Smlouva o poskytování služeb
číslo SWE/19/35

uzavřená podle ustanovení § 1746 odst. 2 zák. č. 89/2012 Sb., občanského zákoníku (dále jen „Občanský zákoník“)

VERA, spol. s r.o.

se sídlem: Praha 6 - Vokovice, Lužná 716/2

kontaktní adresa: Klicperovo náměstí 39/I, 503 51 Chlumec nad Cidlinou

IČ: 62587978, DIČ: CZ62587978

Zastoupena: 

společnost zapsaná v obchodním rejstříku vedeném Městským soudem v Praze,

oddíl C, vložka 34140

bankovní spojení: Fio banka, a. s., číslo účtu: 2400431298/2010

(dále též „**Vera**“ nebo „**Poskytovatel**“)

a

Město Přeštice

se sídlem: Masarykovo nám. 107, 334 01 Přeštice

IČ: 00257125, DIČ: CZ00257125

zastoupené: Mgr. Karlem Naxerou, starostou

(dále též „**Objednatel**“)

(dále jednotlivě také jako **„smluvní strana“** a společně také jako „s**mluvní strany**“)

uzavírají níže uvedeného dne, měsíce a roku tuto Smlouvu o poskytování služeb (dále jen „Smlouva“).

Článek I.

Preambule

1. Poskytovatel prohlašuje, že je distributorem produktu společnosti **První certifikační autorita, a.s.,** se sídlem Praha 9 – Libeň, Podvinný mlýn 2178/6, PSČ 190 00, IČ: 264 39 395 (dále jako „I.CA“ nebo „První certifikační“), která je kvalifikovaným poskytovatelem služeb vytvářejících důvěru podle Nařízení Evropského parlamentu a Rady č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES („eIDAS“) a zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, pro oblast vydávání kvalifikovaných certifikátů pro elektronické podpisy, (kvalifikovaných) elektronických časových razítek, kvalifikované služby ověřování platnosti elektronických

podpisů a pečetí I.CA QVerify, kvalifikovaných certifikátů pro elektronické pečetě, kvalifikovaných certifikátů pro autentizaci internetových stránek a kvalifikované služby ověřování platnosti elektronických podpisů a pečetí. Služba I.CA RemoteSeal, vzhledem k tomu, že není přímo v nařízení eIDAS definována, nemůže být auditována jako kvalifikovaná služba. Nicméně byla posouzena orgánem dohledu, Ministerstvem vnitra ČR, a jeho rozhodnutím čj. MV-68158-6/EG-2018 ze dne 21. června 2018 bylo I.CA povoleno poskytovat službu vytváření kvalifikovaných elektronických pečetí na dálku I.CA RemoteSeal v souladu s politikou této služby a v souladu s technickou a uživatelskou dokumentací zařízení ARX CoSign v8.2 a DocuSign Signature Appliance v8.4. Dále bylo stejným rozhodnutím povoleno I.CA vydávat kvalifikované certifikáty pro elektronické pečetě podle certifikační politiky vydávání kvalifikovaných certifikátů pro elektronické pečetě na dálku (algoritmus RSA), verze 1.00 (identifikátor 1.3.6.1.4.1.23624.10.1.38.1.0). Identifikátor této služby byl uveřejněn v důvěryhodném seznamu České republiky u služby „(78) I.CA – vydávání kvalifikovaných certifikátů“ společně s identifikátorem „QCQSCDManagedOnBehalf“ podle kap. 5.5.9.2.3 technických specifikací ETSI TS 119 612 v2.1.1. Důvěryhodný seznam je veden na https://tsl.gov.cz/publ/TSL_CZ.xtsl.

Článek II.
Předmět smlouvy

1. Předmětem této smlouvy je **zajištění provozu kvalifikované služby ověřování platnosti elektronických podpisů a pečetí** (tj. zaručených elektronických podpisů založených na kvalifikovaném certifikátu pro elektronický podpis, kvalifikovaných elektronických podpisů, kvalifikovaných elektronických pečetí a zaručených elektronických pečetí založených na kvalifikovaném certifikátu pro elektronickou pečeť) v souladu s platnou *Politikou kvalifikované služby ověřování platnosti kvalifikovaných elektronických podpisů a pečetí*, která je vždy v aktuální verzi k dispozici na www.ica.cz. Obchodní označení služby je I.CA QVerify.

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

3. Předmětem této Smlouvy je dále **vydávání kvalifikovaných elektronických časových razítek I.CA** (dále jen "časových razítek" nebo TSA) v souladu s platnou *Politikou vydávání kvalifikovaných elektronických časových razítek systémem TSA2*, která je vždy v aktuální verzi k dispozici na www.ica.cz. 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 I.CA, jménem a heslem nebo IP adresou. Způsob autentizace ke službě časových razítek je uveden v příloze této Smlouvy.

Článek III.
Povinnosti Objednatele

1. Vera poskytuje kvalifikovanou službu ověřování platnosti elektronických podpisů a pečetí v souladu se závazným prohlášením uvedeným v Preambuli této Smlouvy. Objednatel se zavazuje zabezpečit dodržování platné *Politiky kvalifikované služby ověřování platnosti kvalifikovaných elektronických podpisů a pečetí* („Politika“).

2. Vera poskytuje službu vytváření kvalifikovaných elektronických pečetí na dálku v souladu se závazným prohlášením uvedeným v Preambuli této Smlouvy. Objednatel se zavazuje zabezpečit dodržování platné *Politiky služby vytváření kvalifikovaných elektronických pečetí na dálku* („Politika“).

3. Objednatel se zavazuje ve svých projektech, využívajících časová razítka, vydaná na základě této Smlouvy, zabezpečit dodržování platné *Politiky vydávání kvalifikovaných elektronických časových razítek systémem TSA2* dostupné na www.ica.cz (dále jen „Politika“).

4. Veškeré změny a doplňky výše uvedených Politik (v bodech 1 až 3) jsou vůči Objednateli účinné okamžikem předání změn a doplňků na emailovou adresu: podatelna@prestice-mesto.cz.

5. Objednatel je povinen nahradit újmu na jmění vzniklou v souvislosti s nedodržením Politiky.

6. Objednatel se zavazuje neposkytovat plnění poskytnuté Poskytovatelem dalším osobám.

Článek IV.
Povinnosti Vera

1. Vera poskytuje Objednateli *kvalifikovanou službu ověřování platnosti elektronických podpisů a pečetí* (dále též „I.CA QVerify“) v souladu s články 32, 33 a 40 nařízení Evropského parlamentu a Rady č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (eIDAS). Popis služby je uveden v příloze č. 1 této Smlouvy.

2. Vera se zavazuje poskytovat službu I.CA QVerify v režimu 24/7, tedy 24 hodin denně, 7 dní v týdnu, s SLA 98 % za kalendářní den a kapacitou až 50 ověření za minutu.

