Smlouva

o poskytování kvalifikované služby ověřování platnosti kvalifikovaných elektronických podpisů a pečetí

I.CA QVerifyTL

Číslo smlouvy objednatele: 1615 / 23 / 16 / SIS

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

První certifikační autorita, a.s.

Se sídlem:	Praha 9, Podvinný mlýn 2178/6, PSČ 190 00
Zastoupená:	Ing. Petrem Budišem, Ph.D., MBA, předsedou představenstva a Ing. Romanem Kučerou, členem představenstva
IČO:	26439395
DIČ:	CZ26439395
Bankovní spojení:	Československá obchodní banka, a.s.
Číslo účtu:	168457418/0300

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

(dále též „**I.CA**“ nebo „**Poskytovatel**“)

a

Fakultní nemocnice Plzeň

se sídlem	Plzeň – Bory, Edvarda Beneše 1128/13, PSČ 301 00
zastoupená:	MUDr. Václavem Šimánkem, ředitelem
IČO:	00669806
DIČ:	CZ00669806
Bankovní spojení:	ČNB
Číslo účtu:	33739311/0710

(dále též „**Objednatel**“)

(dále jednotlivě také jako **„Strana“** a společně také jako „**Strany**“)

uzavírají níže uvedeného dne, měsíce a roku tuto Smlouvu o poskytování kvalifikované služby ověřování platnosti kvalifikovaných elektronických podpisů a pečetí I.CA QVerifyTL (dále jen „Smlouva“).

Článek I.
Preambule

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

Článek II.
Předmět smlouvy

1. Předmětem plnění této smlouvy je zajištění provozu kvalifikované služby ověřování platnosti kvalifikovaných elektronických podpisů a pečetí v souladu s platnou Politikou kvalifikované služby ověřování platnosti kvalifikovaných elektronických podpisů a pečetí, která je vždy v aktuální verzi k dispozici na www.ica.cz. Obchodní označení služby je I.CA QVerify.

Článek III.
Povinnosti objednatele

1. I.CA poskytuje kvalifikovanou službu ověřování platnosti kvalifikovaných 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“). Veškeré změny a doplňky této Politiky jsou vůči objednateli účinné po podpisu dodatku k této smlouvě podepsaného zástupci obou smluvních stran.

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

3. Objednatel se zavazuje neposkytovat plnění poskytnuté I.CA dalším osobám bez souhlasu I.CA a nezneužívat poskytování služeb I.CA.

Článek IV.
Povinnosti I.CA

1. I.CA poskytuje objednateli Kvalifikovanou službu ověřování platnosti kvalifikovaných elektronických podpisů a pečetí (dále též „I.CA QVerify“ či „I.CA QVerifyTL“) 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. I.CA se zavazuje poskytovat službu I.CA QVerify v režimu 24/7, tedy 24 hodin denně, 7 dní v týdnu, s SLA 99,95 % a kapacitou až 500 ověření za minutu. I.CA se dále zavazuje vyhodnocovat dodržování

SLA 99,95% a v případě porušení SLA předkládat objednateli výsledky vyhodnocení spolu s daňovým dokladem a dodacím listem.

3. I.CA se zavazuje poskytovat:

   a) technickou podporu při provozu služby, řešení nestandardních situací a poradenství související s předmětem této smlouvy prostřednictvím e-mailové adresy verify@ica.cz a telefonní linky 284 081 930.
   b) Hotline v rozsahu Po – Pá 8:00 – 17:00 hod. na výše uvedených kontaktech a provozní pohotovost služby v režimu 24/7 na telefonním čísle 731 657 586.
   c) právní a technickou aktuálnost komponenty pro zajištění komunikace s I.CA, jakož i celou službu I.CA QVerify, s relevantními právními a technickými předpisy a normami v návaznosti na eIDAS.
   d) 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% a kapacita 60 ověření za minutu.

4. I.CA 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.

Článek V.
Smluvní cenové podmínky

1. Cena za poskytování služby I.CA QVerify, tj. za ověření platnosti kvalifikovaných elektronických podpisů a pečetí, bude stanovena podle počtu provedených a poskytnutých ověření v daném kalendářním měsíci podle příslušného objemového pásma, a to jako součin „Ceny za 1 ověření Kč bez DPH“ a počtu skutečně provedených a poskytnutých ověření za kalendářní měsíc. K ceně bude připočteno DPH podle aktuálně platných předpisů.

   SLA 99,95 a propustnost 500 ověření/min.
   Nedostupnost 0,1825 dne, tj. 262,8 min = 4 hod 22 min 48 s.

   Cena za 1 ověření je 5,20 Kč bez DPH, tedy 6,292 Kč s DPH ve výši 21%

2. Cena uvedená v odst. 1. tohoto článku je cenou neměnnou, nejvýše přípustnou a zahrnuje veškeré náklady I.CA související s poskytováním služby I.CA QVerify. Cena může být změněna pouze v souvislosti se změnou daňových předpisů týkající se DPH, a to nejvýše o částku odpovídající této legislativní změně.

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

provedených a poskytnutých ověření; cena bude stanovena jako součin „Ceny za 1 ověření Kč bez DPH“ a počtu skutečně provedených a poskytnutých ověření. DPH bude vyjádřeno dle aktuálně platné legislativy.

