, u kterých je nebo byl vytvořen elektronický podpis s nebo bez časového razítka. Vyhodnocení starších, již expirovaných elektronických podpisů, které doposud obsahují platné časové razítko, je prováděno na základě stažení starších CRL listů, které jsou získávány díky knihovně I.CA GetOneCRL. Jedná se o jedinečnou funkčnost aplikace, která umožňuje ověřovat elektronické podpisy s časovými razítky až po samotnou dobu platnosti časového razítka na rozdíl od jiných aplikací a programů (např. Adobe), které touto funkčností nedisponují.

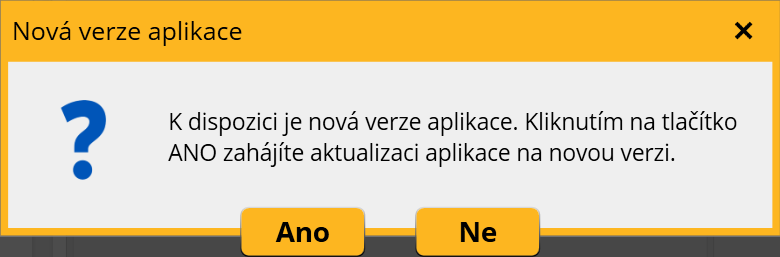


Detailní zobrazení informací o časovém razítku v elektronickém podpisu.



## Automatický online update aplikace

Pokud bude uvolněna nová verze I. CA Secom 2®, aplikace při spuštění sama nabídne uživateli automatický update na novou verzi aplikace. Průběžné aktualizace, jsou tak zárukou, že uživatel bude disponovat vždy aktuální verzí aplikace, které navíc mohou být obohaceny o další nové funkce.



## Minimální systémové požadavky

* + Aplikace je určena pro 32 a 64bitové operační systémy MS Windows
  + Podporované OS: Windows 7, Windows 8 a vyšší
  + Verze .NET: 4.0 a vyšší
  + Pro korektní fungování pluginu pro MS Word je vyžadována funkční instalace MS Office 2007 SP3 nebo novější

## Vydávání archivních kvalifikovaných elektronických časových razítek

Kvalifikované elektronické časové razítko je nástroj, který důvěryhodným způsobem zajišťuje přiřazení aktuálního časového údaje k existujícím datům, informacím, souborům nebo událostem, a to na základě důvěryhodného času odvozeného od UTC.

Kvalifikovaná elektronická časová razítka vydává časová autorita I.CA v souladu s Politikou pro vydávání časových razítek a doporučeními RFC 3161, RFC 3628 a RFC 5280 a dále v souladu s článkem 42 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 v aktuálním znění.

Pro archivní elektronická časová razítka platí všechny předpoklady jako pro klasická kvalifikovaná elektronická časová razítka, tj.:

* Časové razítko je datová zpráva, která **potvrzuje existenci dokumentu v čase**
* Slouží jako důkaz, že datový objekt, ke kterému je připojeno, **existoval bezprostředně před časovým údajem** uloženým v tomto časovém razítku
* Zajišťuje **přiřazení aktuálního časového údaje** k existujícím datům, informacím, souborům nebo událostem
* Spojení **nezpochybnitelného časového údaje** a konkrétních dat je nezbytné zejména pro účely jejich zpětného ověřování
* Časové razítko obsahuje **datum a čas vydání, číslo časového razítka, identifikaci třetí strany**, která časové razítko vydala (poskytovatele certifikačních služeb), **otisk dat (hash),** ke kterým je razítko vydáno, a **elektronickou značku či pečeť poskytovatele certifikačních služeb**, který razítko vydal.

## Nicméně klasické časové razítko není možné ověřit po uplynutí doby platnosti certifikátu serveru časové autority, jehož pomocí poskytovatel certifikačních služeb označil datovou zprávu/časové razítko. Obvyklá doba platnosti certifikátu je 3-5 let. Po uplynutí této doby není možné průkazně ověřit stav podpisu, protože certifikát již není platný.