3. Vera garantuje a nese odpovědnost za výsledek ověření platnosti elektronického podpisu a elektronické pečetě pouze za předpokladu, že data nutná k ověření (odesílaná do prostředí I.CA), generovaná komponentou dodanou I.CA, nebyla jakkoliv pozměněna a nebylo s nimi nijak manipulováno. Pro kontrolu integrity odesílaných dat z prostředí Objednatele a dat přijatých v prostředí I.CA využije I.CA aplikaci, která v případě sporu porovná hashe spočtené z jednotlivých souborů komponentou I.CA (po kontrole autenticity komponenty pomocí hashe) s hashi přijatými v prostředí I.CA. Pokud budou hashe totožné, lze konstatovat, že data byla generován originální komponentou I.CA, jsou správná a nebyla pozměněna.

4. Vera poskytuje Objednateli *službu vytváření kvalifikovaných elektronických pečetí na dálku* (dále též „I.CA RemoteSeal“) v souladu s bodem 52 recitálu, články 29 a 39, Přílohou II body 3 a 4, Přílohou III nařízení Evropského parlamentu a Rady č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (eIDAS) a rozhodnutím Ministerstva vnitra ČR čj. MV-68158-6/EG-2018 ze dne 21. června 2018. Popis služby je uveden v příloze č. 1 této Smlouvy.

5. Vera se zavazuje poskytovat službu I.CA RemoteSeal v režimu 24/7, tedy 24 hodin denně, 7 dní v týdnu, s SLA 99,5 % za kalendářní den a kapacitou až 60 vytvořených pečetí za minutu. Ve stejném rozsahu se Vera zavazuje nabízet službu časových razítek v souvislosti s pečetěním dokumentů.

6. Vera se zavazuje poskytovat:

    a) technickou podporu při provozu služby a řešení nestandardních situací prostřednictvím Helpdesku dodavatele na adrese: https://helpdesk.vera.cz/ih/ihzakaznik v rozsahu Po – Pá 8:00 – 17:00 hod.
    b) právní a technickou aktuálnost komponenty pro zajištění komunikace s I.CA, jakož i celou službu I.CA QVerify, s relevantními právními a technickými předpisy a normami v návaznosti na eIDAS.
    c) za účelem otestování nových verzí služby I.CA QVerify před nasazením do ostrého provozu službu I.CA TQVerify v testovacím prostředí s funkcionalitou obdobnou službě I.CA QVerify v ostrém prostředí, tj. PDF/XML protokol, stejné formáty ověřovaných podpisů; pro testovací prostředí platí SLA 99% za kalendářní den a kapacita 60 ověření za minutu.
    d) právní a technickou aktuálnost komponenty pro zajištění komunikace s I.CA, jakož i celou službu I.CA RemoteSeal, s relevantními právními a technickými předpisy a normami v návaznosti na eIDAS.
    e) za účelem otestování nových verzí služby I.CA RemoteSeal před nasazením do ostrého provozu službu I.CA RemoteSeal v testovacím prostředí s funkcionalitou obdobnou službě I.CA RemoteSeal v ostrém prostředí, pro testovací prostředí platí SLA 95% za kalendářní den a kapacita 10 vytvořených pečetí za minutu.

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

8. Vera se zavazuje Objednateli jako oprávněnému žadateli o služby časové autority poskytovat danou komplexní službu vydávání časových razítek pro jím realizovaná řešení v souladu s platnou Politikou a veškerými relevantními právními předpisy, a to bez omezení počtu vydaných časových razítek po celou dobu trvání Smlouvy.

9. Vera se zavazuje poskytovat Objednateli podporu zaručenou platnou Politikou.

10. Vera se zavazuje poskytovat službu vydávání časových razítek s dostupností 95% za kalendářní den v nepřetržitém režimu 24 hodin denně 7 dní v týdnu (365 x 24) po celou dobu trvání Smlouvy.

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

12. Vera se zavazuje poskytovat službu vydávání časových razítek s propustností 1 ks časových razítek za sekundu. Maximální jednorázová doba nedostupnosti služby činí 10 dnů za rok, plánované odstávky systému časové autority mohou probíhat v noci, o víkendech, svátcích, případně i v době od 07:00 do 18:00 běžného pracovního dne. Počet plánovaných odstávek za kalendářní měsíc není omezen.

Článek V.
Smluvní cenové podmínky

1. Cena za poskytování služby I.CA QVerify, tj. za ověření platnosti elektronických podpisů a pečetí, bude pro Objednatele stanovena podle celkového agregovaného počtu provedených a poskytnutých ověření odebraných Poskytovatelem od I.CA v daném kalendářním měsíci podle příslušného objemového pásma.
   Objednatel obdrží měsíčně aktualizovaný údaj o počtu svých skutečně odebraných ověření, jejich jednotkovou cenu v dosaženém objemovém pásmu a z toho odvozenou cenu celkovou[1], určenou jako součin „Ceny za 1 ověření (Kč bez DPH)“ a počtu skutečně provedených a poskytnutých ověření Objednatelem v příslušném pásmu za kalendářní měsíc uvedeném ve faktuře.
   K ceně bude připočtena DPH podle aktuálně platných předpisů.

Pásmo celkového počtu Poskytovatelem provedených a od I.CA poskytnutých ověření ks/měsíc	**Cena za 1 ověření (Kč bez DPH)**	**Cena za 1 ověření (Kč s DPH 21 %)**
do 100		
101 - 200		
201 - 300		
301 - 500		
501 - 1.000		
1.001 - 3.000		
3.001 - 5.000		
5.001 - 10.000		
10.001 - 50.000		
50.001 - 100.000		
100.001 - 300.000		
300.001 - 500.000		
500.001 - 1.000.000		
1.000.001 - 1.500.000		
1.500.001 - 2.500.000		
2.500.001 - 3.500.000		
3.500.001 - 5.000.000		
5.000.001 - 10.000.000		
nad 10.000.001		

[1] Vera bude tedy poskytovat službu I.CA QVerify (a analogicky též I.CA RemoteSeal a TSA) pro řadu svých zákazníků najednou, čímž dosáhne vyššího (a tedy finančně výhodnějšího) cenového pásma, než když by si každý zákazník Vera pořizoval službu jednotlivě a odebíral nižší počty jednotek definovaných služeb.

2. Cena za poskytování služby I.CA RemoteSeal, tj. za vytvoření kvalifikované elektronické pečetě na dálku, bude pro Objednatele stanovena podle celkového agregovaného počtu vytvořených kvalifikovaných elektronických pečetí odebraných Poskytovatelem od I.CA v daném kalendářním měsíci podle příslušného objemového pásma.
   Objednatel obdrží měsíčně aktualizovaný údaj o počtu svých odebraných pečetí, jejich jednotkovou cenu v dosaženém objemovém pásmu a z toho odvozenou cenu celkovou, určenou jako součin „Ceny za 1 ks pečetění (Kč bez DPH)“ a počtu Objednatelem skutečně vytvořených kvalifikovaných elektronických pečetí v příslušném pásmu za kalendářní měsíc uvedeném ve faktuře.
   K ceně bude připočtena DPH podle aktuálně platných předpisů.

