Dodatek č. 1
k Příkazní smlouva o provozu registrační autority
Vojenské nemocnice Brno pro vydávání kvalifikovaných
a komerčních certifikátů a o poskytování služeb I.CA

uzavřená podle ustanovení § 2430 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „Občanský zákoník")

Smluvní strany

První certifikační autorita, a.s.
se sídlem Podvinný mlýn 2178/6, 190 00 Praha 9
zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, spisová značka B 7136

IČO:	26439395
DIČ:	CZ26439395
zastoupená:	Ing. Petrem Budišem, Ph.D., předsedou představenstva a Ing. Romanem Kučerou, členem představenstva
Bankovní spojení:	Československá obchodní banka, a.s.
Číslo účtu:	168457418/0300

dále jen „Příkazce" nebo „I.CA"

a

Vojenská nemocnice Brno
se sídlem Zábrdovická 3, 615 00 Brno

IČO:	60555530
DIČ:	CZ60555530
zastoupená:	plk. gšt. MUDr. Petr KRÁL, MBA, ředitelem VN Brno
Bankovní spojení:	Česká národní banka
Číslo účtu:	4034881/0710

dále jen „Příkazník" nebo „Nemocnice"

se dohodly na této změně Příkazní smlouvy o provozu registrační autority Vojenské nemocnice Brno pro vydávání kvalifikovaných a komerčních certifikátů a o poskytování služeb I.CA ze dne 16.10.2017 (dále jen „Smlouva"). Účelem uzavření tohoto dodatku č. 1 Smlouvy je rozšíření o čerpání poskytovaných služeb:

- Kvalifikované elektronické časového razítko a archivní kvalifikované elektronické časové razítko I.CA

1) Tímto dochází ke změně znění Preambule smlouvy. Nové znění Preambule:

„Obě smluvní strany se podpisem této smlouvy dohodly na spolupráci, jejímž cílem je zajištění veškerých činností nutných pro vydávání kvalifikovaných a komerčních certifikátů I.CA, kvalifikovaných elektronických časových razítek a archivních kvalifikovaných elektronických časových razítek I.CA pro potřeby Nemocnice. Smlouva má tři části:

- ***Část první*** *– provozování registrační autority Nemocnice (dále též Registrační autority I.CA), zřízené pro Nemocnici*
- ***Část druhá*** *– poskytování certifikačních služeb I.CA pro Nemocnici*
- ***Část třetí –*** *vydávání kvalifikovaných časových razítek a archivních kvalifikovaných časových razítek I.CA pro Nemocnici*"

2) Základní pojmy se rozšiřují o:

PTSA *politika vydání kvalifikovaných elektronických časových razítek*

3) Za druhou část se doplňuje třetí část Smlouvy a před čl. XIX. Doba trvání smlouvy se vkládá:

Část třetí – vydávání kvalifikovaných časových razítek I.CA a archivních kvalifikovaných časových razítek I.CA pro Nemocnici

XIX. Úvodní ustanovení

1) I.CA je oprávněn vydávat kvalifikovaná elektronická časová razítka dle nařízení Evropského parlamentu a Rady (EU) č. 910/2014, o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES ve znění Nařízení Evropského parlamentu a Rady (EU) 2024/1183 ze dne 11.dubna 2024, kterým se mění nařízení (EU) č. 910/2014, pokud jde o zřízení evropského rámce pro digitální identitu („eIDAS2").

XX. Předmět Smlouvy

1) Předmětem plnění této Smlouvy je vydávání kvalifikovaných elektronických časových razítek a archivních kvalifikovaných elektronických časových razítek (dále též „archivní časová razítka") pro potřeby Nemocnice v souladu s platnou politikou vydávání časových razítek (dále jen „PTSA"), která je vždy v aktuální verzi k dispozici na https://www.ica.cz/Userfiles/files/politika/HCA/Kvalifikovane/CZ/P_TSA_RSA_2v07.pdf a současně závazek Nemocnice za odebraná kvalifikovaná časová razítka uhradit sjednanou cenu.

2) Kvalifikovaná elektronická časová razítka a archivní časová razítka (dále společně též „časová razítka"), vydávaná podle této Smlouvy, budou vydávána pouze oprávněnému žadateli. Oprávněným žadatelem se pro účely této Smlouvy rozumí fyzická nebo právnická osoba, která se prokazuje (autentizuje) v elektronické komunikaci platným certifikátem, jménem a heslem nebo IP adresou.

