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 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.

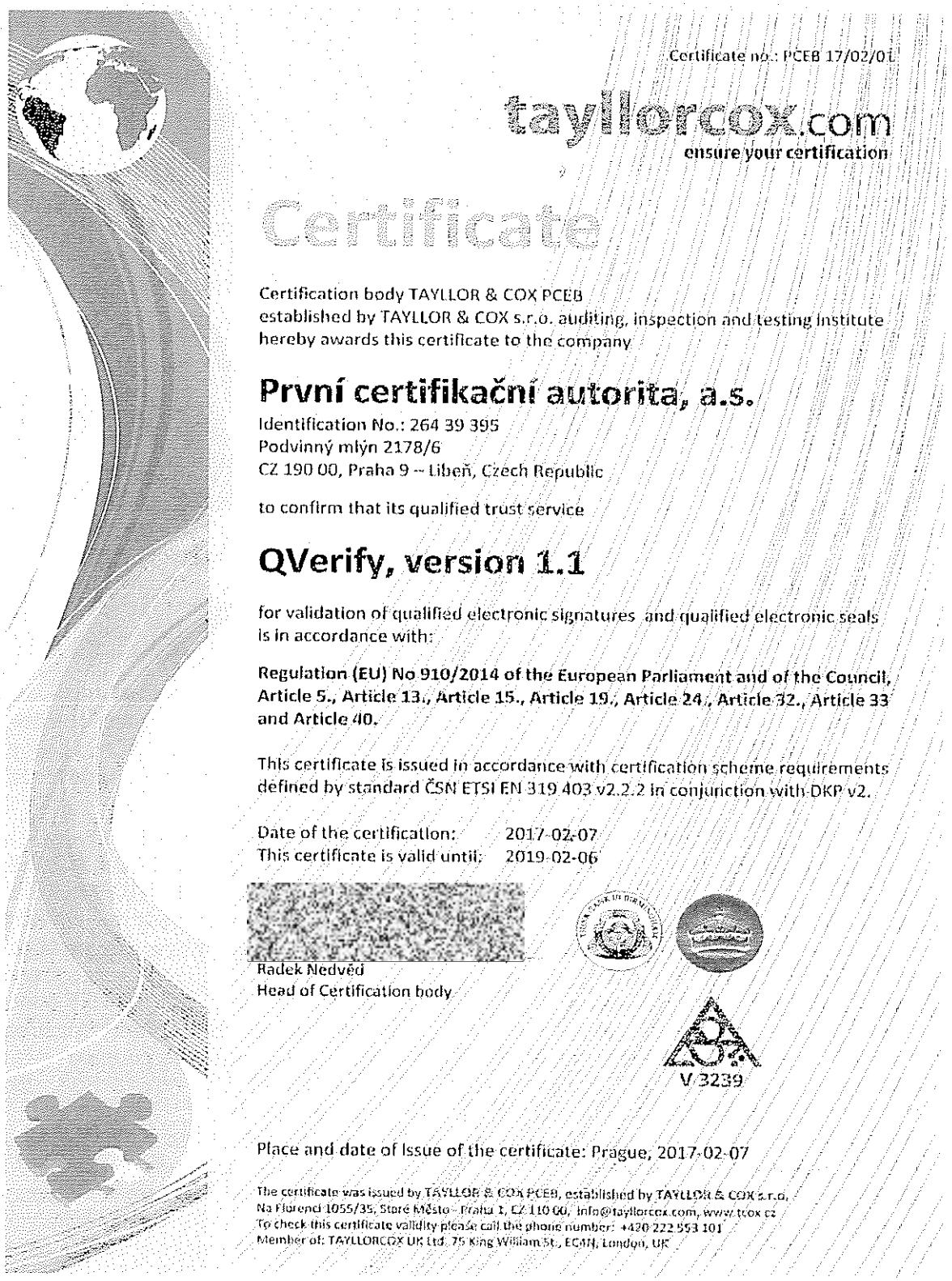
Veřejnoprávní původci mají povinnost ověřování definovanou §4 odst. 4-7 vyhlášky č. 259/2012 Sb., o podrobnostech výkonu spisové služby.