Pásmo počtu pečetění (ks) od - do za měsíc odebraných Poskytovatelem od I.CA	**Cena za 1 ks pečetění (Kč bez DPH)**	**Cena za 1 ks pečetění (Kč s DPH 21 %)**
1 - 100		
101 - 300		
301 - 500		
501 - 1.000		
1.001 - 3.000		
3.001 - 5.000		
5.001 - 10.000		
10.001 - 30.000		
30.001 - 50.000		
50.001 - 100.000		
100.001 - 300.000		
300.001 - 500.000		
500.001 - 1.000.000		
1.000.001 - 5.000.000		
5.000.001 - 10.000.000		

Výlučně ve spojení s pečetěním I.CA RemoteSeal je současně možno dokument digitálně orazítkovat. Cena za tuto verzi časového razítka bude pro Objednatele stanovena podle celkového agregovaného počtu těchto odebraných časových razítek odebraných Poskytovatelem od I.CA v daném kalendářním měsíci podle příslušného objemového pásma. Objednatel obdrží měsíčně aktualizovaný údaj o počtu svých skutečně odebraných časových razítek odebraných v průběhu pečetění, jejich jednotkovou cenu v dosaženém objemovém pásmu a z toho odvozenou cenu celkovou, určenou jako součin „Ceny za jedno časové razítko (Kč bez DPH)“ a počtu Objednatelem skutečně odebraných časových razítek za kalendářní měsíc uvedeném ve faktuře.

K ceně bude připočtena DPH podle aktuálně platných předpisů.

Pásmo počtu Poskytovatelem od I.CA odebraných časových razítek k pečetím ks/měsíc	**Cena za jedno časové razítko (Kč bez DPH**	**Cena za jedno časové razítko (Kč s DPH 21 %)**
0 až 100		
101 až 200		
201 až 500		
501 až 1.000		

1.001 až 2.000		
2.001 až 5.000		
5.001 až 7.500		
7.501 až 10.000		
10.001 až 20.000		
20.001 až 30.000		
30.001 až 50.000		
50.001 až 100.000		
100.001 až 200.000		
200.001 až 300.000		
300.001 až 400.000		
400.001 až 500.000		
500.001 až 1.000.000		

3. Cena za vydání standardních časových razítek bude stanovena jako součin „Ceny za jedno časové razítko (Kč bez DPH)“ a počtu skutečně odebraných časových razítek za kalendářní měsíc uvedeném ve faktuře.
   Objednatel tedy obdrží měsíčně aktualizovaný údaj o počtu svých skutečně odebraných časových razítek, jejich jednotkovou cenu a z toho odvozenou cenu celkovou.
   K ceně bude připočtena DPH podle aktuálně platných předpisů.

Cena za jedno TSA (Kč bez DPH)	**Cena za jedno TSA (Kč s DPH 21%)**

4. Ceny uvedené v odst. 1., 2. a 3. tohoto článku jsou cenami nejvýše přípustnými a zahrnují veškeré náklady související s poskytováním služby. Ceny mohou být změněny pouze v souvislosti se změnou daňových předpisů týkajících se DPH, a to nejvýše o částku odpovídající této legislativní změně, nebo pouze v souvislosti se změnou cenové politiky I.CA.

5. Úhrada poskytování služby I.CA QVerify bude prováděna vždy jednou měsíčně zpětně za uplynulý kalendářní měsíc, v němž I.CA elektronické podpisy pečetě ověřila, a to podle počtu skutečně provedených a poskytnutých ověření. Daňový doklad bude obsahovat počet skutečně provedených a poskytnutých ověření. DPH bude vyjádřeno dle aktuálně platné legislativy.

6. Úhrada poskytování služby I.CA RemoteSeal (případně včetně souvisejících časových razítek) bude prováděna vždy jednou měsíčně zpětně za uplynulý kalendářní měsíc, v němž I.CA vytvořila kvalifikované elektronické pečetě na dálku, a to podle počtu skutečně provedených a poskytnutých vytvořených pečetí. Daňový doklad bude obsahovat počet skutečně vytvořených pečetí (případně též časových razítek). DPH bude vyjádřeno dle aktuálně platné legislativy.

7. Úhrada vydaných časových razítek podle této Smlouvy bude prováděna vždy jednou měsíčně zpětně za uplynulý kalendářní měsíc, v němž I.CA časová razítka vydala, a to podle počtu Objednatelem skutečně odebraných časových razítek. Daňový doklad bude obsahovat počet skutečně odebraných časových razítek. DPH bude vyjádřeno dle aktuálně platné legislativy.

8. Vera je povinna vystavit řádný daňový doklad do 15. dne kalendářního měsíce následujícího po kalendářním měsíci, za který je účtována cena za poskytování služby.

9. Objednatel je povinen uhradit daňové doklady převodem na účet Vera do 30 dnů ode dne doručení daňového dokladu Objednateli. Faktury v elektronické podobě je Vera povinna zasílat Objednateli do datové schránky (id: hcpbx62).

Článek VI.
Sankční ustanovení, odstoupení od smlouvy

1. V případě zaviněného nedodržení parametru SLA dostupnosti služby I.CA QVerify uvedeného v článku IV. odstavci 2. této Smlouvy, tj. pokud dostupnost služby klesne vinou Vera pod 98 % za kalendářní den, je Vera povinna uhradit Objednateli smluvní pokutu ve výši 5.000,- Kč bez DPH za každých započatých 0,1%, o kterých klesne dostupnost poskytované služby pod požadovanou hodnotu (počítáno za kalendářní den s tím, že příslušné průběžné výpočty v případě incidentů Vera předkládá vždy měsíčně zpětně). Měsíční výše smluvní pokuty však nepřesáhne dvojnásobek měsíční ceny za poskytování služby.
2. V případě zaviněného nedodržení parametru SLA dostupnosti služby I.CA RemoteSeal uvedeného v článku IV. odstavci 5. této Smlouvy, tj. pokud dostupnost služby klesne pod 99,5 % za kalendářní den, je Vera povinna uhradit Objednateli smluvní pokutu ve výši 1.000,- Kč bez DPH za každých započatých 0,1%, o kterých klesne dostupnost poskytované služby pod požadovanou hodnotu. Měsíční výše smluvní pokuty však nepřesáhne výši měsíční ceny za poskytování služby.

3. Při nezaplacení ceny za vydaná časová razítka ve lhůtě tvořené součtem doby splatnosti příslušného daňového dokladu a časového období 30 dnů, tj. ve lhůtě 60 dnů od doručení daňového dokladu Objednateli, vyhrazuje si Vera právo nepřijímat od Objednatele další žádosti na vydávání časových razítek a pečetí podle této Smlouvy, a to do doby vyrovnání všech finančních závazků ze strany Objednatele.

