č. 12012001/02.

Dodatek č. 2

k Ujednání o zřízení a provozu mobilních registračních autorit ČSSZ pro vydávání kvalifikovaných a komerčních certifikátů a o poskytování služeb I.CA a zapůjčení potřebného HW a SW vybavení ze dne 6. 1. 2012

(dále jen „Dodatek č. 2")

První certifikační autorita, a.s.

Se sídlem: Praha 9, Podvinný mlýn 2178/6, PSČ 190 00
Zastoupená: [redacted] předsedou představenstva
[redacted] členem představenstva
IČ: 264 39 395
DIČ: CZ26439395
Bankovní spojení: Československá obchodní banka, a.s.
Číslo účtu: [redacted]
zapsaná v obchodním rejstříku, vedeném Městským soudem v Praze, spisová značka B, vložka 7136.

(dále též „**I.CA**")

a

Česká republika - Česká správa sociálního zabezpečení

Se sídlem: Praha 5, Křížová 25, PSČ 225 08
Zastoupená: JUDr. Jiřím Biskupem, ústředním ředitelem
IČ: 00006963
DIČ: neplátce
Bankovní spojení: Česká národní banka
Číslo účtu: [redacted]

(dále též „**ČSSZ**")

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

uzavírají níže uvedeného dne, měsíce a roku tento Dodatek č. 2 k Ujednání o zřízení a provozu mobilních registračních autorit ČSSZ pro vydávání kvalifikovaných a komerčních certifikátů a o poskytování služeb I.CA a zapůjčení potřebného HW a SW vybavení uzavřeného mezi Stranami dne 6. 1. 2012, ve znění jeho Dodatku č. 1 uzavřeného mezi Stranami dne 24. 2. 2016 (dále jen „Ujednání").

Preambule

Strany podpisem tohoto Dodatku č. 2 upřesňují Ujednání o podmínky využití **Kvalifikované služby ověřování platnosti kvalifikovaných a uznávaných elektronických podpisů a kvalifikovaných elektronických pečetí,** jak je níže v tomto Dodatku č. 2 uvedeno.

I.

1. Strany se dohodly na tom, že za dosavadní odst. 4) článku II. Ujednání s názvem **Další specifikace předmětu činnosti a zapůjčení HW a SW vybavení** se vkládá nový odstavec 5), který zní takto:

   5) I.CA poskytuje ČSSZ Kvalifikovanou službu ověřování platnosti kvalifikovaných a uznávaných elektronických podpisů a kvalifikovaných elektronických pečetí (dále též „I.CA Verify") 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. 11 tohoto ujednání.

2. Strany se dále dohodly na tom, že za dosavadní odst. 5) článku IV. Ujednání s názvem **Práva a povinnosti I.CA** se vkládají nové odst. 6) ,7) a 8), které znějí takto:

   6) I.CA se zavazuje poskytovat službu I.CA Verify 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 denně vyhodnocovat dodržování SLA 99,95% a jedenkrát měsíčně předkládat ČSSZ výsledky vyhodnocení spolu s daňovým dokladem a dodacím listem. Pro účely sankcí uvedených v článku X. odst. 1) je vyhodnocován každý kalendářní den zvlášť.

   7) 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 [redacted] a telefonní linky [redacted]
      b) Hotline v rozsahu Po – Pá 8:00 – 17:00 hod. na výše uvedených kontaktech a provozní pohotovost služby v režimu 24/7 na telefonním čísle [redacted]
      c) právní a technickou aktuálnost komponenty pro zajištění komunikace s I.CA, jakož i celou službu I.CA Verify, s relevantními právními a technickými předpisy a normami v návaznosti na eIDAS.
      d) za účelem otestování nových verzí služby I.CA Verify před nasazením do ostrého provozu službu I.CA Verify v testovacím prostředí s funkcionalitou obdobnou službě I.CA Verify v ostrém prostředí, tj. PDF/XML protokol, stejné formáty ověřovaných podpisů; pro testovací prostředí platí SLA 99% a kapacita 60 ověření za minutu.

   8) 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 ČSSZ 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.