XXI. Povinnosti Nemocnice

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

2) Nemocnice nese plnou a výlučnou odpovědnost za újmy na jmění vzniklé v souvislosti s nedodržením PTSA.

3) Nemocnice se zavazuje neposkytovat plnění poskytnuté I.CA dalším osobám bez souhlasu I.CA.

XXII. Povinnosti I.CA

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

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

3) Před uplynutím lhůty 10 let, bude s příkazníkem projednáno, zda bude ověřitelnost platnosti prvního archivního časového razítka navýšena na dalších 10 let a s tím související služby.

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

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

   - archivní časová razítka a data nutná pro jejich ověření,

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

6) Ukončení smluvního vztahu odstoupením, výpovědí nebo jiným způsobem se nedotýká doby trvání závazku I.CA plynoucího z odstavce 14.4. tohoto článku Smlouvy.

7) I.CA se taktéž zavazuje:
   - zajistit, aby časová razítka obsahovala všechny náležitosti stanovené příslušnými obecně závaznými právními předpisy,
   - zajistit, aby časový údaj vložený do časového razítka odpovídal hodnotě koordinovaného světového času při vytváření časového razítka,
   - zajistit, aby data v elektronické podobě, která jsou předmětem žádosti o vydání časového razítka, jednoznačně odpovídala datům v elektronické podobě obsaženým ve vydaném časovém razítku,
   - přijmout odpovídající opatření proti padělání časových razítek,
   - poskytovat na vyžádání třetím osobám podstatné informace o podmínkách pro využívání časových razítek, včetně omezení pro jejich použití; tyto informace lze poskytovat elektronicky.

8) I.CA se zavazuje poskytovat příkazníkovi podporu zaručenou platnou PTSA.

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

10) I.CA prohlašuje, že vydávání časových razítek odpovídá všem požadavkům vyplývajícím z právních předpisů, které se na plnění vztahují.

11) I.CA se zavazuje poskytovat službu vydávání časových razítek s propustností 2 ks časových razítek za sekundu.

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

XXIII. Cena služeb

1) Cena za vydání časových razítek bude stanovena podle skutečného odběru v daném kalendářním měsíci podle příslušného objemového pásma, a to jako součin „Ceny Kč za 1 ks razítka" a počtu skutečně odebraných razítek za kalendářní měsíc dle přiloženého rozpisu. K ceně bude připočteno DPH podle aktuálně platných předpisů.

Kvalifikované elektronické časové razítko Objemové pásmo množství razítek ks/měsíc	**Cena/ks bez DPH**
Do 500	1,00 Kč
Do 1.000	0,90 Kč
Do 2.000	0,75 Kč
Do 5.000	0,60 Kč
Do 7.500	0,55 Kč

2) Cena za vydání archivních časových razítek bude stanovena podle skutečného odběru v daném kalendářním měsíci podle příslušného objemového pásma, a to jako součin „Ceny Kč za 1 ks razítka" a počtu skutečně odebraných razítek za kalendářní měsíc dle přiloženého rozpisu. K ceně bude připočteno DPH podle aktuálně platných předpisů.

Archivní kvalifikované elektronické časové razítko (platnost 10 let) Objemové pásmo množství razítek ks/měsíc	**Cena/ks bez DPH**
Do 500	1,80 Kč
Do 1.000	1,62 Kč
Do 2.000	1,35 Kč
Do 5.000	1,08 Kč
Do 7.500	0,99 Kč

3) Úhrada vydaných časových razítek a archivních časových razítek podle této smlouvy bude prováděna vždy jednou měsíčně zpětně za uplynulý kalendářní měsíc, v nichž I.CA časová razítka vydala, a to podle počtu Nemocnicí skutečně odebraných časových razítek. Daňový doklad bude obsahovat počet skutečně odebraných časových razítek; cena bude stanovena jako součin „Ceny Kč za 1 ks razítka" a počtu skutečně odebraných razítek za kalendářní měsíc.

4) I.CA je povinna vystavit řádný daňový doklad do 15. dne následujícího kalendářního měsíce po kalendářním měsíci, za které je účtována cena za vydaná časová razítka.

5) Nemocnice je povinna uhradit daňové doklady převodem na účet I.CA do 30 dnů ode dne doručení daňového dokladu vystaveného I.CA. Příkazník požaduje elektronické zasílání faktur na e-mailovou adresu: .