4. Každá ze smluvních stran má právo odstoupit od této Smlouvy v případě, poruší-li jedna ze smluvních stran své závazky a povinnosti stanovené touto Smlouvou, a to podstatným nebo opakovaným způsobem. Odstoupení musí mít písemnou formu s uvedením důvodů odstoupení a musí být doručeno druhé smluvní straně, jinak je odstoupení neplatné. Odstoupení od Smlouvy má právní účinky dnem doručení. Od toho dne nesmí smluvní strana, které takto bylo odstoupení doručeno, pokračovat v plnění předmětu Smlouvy vyjma případů, kdy by nečinností hrozila újma na jmění druhé smluvní strany. V takovém případě má smluvní strana za povinnost pokračovat v plnění Smlouvy a zabezpečit předmět Smlouvy takovým způsobem, aby bylo odstraněno nebezpečí shora uvedené újmy na jmění. Odstoupení od smlouvy se řídí § 2001 a násl. Občanského zákoníku.

Článek VII.
Závěrečná ustanovení, termín a místo plnění smlouvy

1. Objednatel s ohledem na ustanovení § 41 zákona č. 128/2000 Sb., o obcích, ve znění pozdějších předpisů, uvádí, že uzavření této Smlouvy za podmínek v ní obsažených bylo schváleno následujícím jednáním:
   Splnění podmínky: schváleno na 29. jednání Rady města Přeštice

   Identifikace dokumentu: usnesením č. 666/2019

   Datum: 21.10.2019

2. Tato Smlouva a vztahy z ní vyplývající se řídí českým právním řádem. Veškeré spory vyplývající z této Smlouvy se smluvní strany budou snažit řešit smírnou cestou. Teprve nepovede-li takové smírčí jednání k vyřešení sporu, bude soudní spor veden u příslušného obecného soudu ČR.

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

4. V případě, že by se některá ustanovení Smlouvy stala neplatnými v důsledku legislativních změn, nestává se neplatnou celá Smlouva. V takovém případě sjednají smluvní strany nové znění dotčených ustanovení tak, aby vystihovalo co nejpřesněji podstatu původního ujednání a aby co nejlépe odpovídalo duchu Smlouvy.

5. Tato Smlouva je uzavřena dnem jejího podpisu oběma smluvními stranami. Účinnosti tato Smlouva nabývá dnem jejího uveřejnění Objednatelem v Registru smluv dle zák. č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (dále jen „Registr smluv“).
6. Tato Smlouva se uzavírá na dobu neurčitou.

7. Místem plnění Smlouvy je sídlo Objednatele.

8. Smlouvu je možné ukončit:
   a) písemnou dohodou smluvních stran;
   b) písemnou výpovědí některé ze smluvních stran, zaslanou druhé smluvní straně, a to buď výpovědí s důvodem, kterým je podstatné porušení ustanovení této Smlouvy druhou smluvní stranou, nebo výpovědí bez uvedení důvodu. V obou případech se uplatní výpovědní doba v délce 30 kalendářních dnů počínající běžet prvním dnem měsíce následujícího po dni, kdy bylo písemné vyhotovení výpovědi prokazatelně doručeno druhé smluvní straně.

9. Písemnou dohodou smluvních stran je Smlouva ukončena ke dni v této dohodě uvedenému a není-li v dohodě takový den uveden, pak ke dni podpisu dohody oběma smluvními stranami.

10. Ukončením Smlouvy nejsou smluvní strany zbaveny povinnosti vyrovnat veškeré závazky vzniklé v důsledku platnosti a účinnosti této Smlouvy a učinit veškeré úkony, které nesnesou odkladu a které jsou nutné k zabránění vzniku škody jedné ze smluvních stran.

11. Smluvní strany se dohodly, že se ve vztazích mezi smluvními stranami vyplývajících z této Smlouvy neuplatní §§ 1895 – 1900 zák. č. 89/2012 Sb., občanského zákoníku.

12. Tato Smlouva může být změněna dohodou obou smluvních stran. Dohoda o změně Smlouvy nebo o jejím zrušení musí mít písemnou formu označenou jako vzestupně číslované dodatky a musí být podepsána oprávněnými zástupci obou smluvních stran.

13. Smluvní strany mohou zveřejnit ve svých informačních materiálech, že I.CA je poskytovatelem služeb I.CA QVerify, I.CA RemoteSeal a časových razítek pro Objednatele.

14. Smlouva je vyhotovena ve dvou vyhotoveních, z nichž každá smluvní strana obdrží po jednom vyhotovení.

15. V návaznosti na výše ujednané, smluvní strany prohlašují, že skutečnosti uvedené v této Smlouvě nepovažují ani za obchodní tajemství ani za důvěrné informace a udělují svolení k jejich užití, uveřejnění do Registru smluv či jejímu zveřejnění na internetových stránkách www.prestice-mesto.cz, a to bez stanovení jakýchkoliv omezení či podmínek.

16. Seznam příloh, které tvoří nedílnou součást Smlouvy:

    Příloha č. 1 – Popis služby I.CA QVerify.

    Příloha č. 2 – Popis služby I.CA RemoteSeal

    Příloha č. 3 – Vzor emailové zprávy nebo protokolu o požadavku zavedení klienta přeprodejce k odběru TSA nebo ATSA + Nastavení prostředí TSA

V Praze dne 31.10.2019

Za Poskytovatele: Vera, spol. s r.o.

_____

VERA, spol. s r.o.

V Přešticích dne 6.11.2019

Za Objednatele: město Přeštice

_____

Mgr. Karel Naxera, starosta

město Přeštice

Příloha č. 1

Popis služby I.CA QVerify

Východisko služby:

Nařízení Evropského parlamentu a Rady č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (eIDAS), konkrétně články 32, 33 a 40.

Nařízení:

a) stanoví podmínky, za nichž členské státy uznávají prostředky pro elektronickou identifikaci fyzických a právnických osob, které spadají do oznámeného systému schématu elektronické identifikace jiného členského státu;
b) stanoví pravidla pro služby vytvářející důvěru;
c) stanoví právní rámec pro elektronické podpisy, elektronické značky, elektronická časová razítka, elektronické dokumenty, služby registrovaného elektronického doručování a certifikační služby pro autentizaci internetových stránek.

Jednou ze služeb vytvářejících důvěru, která může být poskytována pouze kvalifikovaným poskytovatelem služeb vytvářejících důvěru (dle minulé terminologie akreditovaným poskytovatelem certifikačních služeb, I.CA), je kvalifikovaná služba ověřování platnosti elektronických podpisů a pečetí I.CA QVerifyTL (také „I.CA QVerify“) (čl. 32, 33 a 40 eIDAS), tedy ověřování platnosti zaručených elektronických podpisů založených na kvalifikovaném certifikátu pro elektronický podpis, kvalifikovaných elektronických podpisů, kvalifikovaných elektronických pečetí a zaručených elektronických pečetí založených na kvalifikovaném certifikátu pro elektronickou pečeť.).