3. Strany se dále dohodly na tom, že za dosavadní článek **VIII. Podmínky vydávání SSL certifikátů** Ujednání se vkládá nový článek **IX.** s názvem **Cenové podmínky poskytování služby I.CA Verify**, který zní takto:

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

Pásmo počtu provedených a poskytnutých ověření ks/měsíc	Cena za 1 ověření Kč bez DPH	Cena za 1 ověření Kč s DPH ve výši 21%
do 10 000	5,20	6,292
10 001-50 000	2,60	3,146
50 001-100 000	1,95	2,360
100 001 – 300 000	1,56	1,888
300 001 – 500 000	1,30	1,573
500 001 – 1 000 000	1,04	1,258
1 000 001 – 1 500 000	0,975	1,180
1 500 001 – 2 500 000	0,91	1,101
2 500 001 – 3 500 000	0,845	1,022
3 500 001 – 5 000 000	0,715	0,865
5 000 001 – 10 000 000	0,52	0,629
nad 10 000 001	0,39	0,472

2) Ceny uvedené v odst. 1. tohoto článku jsou cenami neměnnými, nejvýše přípustnými a zahrnují veškeré náklady I.CA související s poskytováním služby I.CA Verify. Ceny mohou být změněny 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 Verify bude prováděna vždy jednou měsíčně zpětně za uplynulý kalendářní měsíc, v němž I.CA kvalifikované a uznávané elektronické podpisy a kvalifikované elektronické 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 v příslušném pásmu za kalendářní měsíc dle rozpisu uvedeného v odst. 1. tohoto článku. 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 Verify.

5) ČSSZ je povinna uhradit daňové doklady převodem na účet I.CA do 30 dnů ode dne doručení daňového dokladu, vystaveného I.CA, na adresu sídla ČSSZ a doručeného písemně na adresu sídla ČSSZ podle údajů v tomto ujednání.

6) Daňový doklad musí mít náležitosti daňových a účetních dokladů stanovených platnými a účinnými právními předpisy. ČSSZ je oprávněna 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 ČSSZ neocitá v prodlení. Lhůta splatnosti počíná běžet znovu od opětovného doručení náležitě doplněného či opraveného daňového dokladu.

4. Strany se dále dohodly na tom, že za nový článek **IX.** Ujednání s názvem **Cenové podmínky poskytování služby I.CA Verify** se vkládá nový článek **X.** Ujednání s názvem **Sankční ustanovení**, který zní takto:

„X.
Sankční ustanovení

1) V případě zaviněného nedodržení parametru SLA dostupnosti služby I.CA Verify uvedeného v článku IV. odstavci 6. tohoto ujednání, tj. pokud dostupnost služby klesne pod 99,95% za kalendářní den, je I.CA povinna uhradit ČSSZ 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 I.CA předkládá vždy měsíčně zpětně). Měsíční výše smluvní pokuty však nepřesáhne dvojnásobek měsíční ceny za poskytování služby.

2) V případě nesplnění povinností uvedených v článku IV. odstavci 7. písm. a) a b) tohoto ujednání je I.CA povinna uhradit ČSSZ smluvní pokutu ve výši 5.000,- Kč bez DPH za každé takové porušení.

3) V případě nesplnění povinností uvedených v článku IV. odstavci 7. písm. c) tohoto ujednání je I.CA povinna uhradit ČSSZ smluvní pokutu ve výši 100.000,- Kč bez DPH za každé takové porušení.

4) V případě nesprávného vyhodnocení platnosti podpisu ze správných vstupních dat je I.CA povinna uhradit ČSSZ smluvní pokutu ve výši 100.000,- 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 ČSSZ na náhradu případné újmy na jmění.".

5. Strany se dále dohodly na tom, že dosavadní článek **IX.** Ujednání s názvem **Závěrečná ustanovení** se nově označuje jako článek **XI.** s názvem **Závěrečná ustanovení**, a nově zní takto:

„XI.
Závěrečná ustanovení

1) Nedílnou součástí tohoto ujednání jsou:
   a) Příloha č. 1 – Technické, procesní a bezpečnostní požadavky
   b) Příloha č. 2 – Plná moc (vzor)
   c) Příloha č. 3 – CPQC, CPQSC a PSQRA
   d) Příloha č. 4 – CPKC a PSKRA
   e) Příloha č. 5 – Rozsah a forma součinnosti při provozování Registrační autority

f) Příloha č. 6 – Prohlášení pověřené osoby (vzor)
g) Příloha č. 7 – Přehled umístění Registračních autorit ČSSZ (RA ČSSZ)
h) Příloha č. 8 – Certifikační politika pro SSL certifikáty
i) Příloha č. 9 - Potvrzení o zaměstnaneckém poměru – plná moc
j) Příloha č. 10 - Informace a postup získání SSL certifikátu
k) Příloha č. 11 – Popis Kvalifikované služby ověřování platnosti kvalifikovaných a uznávaných elektronických podpisů a kvalifikovaných elektronických pečetí."