6) Daňový doklad musí mít náležitosti daňových a účetních dokladů stanovených platnými právními předpisy. Nemocnice je oprávněna daňový doklad, který nebude splňovat náležitosti podle platných právních předpisů, vrátit I.CA. I.CA je povinna nedostatky daňového dokladu odstranit a vystavit nový daňový doklad. Na základě vadně vystaveného daňového dokladu ve smyslu tohoto odstavce se Nemocnice neocitá v prodlení se splatností. Lhůta splatnosti počíná

běžet znovu od opětovného doručení náležitě doplněného či opraveného daňového dokladu.

4) Články XIX. Doba trvání a XX. Závěrečné ustanovení se přečíslují na XXIV. A XXV..

5) Nově se doplňuje příloh č. 10 – Popis služby Kvalifikovaného elektronického časového razítka I.CA

6) Tento dodatek č. 1 Smlouvy nabývá platnosti a účinnosti dnem jeho podpisu. Tento dodatek je vyhotoven a podepsán pouze elektronicky (včetně vložených nových příloh). Ostatní ujednání Smlouvy zůstávají beze změny.

V Praze dne

První certifikační autorita, a.s.

Ing. Petr Budiš, Ph.D.
předseda představenstva

Ing. Roman Kučera
člen představenstva

V Brně dne

Vojenská nemocnice Brno, p. o.

plk. gšt. MUDr. Petr KRÁL, MBA
ředitel VN Brno

Popis služby Kvalifikovaného elektronického časového razítka I.CA

Základní informace

Co je časové razítko

Časové razítko zajišťuje přiřazení aktuálního časového údaje k existujícím datům, informacím, souborům nebo událostem. Připojuje se tedy k dokumentům, datům či elektronickému podpisu, u kterých chceme mít v budoucnu možnost ověřit, že v této podobě existovaly před časem uvedeným v časovém razítku.

Služba je poskytována na základě uzavřené smlouvy. Časová razítka jsou vydávána časovou autoritou I.CA na základě elektronické žádosti v normalizovaném tvaru, jejíž součástí je otisk dat (hash), pro která má být elektronické časové razítko vystaveno. Pokud žádost obsahuje všechny požadované náležitosti, časová autorita vytvoří odpověď obsahující otisk dat, který byl součástí příslušné žádosti, doplněný o aktuální časový údaj a další parametry a zašle ji žadateli.

Legislativa

- 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 (eIDAS)
- Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce

Politika a normy

- Politika pro vydávání elektronických časových razítek
- Normy: RFC 3161, RFC 3628, RFC 5280

Časové razítko obsahuje

Vydané časové razítko obsahuje minimálně:

- Unikátní číslo časového razítka
- Označení pravidel, podle kterých bylo časové razítko vydáno
- Časový údaj, jehož odchylka nepřesáhne 1 sekundu od UTC (+/- 500 ms TSA I.CA)
- Data v elektronické podobě - otisk (hash) dat, pro která bylo časové razítko vydáno
- Elektronickou značku serveru, který časové razítko vydal

Dostupnost služby

Služba je dostupná v režimu 365 x 24 hodin, jedná se tedy o nepřetržitou službu. I.CA garantuje vysokou spolehlivost dostupnosti dané služby, což dokumentují jednotlivé aplikace a také významní zákazníci, kteří provoz svých řešení spojili s odběrem časových razítek. I.CA

Kvalifikovaná Elektronická časová razítka – Popis řešení

Obvyklý postup a kroky při využívání služby časových razítek:

1. Realizace zprovoznění testování odběru časových razítek
2. Uzavření smlouvy I.CA s klientem
3. Zahájení odběru časových razítek.

Komunikace klient – autorita časových razítek

Komunikace mezi klientem žádajícím o časové razítko a serverem časové autority probíhá on-line v režimu žádost ⇔odpověď.

Pro komunikaci s autoritou časových razítek a práci s časovými razítky svým klientům I.CA zdarma poskytuje:

- **Aplikaci I.CA QTSA** pro prostředí Windows, která umožňuje získání časového razítka ke konkrétnímu dokumentu, resp. souboru. Je vhodná pro vydání časového razítka jednotlivě koncovým uživatelem. Časové razítko ukládá ve formátu TST (TimeStampToken) nebo TSR (TimeStampResponse).
- **Sady řádkových/dávkových klientů** – platforma C, Java.
- **Knihovny DLL** - knihovny, které I.CA dodává, jsou k dispozici pro prostředí Windows a Unix. Jsou určeny k integraci do vlastních systémů pro automatizované využívání služby časové autority.
- **Knihovna pro operační systém Linux**, je dodávána jako nativní knihovna ve 32 bitové i 64 bitové verzi, včetně potřebných souborů a dalších podpůrných knihoven. Současně je dodávána i testovací aplikace.