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.

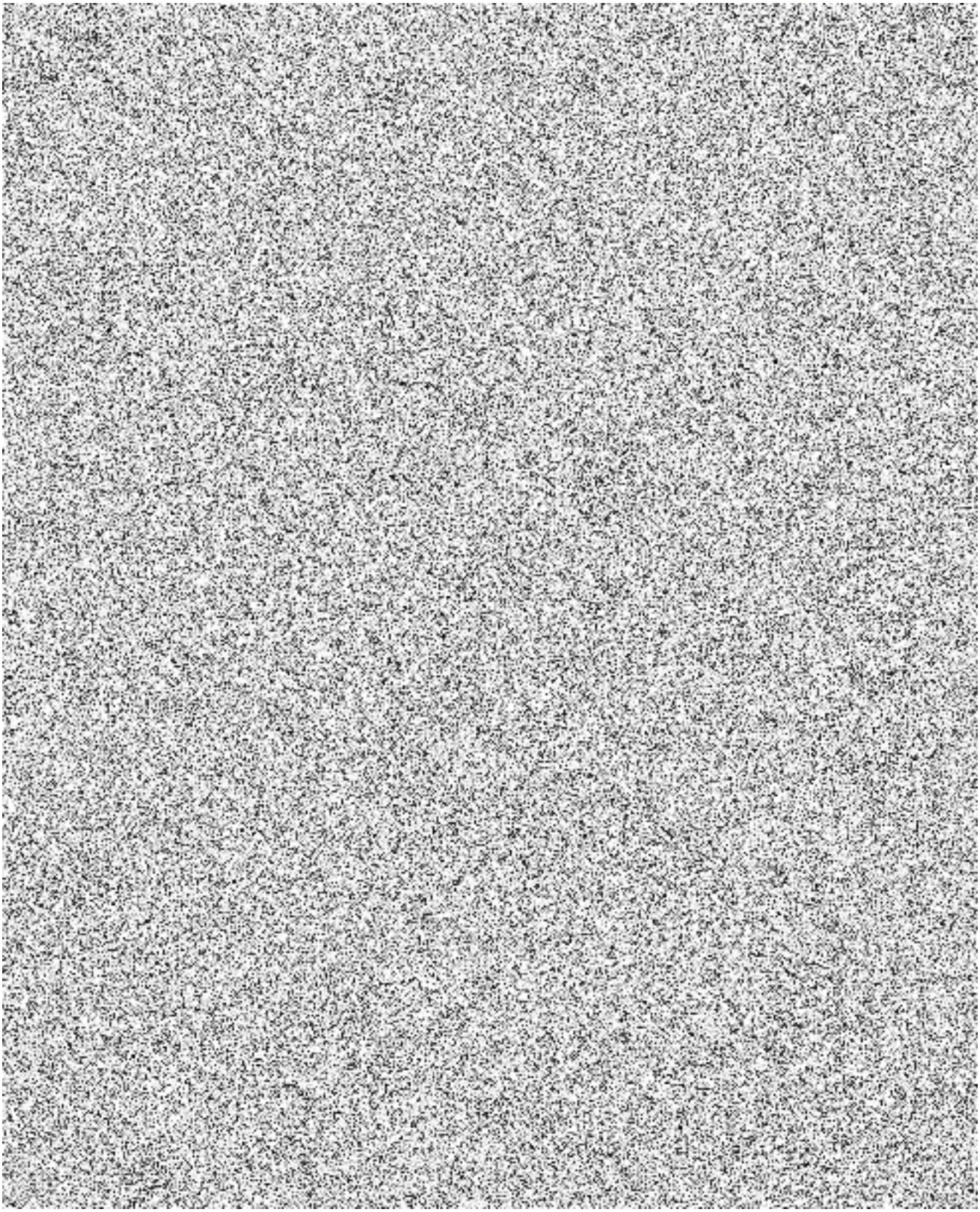
Veřejnoprávní původci mají povinnost ověřování definovanou §4 odst. 4-7 vyhlášky č. 259/2012 Sb., o podrobnostech výkonu spisové služby.

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:

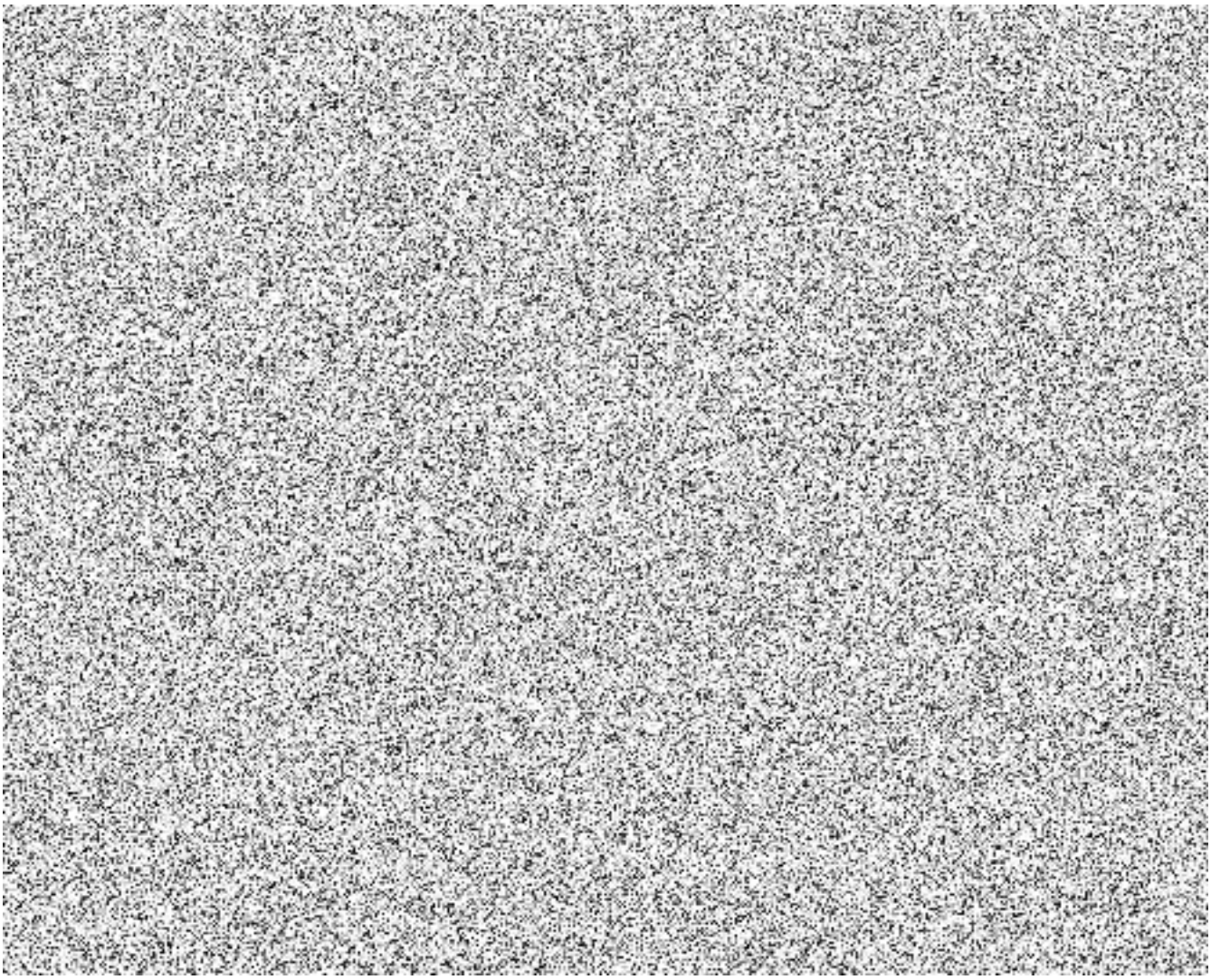
„V případě kvalifikovaného poskytovatele služeb vytvářejících důvěru se úmysl nebo nedbalost předpokládá, pokud daný kvalifikovaný poskytovatel služeb vytvářejících důvěru neprokáže, že škoda podle prvního pododstavce nastala bez jeho úmyslu nebo nedbalosti.“

