Č. 120120001103

Dodatek č. 3

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. 3")

První certifikační autorita, a.s.

Se sídlem: Praha 9, Podvinný mlýn 2178/6, PSČ 190 00
Zastoupená: [redacted] předsedou představenstva
[redacted] členem představenstva
IČ: 26439395
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. 3 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 a Dodatku č. 2 uzavřeného mezi Stranami dne 25. 7. 2016 (dále jen „Ujednání").

Preambule

Strany podpisem tohoto Dodatku č. 3 upřesňují Ujednání o technické podmínky ukládání PDF protokolů **Kvalifikované služby ověřování platnosti kvalifikovaných a uznávaných elektronických podpisů a kvalifikovaných elektronických pečetí** a předání příslušných dat o ověření, jak je níže v tomto Dodatku č. 3 uvedeno.

[redacted]

I.

1. Strany se dohodly na tom, že za dosavadní odst. 8) článku IV. Ujednání s názvem **Práva a povinnosti I.CA** se vkládají nové odst. 9) až 11), které znějí takto:

   9) I.CA se zavazuje ukládat data, na jejichž základě bylo provedeno ověření platnosti elektronického podpisu a elektronické pečetě, a která byla ve formě xml protokolu on-line odeslána ČSSZ, bezpečným a důvěryhodným způsobem po celou dobu trvání skartačních lhůt dle požadavků ČSSZ, a to pro účely budoucího generování PDF verze protokolu o ověření. V případě ukončení smluvního vztahu předá I.CA všechna uložená data na vhodném paměťovém médiu ČSSZ.

   10) Na základě požadavku oprávněné osoby ČSSZ se I.CA zavazuje podle jednoznačného čísla xml protokolu vyhledat příslušná předmětná data a vygenerovat na jejich základě PDF verzi protokolu o ověření. Tento protokol je I.CA povinna předat ČSSZ ve lhůtě 48 hodin od převzetí požadavku v pracovních dnech. V případě, že se v době 48 hodin vyskytne den pracovního klidu či svátek, prodlužuje se lhůta o tyto dny.

   11) Oprávněnými osobami ČSSZ podle předchozího odstavce jsou:
   [redacted] e-mail: [redacted] tel: [redacted]
   [redacted] e-mail: [redacted] tel: [redacted]
   [redacted] e-mail: [redacted] tel: [redacted]
   Všichni ID datové schránky: 49kaiq3.

II.

2. Strany se dále dohodly na tom, že za dosavadní odst. 4) článku X. Ujednání s názvem **Sankční ustanovení** se vkládají nové odst. 5) a 6), které znějí takto:

   5) V případě nesplnění povinnosti uvedené v článku IV. odstavci 9. tohoto ujednání je I.CA povinna uhradit ČSSZ smluvní pokutu ve výši 10.000,- Kč bez DPH za každé takové porušení.

   6) V případě nesplnění povinnosti uvedené v článku IV. odstavci 10. tohoto ujednání je I.CA povinna uhradit ČSSZ smluvní pokutu ve výši 10.000,- Kč bez DPH za každé takové porušení.

III.

3. Strany se dohodly na tom, že dosavadní Příloha č. 11 s názvem **Popis Kvalifikované služby ověřování platnosti kvalifikovaných a uznávaných elektronických podpisů a kvalifikovaných elektronických pečetí** se nahrazuje novým zněním Přílohy č. 11 s názvem **Popis Kvalifikované služby ověřování platnosti kvalifikovaných a uznávaných elektronických podpisů a kvalifikovaných elektronických pečetí**, a nově zní takto:

[redacted]

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.

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 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:

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

- 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 ve formě XML elektronicky podepsané datové struktury
8. Uložení dat pro následné generování PDF protokolu s výsledkem ověření v prostředí I.CA na základě požadavku oprávněné osoby ČSSZ
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:
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.

[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 má charakter:

1. Odpovědi v definované struktuře (xml data), vhodné pro automatizované zpracování. Odpověď bude elektronicky podepsána a zasílána automaticky on-line.
2. PDF elektronicky podepsaného protokolu s připojeným časovým razítkem. Protokol bude ve výstupním datovém formátu PDF/A verze 1b vygenerován na základě požadavku ČSSZ (po sdělení jednoznačného čísla/identifikátoru protokolu) z uložených předmětných dat a předán ČSSZ ze strany I.CA do 48 hodin v pracovních dnech.

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. O ověřování certifikátů zahraničních kvalifikovaných poskytovatelů zemí EU bude služba postupně rozšířena.
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.
- 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.

[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.

Příloha – certifikát kvalifikované služby

Certificate no.: PCEB 17/02/01

.com
ensure your certification

Certification body TAYLLOR & COX PCEB
established by TAYLLOR & COX s.r.o. auditing, inspection and testing institute
hereby awards this certificate to the company

První certifikační autorita, a.s.

Identification No.: 264 39 395
Podvinný mlýn 2178/6
CZ 190 00, Praha 9 – Libeň, Czech Republic

to confirm that its qualified trust service

QVerify, version 1.1

for validation of qualified electronic signatures and qualified electronic seals is in accordance with:

Regulation (EU) No 910/2014 of the European Parliament and of the Council, Article 5., Article 13., Article 15., Article 19., Article 24., Article 32., Article 33 and Article 40.

This certificate is issued in accordance with certification scheme requirements defined by standard ČSN ETSI EN 319 403 v2.2.2 in conjunction with DKP v2.