Proto I.CA nabízí službu archivních kvalifikovaných elektronických časových razítek, jež je založena na technologii časových razítek, jejich řetězení a ukládaní; princip vychází z RFC 4998 Evidence Record Syntax. Prvním razítkem je označen hash dokumentu, druhým razítkem v řadě hash prvního razítka atd. Interní aplikace I.CA nepracuje s původním razítkovaným dokumentem.

Služba je dostupná v **režimu 365 x 24 hodin**, tedy jedná se o nepřetržitou službu.

U časových razítek vydávaných jako archivní se I.CA zavazuje zajistit ověřitelnost platnosti časového razítka a tím i jeho průkaznost po dobu 10 let od vydání prvotního časového razítka.

Výsledek ověření je ukládán v interních systémech I.CA. Ukončení smluvního vztahu odstoupením, výpovědí nebo jiným způsobem se nedotýká doby trvání tohoto závazku I.CA.

## Tuto službu nabízí I.CA jako službu plně zajištěnou v prostředí I.CA. Procesy potřebné pro zajištění ověřitelnosti jsou realizovány v systémech I.CA bez součinnosti zadavatele.

**Vlastnosti**

Klient odebírá klasická časová razítka, interní aplikace I.CA hlídá platnost časového razítka konkrétního klienta, se kterým existuje právní vztah – smlouva na vydávání archivních časových razítek. Před expirací platnosti časového razítka, resp. před koncem platnosti certifikátu serverů časové autority, nejdříve však po vydání nového certifikátu TSS, aplikace časové razítko přerazítkuje a uloží v interních systémech I.CA.

I.CA k datu podpisu smlouvy poskytne webovou on-line aplikaci dostupnou zadavateli k ověření stavu archivního časového razítka po zadání SN razítka či hash dokumentu.

Minimálně po dobu 10 let od vydání prvotní archivního časového razítka vyhledá na základě dotazu klienta I.CA konkrétní razítko spolu s následnými razítky v nepřerušené řadě a vyhledanou řadu razítek předá klientovi, a to v těchto formách:

* Přerazítkované razítko – zřetězená řada razítek a data nutná pro ověření. Kromě řady razítek poskytne I.CA klientovi data potřebná pro ověření časových razítek, tj. kořenový certifikát a CRL vztahující se k certifikátu TSS a CRL. Dále poskytne kořenový certifikát a první CRL vydané po vydání prvního razítka, které může klient využít k ověření podpisu razítkovaného souboru, je-li tento podepsán.
* Protokol o řetězených/přerazítkovaných razítkách podepsaný I.CA, kterým se stvrzuje, že původní razítko bylo přerazítkováno a je technicky ověřitelné v době žádosti o protokol; protokol je dostupný přes webové rozhraní s autentizací komerčním certifikátem. Na základě protokolu si může klient požádat o poskytnutí přerazítkovaného razítka a uložit si jej ve svém archivu.
* Službu na vyhledání přerazítkovaného razítka. Výstupem je archiv obsahující požadovanou řadu razítek k dokumentu zaslaný klientovi na zadanou e-mail adresu
* Kompletní strukturu pro potřeby např. soudního znalce, tj. řada razítek, CRL, kořenový certifikát, certifikát TSA.

Archivní elektronická časová razítka najdou uplatnění především tam, kde klient potřebuje uložit dokumenty či data na delší časové období (cca 10 i více let) a současně důvěryhodným způsobem po celou dobu uložení prokázat platnost dokumentu, čas jeho uložení, neměnnost obsahu.

**Využitím služby ATSA v prostředí První certifikační autority, a.s., lze ušetřit nemalé finanční prostředky potřebné pro vybudování archivního systému**, veškerou odpovědnost za prokázání platnosti všech zřetězených časových razítek (a tím platnost původního dokumentu) garantuje První certifikační autorita, a.s. (sankční ustanovení ve smlouvě), klient pouze standardním způsobem razítkuje časovými razítky.