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 daných technickými normami, na něž se eIDAS odkazuje. Postupy a vlastní fungování služby ověřování elektronického podpisu tak bylo prověřeno nezávislými experty subjektu posuzování shody, Českým institutem pro akreditaci (nejvyšší orgán v ČR pro tuto oblast) a Ministerstvem vnitra ČR jako gesčním orgánem pro oblast eIDAS v ČR.

Příslušný certifikát I.CA:



Podle eIDAS zveřejňuje Ministerstvo vnitra ČR seznam kvalifikovaných poskytovatelů a kvalifikovaných služeb vytvářejících důvěru na webové stránce:
http://www.mvcr.cz/clanek/seznam-kvalifikovanych-poskytovatelu-sluzeb-vytvarejicich-duveru-a-poskytovanych-kvalifikovanych-sluzeb-vytvarejicich-duveru.aspx



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

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

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

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

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

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

1. je jednoznačně spojen s podepisující osobou,

2. umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě,
3. byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou,
4. je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat (§2 odst. b) ZoEP).

V přechodném 2-letém období daném zákonem č. 297/2016 Sb. neověřuje služba I.CA QVerify platnost elektronických značek založených na (kvalifikovaných) systémových certifikátech. Důvodem je skutečnost, že elektronické značky nebyly definovány Směrnicí 1999/93, tudíž nejsou do eIDAS převzaty. Služba I.CA QVerify tak nemohla být auditována jako kvalifikovaná služba dle eIDAS.

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

Stručný popis (manažerské shrnutí):
Služba je koncipována jako komponenta pro ověření platnosti podpisu instalovaná v prostředí klienta a volaná obvykle spisovou službou. Služba ověření podpisu pracuje s dokumenty ve standardních a legislativně podporovaných formátech PAdES a CAdES B-B a B-T (CAdES v interní i externí verzi) a XAdES B-B a B-T[2]. Výstupem je stav ověření (platný/neplatný podpis, nelze ověřit, důvod, proč nelze ověřit nebo proč je podpis neplatný), čas, ke kterému se ověřovalo, zdroj času (čas obdržení požadavku, časové razítko, parametr zadaný uživatelem, data, na základě kterých bylo ověření provedeno, legislativní typ podpisu, zda je certifikát na QESigCD). Ověření má charakter elektronicky podepsané XML odpovědi v definované struktuře, vhodné pro automatizované zpracování. Současně jsou ukládána data pro následné generování PDF protokolu v případě požadavku klienta (generuje I.CA). Jeho účelem je potvrdit výsledek ověření elektronického podpisu i v lidsky čitelné formě v případě požadavku klienta např. před soudem.

Podrobný popis:
Služba podporuje ověření dokumentu ve standardních a legislativně podporovaných formátech:

- PAdES B-B a B-T
- CAdES B-B a B-T (v interní i externí verzi)
- XAdES B-B a B-T.

Časový okamžik, ke kterému je možné platnost podpisu ověřit:
Služba umožní vybrat[3], k jakému času má ověřování proběhnout (v sestupném pořadí):

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

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

[2] Prováděcí rozhodnutí Komise (EU) č. 2015/1506.
[3] Lze ponechat jako parametrické či definovat jednu z možností.

Kompletní ověření je prováděno na serveru v prostředí I.CA. Pomocí komponenty I.CA[4] 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 certifikát I.CA)
3. Výpočet hashe z podepsaných dat, získání podpisové struktury
4. Zaslání dat k ověření ze strany klienta na server I.CA
5. Provedení vstupních kontrol
6. Provedení ověření jednotlivých podpisů (tj. dvojic podpisová struktura + hash)
7. Sestavení odpovědi s výsledkem ověření - XML elektronicky podepsaná datová struktura (zasílaná on-line)
8. Uložení dat pro následné generování PDF protokolu s výsledkem ověření v prostředí I.CA
9. Předání výsledku ověření v XML struktuře aplikaci klienta
10. Zalogování procesu ověření
11. Záznam do STAT o využití služby
12. Konec zpracování.

Výstupem služby je:
Stav ověření:

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

Stav ověření má charakter:

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

Omezující podmínky:

a) Ověřuje se platnost podpisu či podpisů v daném dokumentu. PDF protokol i XML data budou obsahovat tabulkovou strukturu vážící se k jednomu podpisu a struktur bude tolik, kolik bude v dokumentu podpisů (PDF/XML protokol je vždy jeden pro jeden dokument)[5].
b) Ověřovány jsou podpisy založené na certifikátech vydaných všemi důvěryhodnými poskytovateli zemí EU (EUTL, LoTL).

[4] 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.
[5] Viz příklad v příloze.

c) Ověřovány budou i podpisy založené na již expirovaných certifikátech, a to i tehdy, pokud je v dokumentu již expirované časové razítko. To znamená, že ověření takového podpisu nebude odmítnuto, ale ověření proběhne s výsledkem, že podpis je neplatný a bude standardně vystaven protokol o ověření.
d) Časová razítka jsou vydávána časovou autoritou I.CA.

Podporované platformy - klientská komponenta.
Klientská komponenta je realizována v Javě 32b a 64b a .NET.