Dalším způsobem je vlastní zpracování datové struktury. Toto použití vyžaduje znalost normy pro časová razítka, která mimo jiné definuje datovou strukturu časového razítka (RFC 3161). Přičemž je třeba dodržet politiku vydávání časových razítek.

Zároveň je možné od I.CA obdržet dokumentaci SDK (Software Development Kit) DSE200 společnosti nCipher. Podmínkou poskytnutí této dokumentace je uzavření Smlouvy o mlčenlivosti, v souladu s požadavky společnosti Thales (nCipher).

Autentizace ke službě časové autority

Systém časové autority je autentizován, podporovány jsou následující způsoby autentizace:

- **Komerční certifikát vydaný I.CA** – tento komerční certifikát je po podpisu smlouvy klientovi vydán zdarma. Zákazníci časové autority mohou zároveň tento certifikát použít i pro přístup ke klientským službám, které jsou nabízeny a spojeny se službou časové autority.
- **Statická IP adresa** (vždy se jedná o IP adresu koncového počítače žadatele o časové razítko).
- **Jméno a heslo** (heslo je specifikováno na straně I.CA).

Testování služby TSA

Testování pro své potenciální klienty poskytuje I.CA zdarma po dobu jednoho měsíce. Po dohodě je možné testovací období prodloužit.

Postup zajištění testovacího certifikátu a přístupu do testování TSA:

- Instalace certifikátů testovací časové autority. Tyto certifikáty nejsou veřejně dostupné, v případě zájmu o testování vám budou na vyžádání zaslány.
- Žádost o testovací komerční certifikát, kterou vytvoříte pomocí našich webových stránek . Tento proces vydání testovacího certifikátu je automatický, žadateli je vydaný certifikát zaslán v zip formátu na e-mail, který při žádosti zadá. Tento certifikát má ovšem platnost pouze 30 dní. Je-li předpoklad, že by testování mohlo překročit 30 dní od vydání certifikátu, zašlete vygenerovanou žádost o testovací komerční certifikát na e-mail: . Bude Vám vydán testovací komerční certifikát s delší dobou platnosti.
- Pro autentizaci jménem a heslem Vám bude přístupové jméno i heslo nastaveno na straně I.CA. Pro změnu hesla je poskytnut klientovi speciální script, ten je spolu s návodem zaslán na vyžádání, přístup ke scriptu je autentizován testovacím komerčním certifikátem I.CA.
- Pro autentizaci statickou IP adresou musí tuto adresu klient sdělit.
- Nastavení na straně klienta žádajícího o testovací časové razítko. URL serveru časové autority a OID politiky jsou uvedeny níže.
- Po zavedení testovacího certifikátu do Vašeho TSA klienta můžete vyzkoušet vydání časového razítka z TSS serverů.

V současné době je testovací zařízení nastaveno pouze pro ověření možnosti vydání časového razítka. Není nastaveno pro zátěžovou zkoušku (nutno sjednat individuálně).

Pro zjednodušení zahájení odběru razítek nabízí I.CA před zahájením rutinního odběru zpřístupnění ostrého prostředí s ostrými autentizačními údaji zdarma k otestování. Zahájení fakturace nastává obvykle počátkem následujícího kalendářního měsíce.

Nastavení testovacího prostředí:

- autentizace **testovacím komerčním certifikátem**:
  - Politika časové autority - 1.3.6.1.4.1.23624.10.3.50.2.0
  - Server časové autority -

- autentizace **jménem a heslem spojení https:**
  - Politika časové autority - 1.3.6.1.4.1.23624.10.3.50.2.0
  - Server časové autority - _____

- autentizace **jménem a heslem spojení http:**
  - Politika časové autority - 1.3.6.1.4.1.23624.10.3.50.2.0
  - Server časové autority - _____

- autentizace **statickou IP adresou:**
  - Politika časové autority - 1.3.6.1.4.1.23624.10.3.50.2.0
  - Server časové autority - _____

Do systému je přístup pouze s testovacími komerčními certifikáty.

Postup nastavení ostrého prostředí

Nastavení ostrého odběru razítek (viz web I.CA _____
).