6. Strany se dohodly na tom, že dosavadní přílohy č. 1 až č. 10 Ujednání se doplňují o novou přílohu, a to o přílohu č. 11 s názvem Popis Kvalifikované služby ověřování platnosti kvalifikovaných a uznávaných elektronických podpisů a kvalifikovaných elektronických pečetí.

II.

1. Ostatní ujednání Ujednání zůstávají tímto Dodatkem č. 2 nedotčena.

2. Tento Dodatek č. 2 nabývá platnosti a účinnosti dnem jeho podpisu Stranami.

3. Tento Dodatek č. 2 je vyhotoven v pěti (5) vyhotoveních v českém jazyce s platností originálu, z nichž dvě (2) vyhotovení obdrží I.CA a tři (3) vyhotovení obdrží ČSSZ.

4. Nedílnou součástí tohoto Dodatku č. 2 je nová příloha č. 11 Ujednání, tedy:

   - Příloha č. 11 – Popis Kvalifikované služby ověřování platnosti kvalifikovaných a uznávaných elektronických podpisů a kvalifikovaných elektronických pečetí.

5. Strany se s tímto Dodatkem č. 2 důkladně seznámily a prohlašují, že jeho textu porozuměly a na důkaz své svobodné a určité vůle připojují níže své podpisy.

V Praze dne 12/7/2016

První certifikační autorita, a.s.

[redacted]

předseda představenstva

[redacted]

člen představenstva

CERTIFICATION AUTHORITY

První certifikační autorita, a.s.
Podvinný mlýn 2178/6, 190 00 Praha 9
IČ: 26439395 (880)

V Praze dne 25 -07- 2016

Česká republika -
Česká správa sociálního zabezpečení

[redacted]

JUDr. Jiří Biskup
ústřední ředitel

Příloha č. 11

Popis Kvalifikované služby ověřování platnosti kvalifikovaných a uznávaných elektronických podpisů a kvalifikovaných elektronických pečetí

Východisko služby:
Nařízení Evropského parlamentu a Rady č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (eIDAS), konkrétně článků 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 současné terminologie akreditovaným poskytovatelem certifikačních služeb, I.CA), je kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů (čl. 32 a 33 Nařízení).

Vzhledem k tomu, že Návrh zákona o službách vytvářejících důvěru pro elektronické transakce (tzv. Adaptační zákon) zavádí 2leté 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 Verify rozšířena oproti požadavkům eIDAS i o ověřování platnosti uznávaného elektronického podpisu.

Dále s odkazem na to, že kvalifikované elektronické pečetě mohu být vydávány kvalifikovanými poskytovateli služeb vytvářejících důvěru až po nastavení systému auditu ze strany Českého institutu pro akreditaci, provedení auditu a zařazení na seznam služeb vytvářejících důvěru, nebude v této fázi služba I.CA Verify moci ověřovat kvalifikované elektronické pečetě. Tato služba bude o ověřování kvalifikovaných elektronických pečetí rozšířena bezprostředně poté, co první kvalifikovaný poskytovatel služeb vytvářejících důvěru zahájí na území České republiky vydávání kvalifikovaných certifikátů pro elektronické pečetě.

V přechodném 2letém období daném Adaptačním zákonem služba I.CA Verify nebude ověřovat platnost elektronických značek založených na kvalifikovaných systémových certifikátech. Důvodem je skutečnost, že elektronické značky nebyly definovány Směrnicí 1999/93, tudíž nejsou do eIDAS přejaty. Služba I.CA Verify tak nemůže být auditována jako kvalifikovaná služba.