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

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

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:

www.ICA.cz

PROTOKOL Č. 23794699

O OVĚŘENÍ PLATNOSTI KVALIFIKOVANÉHO ELEKTRONICKÉHO PODPISU A PEČETĚ

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

PODPIS 1

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

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

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

PODPIS 2

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

První certifikační autorita, a. s. je zapsána v obchodním rejstříku, vedeném u Městského soudu v Praze. Den zápisu: 12. 3. 2001,
Spisová značka: oddíl B., vložka 7136. IČ: 26 43 93 95 DIČ: CZ26439395 [redacted]

Stránka 1 z 2

Příloha č. 2

Služba vytváření kvalifikovaných elektronických pečetí na dálku I.CA RemoteSeal

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 bod 52 recitálu, články 29 a 39, body 3 a 4 Přílohy II a Příloha III.

Právní základ

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

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

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

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

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

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

Existují dva typy QSealCD:

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

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

Seznam EU pro QSealCD

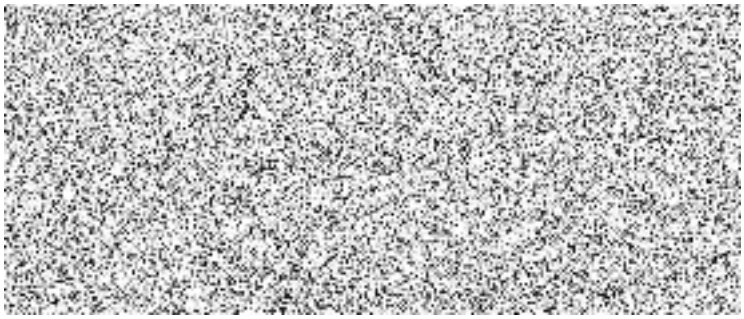
„Compilation of Member States notification on SSCDs and QSCDs“
https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds

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

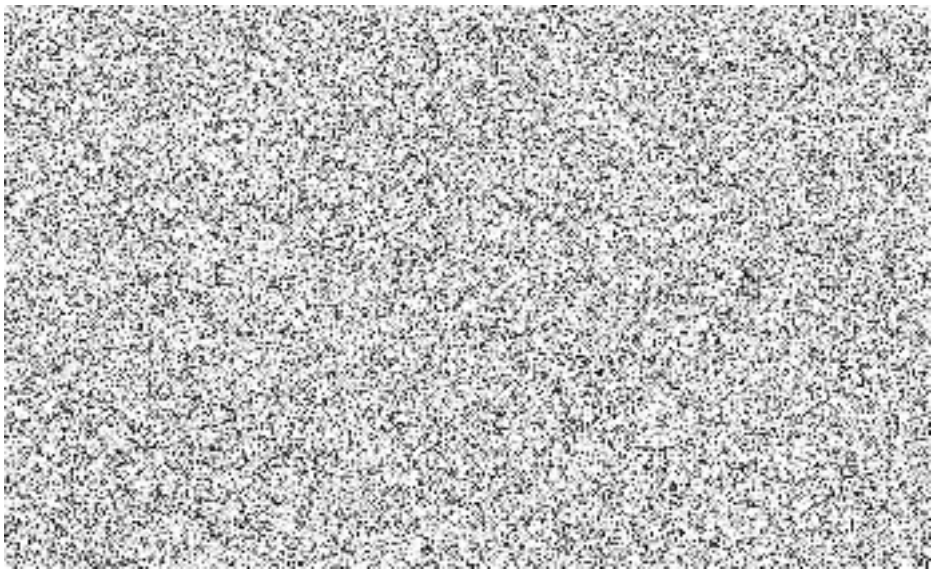
Výběr QSealCD pro službu I.CA RemoteSeal

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

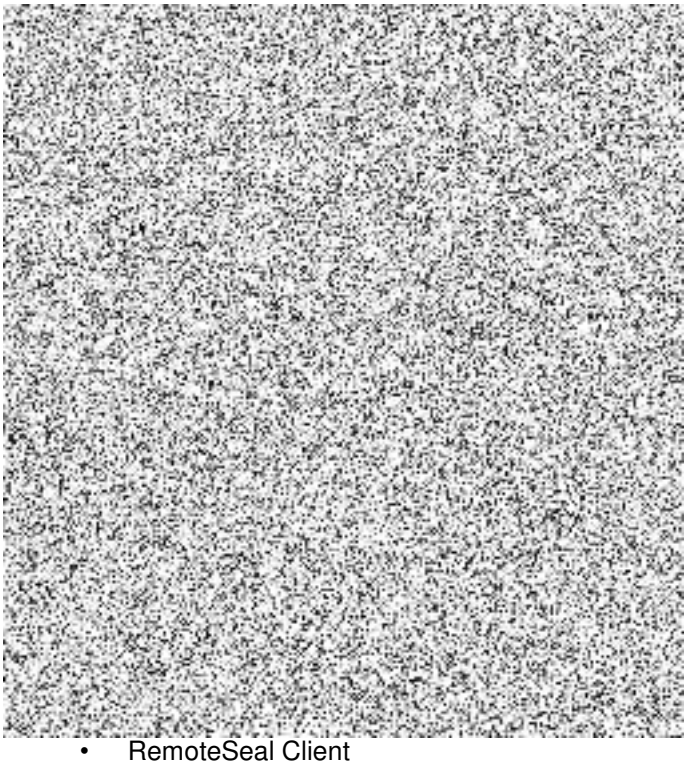
List of QSCDs	
Name:	-
Name:	**ARX CoSign v8.2**
Applicant	ARX (Algorithmic Research, Ltd.)
Qualified Signature Creation Device (QSigCD)	yes IMPORTANT NOTE: Device aimed to be managed on behalf of the user (signatory) by a QTSP that can be only considered as QSigCD when duly operated by a QTSP in accordance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



Architektura služby



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



- RemoteSeal Client
- Klientská komponenta sloužící k zadávání transakcí (požadavků na opečetění dat) do systému RemoteSeal.

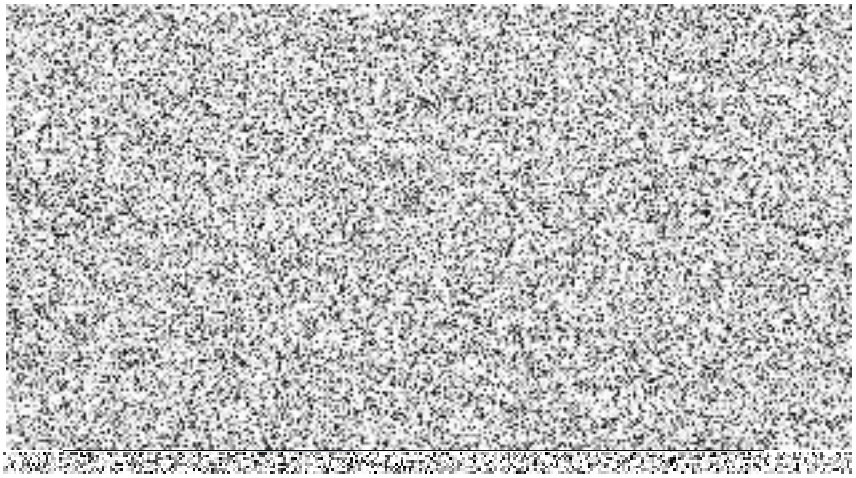
- Nativní C++ jádro
- Distribuováno ve formě:
- JAR pro Java
- .NET assembly pro .NET
- V případě zájmu možno volat přímo nativní jádro.