4. I.CA je povinna vystavit řádný daňový doklad do 15. dne kalendářního měsíce následujícího po kalendářním měsíci, za který je účtována cena za poskytování služby I.CA QVerify.

5. Objednatel je povinen uhradit daňové doklady převodem na účet I.CA do 30 dnů ode dne doručení daňového dokladu, vystaveného I.CA, na adresu sídla objednatele a doručeného písemně na adresu sídla objednatele podle údajů v této Smlouvě.

6. Daňový doklad musí mít náležitosti daňových a účetních dokladů stanovených platnými a účinnými právními předpisy. Objednatel je oprávněn daňový doklad, který nebude splňovat náležitosti podle platných a účinných 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 objednatel neocitá v prodlení. Lhůta splatnosti počíná běžet znovu od opětovného doručení náležitě doplněného či opraveného daňového dokladu.

Článek VI.
Sankční ustanovení, odstoupení od smlouvy

1. V případě zaviněného nedodržení parametru SLA dostupnosti služby I.CA QVerify uvedeného v článku IV. odstavci 1. této Smlouvy, tj. pokud dostupnost služby klesne pod 99,95% za kalendářní den, je I.CA 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). Měsíční výše smluvní pokuty však nepřesáhne dvojnásobek měsíční ceny za poskytování služby.

2. V případě nesplnění povinností uvedených v článku IV. odstavci 3. písm. a) a b) této Smlouvy je I.CA povinna uhradit objednateli smluvní pokutu ve výši 5.000,- Kč bez DPH za každé takové porušení.

3. V případě nesplnění povinností uvedených v článku IV. odstavci 3. písm. c) tohoto ujednání je I.CA povinna uhradit objednateli smluvní pokutu ve výši 10.000,- Kč bez DPH za každé takové porušení.

4. V případě nesprávného vyhodnocení platnosti podpisu ze správných vstupních dat je I.CA povinna uhradit objednateli smluvní pokutu ve výši 10.000,- Kč bez DPH za každé takové porušení, avšak pouze v případě, že data nutná k ověření (která se odesílají do prostředí I.CA), generovaná komponentou dodanou I.CA, nebyla jakkoliv pozměněna a nebylo s nimi nijak manipulováno. Tím není dotčeno právo objednatele na náhradu případné újmy na jmění.

5. 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. 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.

2. 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.

3. 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.

4. Tato Smlouva nabývá platnosti a účinnosti dnem jejího podpisu oběma smluvními stranami.

5. Tato Smlouva se uzavírá na dobu určitou od 1.1.2024 do 31.12.2024. Účinnosti nabývá dnem zveřejnění v registru smluv.

6. Místem plnění Smlouvy je sídlo objednatele.

7. 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 následujícím po dni, kdy bylo písemné vyhotovení výpovědi prokazatelně doručeno druhé smluvní straně.

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

9. 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 na straně jedné ze smluvních stran.

10. Smluvní strany se dohodly, že se ve vztazích mezi I.CA a objednatelem vyplývajících z této Smlouvy neuplatní §§ 1895 – 1900 zák. č. 89/2012 Sb., občanského zákoníku.

11. 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.

12. Smluvní strany mohou zveřejnit ve svých informačních materiálech, že I.CA je poskytovatelem služby I.CA QVerify pro objednatele.

13. Tato Smlouva je vyhotovena ve dvou vyhotoveních, z nichž obě smluvní strany obdrží po jednom vyhotovení.

14. Seznam příloh, které tvoří nedílnou součást této smlouvy:

    a) Příloha č. 1 – Popis služby QVerify.

V Praze dne ……

Za poskytovatele:

……..
Ing. Petr Budiš, Ph.D., MBA
předseda představenstva

……..
Ing. Roman Kučera
člen představenstva

V Plzni dne …….

Za objednatele:

……
MUDr. Václav Šimánek, Ph.D.
ředitel

Příloha č. 1

Popis kvalifikované služby ověřování platnosti uznávaných/kvalifikovaných elektronických podpisů/pečetí
I.CA QVerifyTL

Východisko služby:

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

Nařízení:

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

b) stanoví pravidla pro služby vytvářející důvěru;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1. je jednoznačně spojen s podepisující osobou,

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

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

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

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

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

Podrobný popis:

Služba podporuje ověření dokumentu ve standardních a legislativně podporovaných formátech:

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

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

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

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

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

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

lze pokračovat na ověřování razítek.

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

Časový okamžik, ke kterému je možné platnost podpisu ověřit:

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

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

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

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

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

Základní postup ověření:

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

Výstupem služby je:

Stav ověření:

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

Stav ověření má charakter:

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

Omezující podmínky:

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

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

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.

[4] Viz příklad v příloze.

Příklad PDF protokolu:

CERTIFICATION AUTHORITY

www.ICA.cz

PROTOKOL Č. 23794699

O OVĚŘENÍ PLATNOSTI KVALIFIKOVANÉHO ELEKTRONICKÉHO PODPISU A PEČETĚ

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

PODPIS 1

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

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

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

PODPIS 2

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