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 a webová služba pro ověření platnosti podpisu. Služba ověření podpisu pracuje s dokumenty ve standardních a legislativně podporovaných formátech PAdES a CAdES B-Level a T-Level (CAdES v interní i externí verzi) a XAdES B-Level a T-Level[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). Ověření má charakter elektronicky podepsaného PDF protokolu s připojeným časovým razítkem a XML odpovědi

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

v definované struktuře, vhodné pro automatizované zpracování. XML odpověď je také elektronicky podepsána.

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

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

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 času zadanému ČSSZ (k času, kdy bylo podání přijato do interního systému ČSSZ; parametr předávaný ČSSZ)
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 bude poskytována jako rozdělená mezi klienta a server.

Kompletní ověření bude prováděno na serveru v prostředí I.CA. Pomocí komponenty I.CA[3] umístěné a volané z prostředí ČSSZ 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 ČSSZ.

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 ČSSZ na server I.CA
5. Provedení vstupních kontrol
6. Provedení ověření jednotlivých podpisů (tj. dvojic podpisová struktura + hash)
7. Sestavení odpovědi s výsledkem ověření. Dle vstupního parametru služby:
    a. PDF elektronicky podepsaný protokol s připojeným časovým razítkem (generován v nočních hodinách, k dispozici pro autentizované stažení do prostředí ČSSZ)
    b. 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 ČSSZ
10. Zalogování procesu ověření
11. Záznam do STAT o využití služby
12. Konec zpracování.

Pro kontrolu integrity odesílaných dat z prostředí ČSSZ a dat přijatých v prostředí I.CA použije 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.

Výstupem služby je:

[2] Lze ponechat jako parametrické či definovat jednu z možností.
[3] Komponenta mimo parsování podpisu a zajištění potřebných dat pro ověření zajišťuje komunikaci s interním systémem I.CA; za její aktuálnost (právní i technickou) a integritu odpovídá I.CA. Komponenta neumožňuje komunikaci s jiným poskytovatelem než I.CA.

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)
- hash ověřovaných dat.

Stav ověření má charakter:

1. PDF elektronicky podepsaného protokolu s připojeným časovým razítkem. Protokol bude ve výstupním datovém formátu PDF/A verze 1b. Protokol bude možné si stáhnout na vyhrazeném autentizovaném URL, a to od 07:00 následující den (generování, zpracování a uložení proběhne v nočních hodinách).
2. Odpovědi v definované struktuře (xml data), vhodné pro automatizované zpracování. Odpověď bude elektronicky podepsána a zasílána automaticky on-line.

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

Omezující podmínky:

a) Ověřuje se platnost podpisu či podpisů v daném dokumentu. Protokol i XML data budou obsahovat tabulkovou strukturu vážící se k jednomu podpisu a struktur bude tolik, kolik bude v dokumentu podpisů (protokol/XML data je vždy jeden pro dokument)[4].
b) Ověřovány budou podpisy založené na certifikátech vydaných I.CA, PostSignum a eIdentity. Certifikáty zahraničních poskytovatelů ověřovány budou dle požadavků ČSSZ (placená služba rozšíření).
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 budou vydána časovou autoritou I.CA.

Podporované platformy - klientská komponenta.
Klientská komponenta bude realizována v Javě 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.

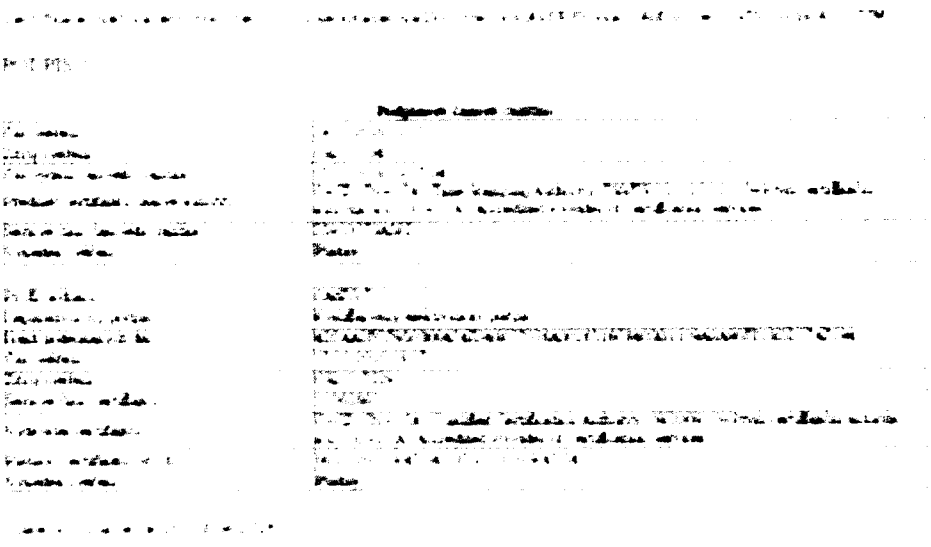
Dostupnost:

- Služba bude poskytována v režimu 24/7 s SLA 99,95% a kapacitou až 500 ověření za minutu.

[4] Návrh viz příloha. Definitivní podoba protokolu bude definována normou EN 319 102-2 Procedury pro vytvoření a ověření elektronického podpisu, část 2: formát výsledku ověření. Prozatím není k dispozici.

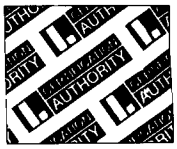
- Prokazatelnost odpovědnosti (I.CA vůči ČSSZ): bude zalogován hash dat, která byla ověřována, a ten bude i součástí vydaného a elektronicky podepsaného protokolu.
- Nepopiratelnost odpovědnosti (I.CA vůči ČSSZ): elektronicky podepsaný protokol s výsledkem ověření.

Příloha – příklad PDF protokolu



Příloha – příklad XML protokolu


```
<?xml version="1.0" encoding="UTF-8"?>
<ICASignatureVerificationReport version="2.0">
        <ReportMetadata>
                <Generated>2016-04-15T05:58:45Z</Generated>
                <ServiceVersion>1</ServiceVersion>
                <ServiceProfile>ICA_verify_v1</ServiceProfile>
        </ReportMetadata>
        <ReportID>40</ReportID>
        <UserNotice>Tento protokol je vydán pro testovací účely</UserNotice>
        <FileName>C:\Data\a\PAdES-BES bez razítka\03 Gorniak QSCD ENISA.pdf</FileName>
        <Signatures>
                <Signature>
                        <SignedData>
                                <SignatureName>PAdES-BES_1</SignatureName>
                                <SignedDataDigest algorithm="2.16.840.1.101.3.4.2.1">XUhYmLz8fs1aitMv/dC9FJ1TJQOsleM3oH8cAg44=</SignedDataDigest>
                        </SignedData>
                        <SignatureStandard>PAdES-BES</SignatureStandard>
                        <LegalStatus>Advanced Electronic Signature based on Qualified Certificate electronic signature</LegalStatus>
                        <VerifyTime>2016-04-09T05:52:50Z</VerifyTime>
                        <ValidationData>
                                <Certificate sn="11045444" issuer="C=CZ,CN=I.CA - Qualified Certification Authority, 09/2009,O=První certifikační autorita, a.s.,OU=I.CA - Accredited Provider of Certification Services" />
                                <Certificate sn="10500000" issuer="C=CZ,CN=I.CA - Qualified Certification Authority, 09/2009,O=První certifikační autorita, a.s.,OU=I.CA - Accredited Provider of Certification Services" />
                                <CRL crlNumber="7092" issuer="C=CZ,CN=I.CA - Qualified Certification Authority, 09/2009,O=První certifikační autorita, a.s.,OU=I.CA - Accredited Provider of Certification Services" />
                        </ValidationData>
                        <SignerCertificate>
                                <SN>11045444</SN>
                                <Subject>C=CZ,CN=Ing.[redacted]O=První certifikační autorita, a.s.,title=Obchodní ředitel segmentu veřejná správa,serialNumber=ICA - 10222243</Subject>
                                <NotBefore>2015-07-24T14:56:25Z</NotBefore>
                                <NotAfter>2016-07-23T14:56:25Z</NotAfter>
                                <Issuer>C=CZ,CN=I.CA - Qualified Certification Authority, 09/2009,O=První certifikační autorita, a.s.,OU=I.CA - Accredited Provider of Certification Services</Issuer>
                        </SignerCertificate>
                        <VerifyResult>
                                <Result>VALID</Result>
                        </VerifyResult>
                </Signature>
        </Signatures>
</ICASignatureVerificationReport>
```


AUTHORITY