Date of the certification: 2017-02-07
This certificate is valid until: 2019-02-06

[redacted]
Head of Certification body

V 3239

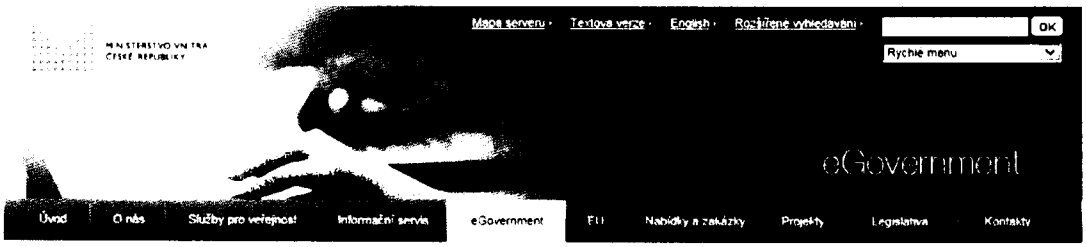
Place and date of issue of the certificate: Prague, 2017-02-07

The certificate was issued by TAYLLOR & COX PCEB, established by TAYLLOR & COX s.r.o.
Na Florenci 1055/35, Staré Město Praha 1, CZ 110 00, [redacted] www.tcox.cz
To check this certificate validity please call the phone number: [redacted]
Member of: TAYLLORCOX UK Ltd. 75 King William St., EC4N, London, UK

[redacted]

Příloha – seznam kvalifikovaných poskytovatelů

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



POVINNĚ ZVEŘEJŇOVANÉ INFORMACE

Seznam kvalifikovaných poskytovatelů služeb vytvářejících důvěru a poskytovaných kvalifikovaných služeb vytvářejících důvěru

Číslo	Poskytovatelé certifikačních služeb	Kvalifikované služby	Zahájení poskytování
1	První certifikační autorita, a. s.		
2	Česká pošta, s. p.		
3	eIdentity a. s.		

Policie ČR

Hasiči ČR

Státní služba

Registr smluv

CENTRUM PROTI TERORISMU A HYBRIDNÍM HROZBÁM

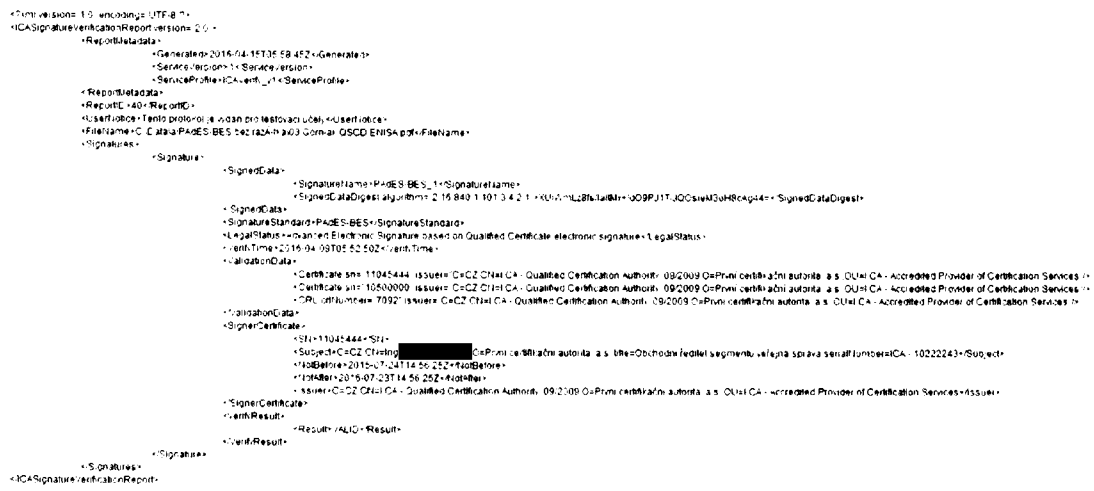
PRŮMYSLOVÉ ZÓNY A BEZPEČNOST

Příloha – příklad PDF protokolu

PROTOKOL č. 191

O OVĚŘENÍ PLATNOSTI KVALIFIKOVANÉHO ELEKTRONICKÉHO PODPISU

Příloha – příklad XML protokolu



IV.

1. Ostatní ujednání Ujednání zůstávají tímto Dodatkem č. 3 nedotčena.

2. Tento Dodatek č. 3 nabývá platnosti dnem jeho podpisu Stranami a účinnosti dne 1. 7. 2017.

3. Tento Dodatek č. 3 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. Strany se s tímto Dodatkem č. 3 důkladně seznámily a prohlašují, že jeho textu porozuměly a na důkaz své svobodné a určité vůle připojují níže své podpisy.

V Praze dne 19/6/2017

První certifikační autorita, a.s.

[redacted]

předseda představenstva

[redacted]

člen představenstva

V Praze dne 26-06-2017

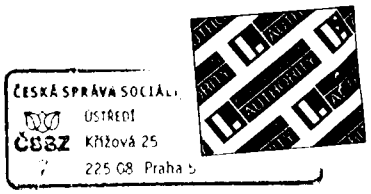
Česká republika -
Česká správa sociálního zabezpečení

[redacted]

JUDr. Jiří Biskup
ústřední ředitel

ČESKÁ SPRÁVA SOCIÁLNÍHO ZABEZPEČENÍ

I. CERTIFICATION AUTHORITY
První certifikační autorita, a.s.
Podvinný mlýn 2178/6, 190 00 Praha 9
[redacted]26439395
880


ČESKÁ SPRÁVA SOCIÁL
ČSSZ
ÚSTŘEDÍ
Křižová 25
225 08 Praha 5