Postup je následující:
Rozhodněte, jakým způsobem budete chtít službu využívat:

- prostřednictvím aplikace QTSAklient pro prostředí Windows, kterou zdarma poskytuje I.CA. Aplikace umožňuje získání časového razítka ke konkrétnímu dokumentu resp. souboru. Je proto vhodná pro situace, kdy jsou časová razítka požadována jednotlivě konkrétním uživatelem.
- zakomponováním relevantních knihoven (dodávaných I.CA) do vlastního systému a automatizované využívání této služby. Knihovny jsou k dispozici pro prostředí Windows, Unix a Linux.
- vlastním zpracováním datové struktury, kterou poskytne důvěryhodná časová autorita I.CA. Toto použití vyžaduje znalost normy pro časová razítka, která mimo jiné definuje datovou strukturu časového razítka (RFC 3161).
- pomocí sady řádkových klientů pro Windows (platforma C, Java). V těchto případech kontaktujte, prosím, .

Autentizace k odběru časových razítek je možná čtyřmi způsoby:
> komerčním certifikátem:
Politika časové autority - 1.3.6.1.4.1.23624.10.1.50.2.0

Server časové autority -
Hash algoritmus - SHA-256, 512

> jménem a heslem HTTPS
Politika časové autority - 1.3.6.1.4.1.23624.10.1.50.2.0
Server časové autority - _____

Hash algoritmus - SHA-256, 512

> jménem a heslem HTTP
Politika časové autority - 1.3.6.1.4.1.23624.10.1.50.2.0
Server časové autority - _____

Hash algoritmus - SHA-256, 512

> statickou IP adresou
Politika časové autority - 1.3.6.1.4.1.23624.10.1.50.2.0
Server časové autority - _____

Hash algoritmus - SHA-256, 512

Pro zjednodušení zahájení odběru razítek nabízí I.CA zpřístupnění ostrého prostředí s ostrými autentizačními údaji zdarma k „otestování"; zahájení fakturace nastává obvykle počátkem následujícího kalendářního měsíce či dle dohody.

Archivní kvalifikovaná časová razítka – Popis řešení

Pro archivní časová razítka platí všechny předpoklady jako pro klasická 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 poskytovatele certifikačních služeb**, který razítko vydal.

Nicméně klasické časové razítko není možné ověřit po skončení platnosti certifikátu serveru časové autority, kterým poskytovatel certifikačních služeb označil časové razítko. Obvyklá doba platnosti certifikátu je cca 5

let. Po uplynutí této doby není možné průkazně ověřit stav podpisu, protože certifikát expiroval.

Po skončení platnosti kvalifikovaného certifikátu, kterým je podepsán dokument, a na kterém je založen uznávaný elektronický podpis, a skončení platnosti certifikátu, na kterém je založena elektronická značka poskytovatele služeb vytvářejících důvěru, kterou je označeno časové razítko, není technicky možné ověřit stav podpisu. Důkazní břemeno neplatnosti dokumentu leží vždy na protistraně, která však stejně jako první strana není schopna platnost či neplatnost prokázat. Prokázat platnost či neplatnost je možné při použití metody řetězení časových razítek, kterou se prodlužuje doba, po kterou lze ověřit platnost kvalifikovaného certifikátu, kterým je podepsán dokument.

Proto I.CA nabízí službu archivních časových razítek (ATSA), 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.

Tuto službu nabízí I.CA jako službu plně zajištěnou v prostředí I.CA

Vlastnosti archivních časových razítek

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 aplikace časové razítko přerazítkuje a uloží v interních systémech I.CA. Na základě dotazu klienta vyhledá 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-mailovou adresu.
- **Kompletní strukturu** pro potřeby např. soudního znalce, tj. řada razítek, CRL, kořenový certifikát, certifikát TSA.

Archivní 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.

Autentizace k odběru archivních časových razítek je možná čtyřmi způsoby:

> komerčním certifikátem:

Politika časové autority - 1.3.6.1.4.1.23624.10.1.50.2.0
Server časové autority - _____

Hash algoritmus - SHA-256, 512

> jménem a heslem HTTPS

Politika časové autority - 1.3.6.1.4.1.23624.10.1.50.2.0
Server časové autority - _____
- SHA-256, 512

> jménem a heslem HTTP

Politika časové autority - 1.3.6.1.4.1.23624.10.1.50.2.0
Server časové autority - _____

Hash algoritmus - SHA-256, 512

> statickou IP adresou

Politika časové autority - 1.3.6.1.4.1.23624.10.1.50.2.0
Server časové autority - _____

Hash algoritmus - SHA-256, 512