Zřízení služby

Zřízení služby bude probíhat na vybraných pobočkách RA následujícím způsobem:

- Klient navštíví pobočku registrační autority (RA).
- Operátor RA vydá klientovi prvotní autentizační komerční certifikát (**FAC** - First Authentication Certificate) na aktivační kartu/token (viz názvosloví). FAC je nutné zavést do AUTHu jako autentizační certifikát pro RemoteSeal pro daného uživatele (budou provádět ručně obchodníci na základě SN certifikátu, které jim zašle klient).
- Operátor RA připraví žádost o pečetící certifikát pro uživatele.
- Operátor RA vygeneruje párová data pro pečetící certifikát (z pohledu operátora atomická operace) což obnáší:
    - ICARA pomocí **RSeS** (RemoteSealServer) založí pro klienta uživatele na DSA včetně prvotního hesla **FP** (First Password).
    - ICARA náhodně vygeneruje nové heslo **PP** (Production Password) (drženo pouze v RAM)
    - ICARA náhodně vygeneruje 256b AES šifrovací klíč **SK** (Secret Key)
    - ICARA zašifruje pomocí AES-KW (kde **K** je **SK** a **PP** je **W**) do výsledku **CPP** (Ciphered Production Password)
    - ICARA zašifruje pomocí RSAES_PKCS#1 v1.5 klíč **SK** veřejným klíčem **FAC** do výsledku $\mathbf{CSK_{FAC}}$ (Ciphered Secret Key)
    - ICARA následně uloží do RSeS kryptogramy $\mathbf{CSK_{FAC}}$ a **CPP**
    - ICARA provede aktivaci uživatelského účtu v DSA pomocí FP (a tudíž i změnu hesla na PP).
    - ICARA provede pod účtem uživatele (s heslem PP) generování párových dat pro vydání prvotního pečetícího certifikátu.
- Operátor RA pomocí ICARA podepíše žádost o vydání pečetícího certifikátu privátním klíče párových dat na DSA (zde můžeme teoreticky zapojit uživatele, aby zadal PIN na pinpadové čtečce (pro rozšifrování **CPP** pomocí privátního klíče **FAC**)
- Na základě žádosti proběhne na CA vydání pečetícího certifikátu.
- Pečetící certifikát:
    - CA pošle na mailovou adresu uživatele.
    - ICARA uloží na čipovou kartu uživatele.
    - ICARA uloží na DSA (díky přihlášení jako uživatel)
- Klient odchází z RA s aktivační(m) kartou/tokenem.

Aktivace RSeC



- Pro aktivaci RSeC spustí uživatel (např.: oprávněná osoba úřadu) dodávanou GUI utilitu RSeActivationUtil (dále jen utilita)
- Utilita vyzve uživatele k vložení aktivační karty (potažmo aktivačního tokenu), načež utilita:
    - Naváže spojení s RSeS pomocí oboustranně autentizovaného HTTPS za pomoci **FAC** (uživatel bude vyzván k zadání PINu)
    - Automaticky vytvoří žádost o vydání následného certifikátu **SACi** (Secondary Authentication Certificate číslo i), která bude podepsána **FAC** a privátní klíč k **SACi** se bude generovat v SW (nikoliv na kartě)
    - Žádost se odešle ke zpracování na CA, kde se obratem vydá následný certitifikát **SACi** a ten se stáhne zpět do utility
    - Utilita si z RSeS stáhne $\mathbf{CSK_{FAC}}$ (drží se pouze v RAM)
    - Pomocí privátního klíče **FAC** na aktivační kartě dešifruje $\mathbf{CSK_{FAC}}$ na **SK** (drží se pouze v RAM)
    - Zašifruje pomocí RSAES_PKCS#1 v1.5 klíč **SK** veřejným klíčem **SACi** do výsledku $\mathbf{CSK_{SACi}}$
    - Utilita následně uloží do RSeS kryptogram $\mathbf{CSK_{SACi}}$
- Utilita může případně uživatele vyzvat k dalším nastavením RSeC, pokud nějaká budou (např.: přidávání TS, viditelný podpis, reason, location pokud se tyto nebudou nastavovat pomocí RSeCAPI)
- Následně utilita vytvoří aktivační soubor, kde bude uložen certifikát **SACi** včetně privátního klíče.
- Uživatel tento aktivační soubor následně načte do spisové služby (obecně do aplikace volající RSeC), která jej bude pro použití RemoteSeal předávat do RSeC.

Technické parametry RSeActivationUtil

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

Opečetění dokumentu

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

Automatické prodloužení služby

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

Obnova pečetícího certifikátu

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

Podporované formáty podpisu:

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

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 99,5% a kapacitou až 60 ověření za minutu.

Příloha č. 3

Vzor emailové zprávy nebo protokolu o požadavku zavedení klienta přeprodejce k odběru TSA nebo ATSA

Název přeprodejce: …….

Název klienta: ..... (Organizace, OSVČ, Fyzická osoba)

Služba: ..... (TSA nebo ATSA, či obojí)

Způsob autentizace: ..... (Komerčním certifikátem I.CA nebo jméno heslo)

- ad1) Sériové číslo certifikátu ..... (dekadický nebo hexadecimální tvar)
- ad2) Autentizace jménem a heslem
    - Jméno ..... (min. 8 znaků bez diaktriky)
    - Heslo ..... (min. 8 znaků bez diaktriky)

Email nebo zprávu vždy poslat na kontaktní osobu I.CA, která zajistí zavedení klienta do systému I.CA. Zavedení do systému trvá vždy min. jednu hodinu.

Nastavení prostředí TSA

Ostré/produkční TSA

produkční služba	**autorizace**	**typ spojení**	**URL**
TSA	certifikátem	neanonymní HTTPS	https://tsa.ica.cz/cgi-bin/razitko.cgi
TSA	jménem a heslem	neanonymní HTTPS	https://tsabase.ica.cz/cgi-bin/razitko_base.cgi
TSA	jménem a heslem	HTTP	http://tsabase.ica.cz/cgi-bin/razitko_base.cgi

OID politika	1.3.6.1.4.1.23624.10.1.50.1.0

Pokud nemáte nainstalovány všechny relevantní kořenové certifikáty, (root certifikáty, certifikát serveru TS), nainstalujte si je pomocí aplikace I.CA Rootman (http://www.ica.cz/Korenove-certifikaty).