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 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:



Certificate no.: PCEB 17/02/01

taylloreox.com
ensure your certification

Certificate

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

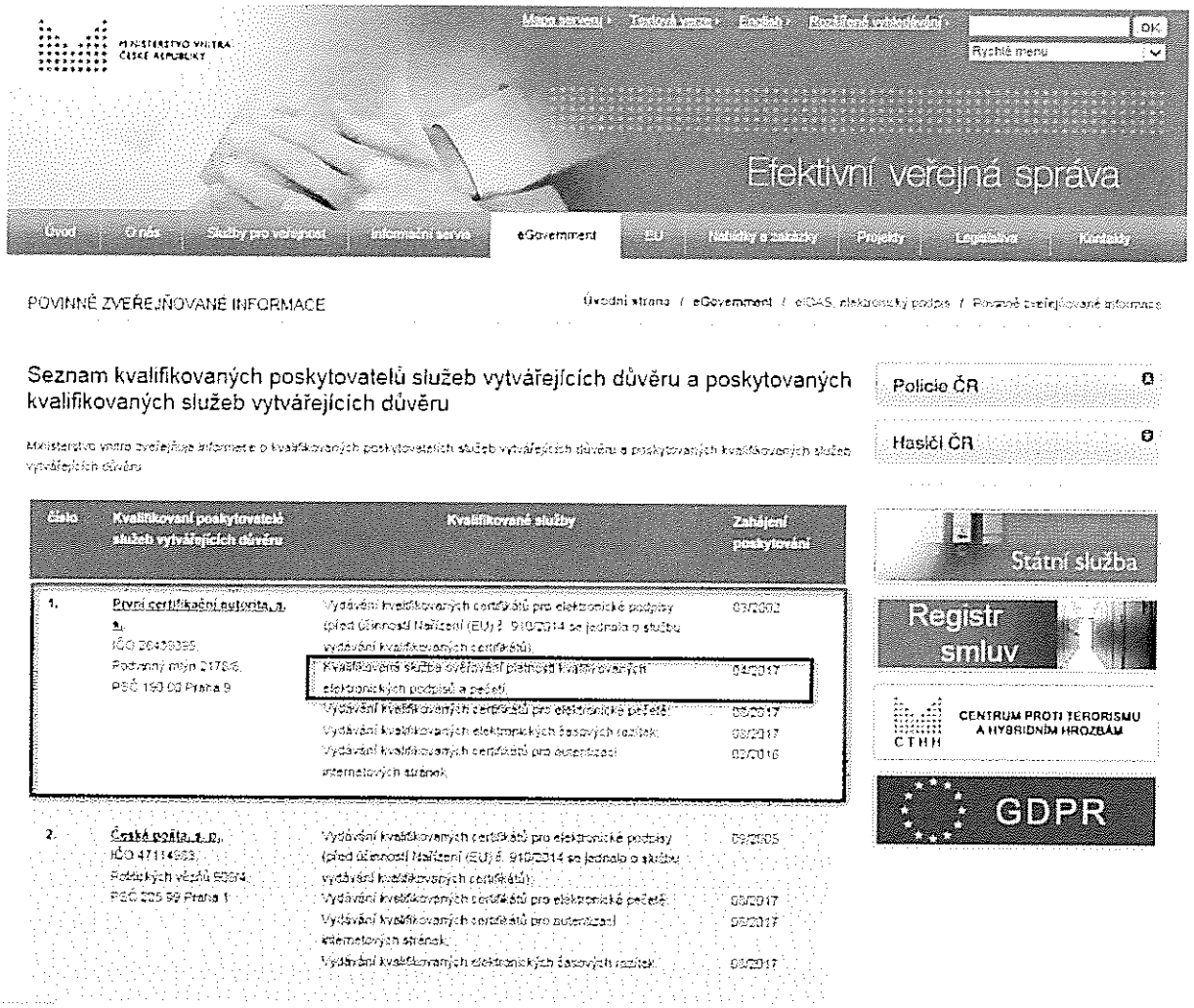
Radek Nedvěd
Head of Certification body

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, info@taylloreox.com, www.tcox.cz
To check this certificate validity please call the phone number: +420 222 553 101
Member of: TAYLLORCOX UK Ltd. 75 King William St., EC4N, London, UK

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/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:

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	Platné

Profil podpisu	EN 319 142-1 PAdES-B-T
Legislativní typ podpisu	Zaručený elektronický podpis založený na Kvalifikovaném certifikátu
Hash podepsaných dat	2556A8BF621848B67BFFF3483071250C191E5A1C7770EC1FDE52FB6C628BF1A1
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