I.CA QVerifyTL aktuální stav, praktické zkušenosti

Ing. Roman Kučera
První certifikační autorita, a.s.

24. 4. 2019

Kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů a pečetí

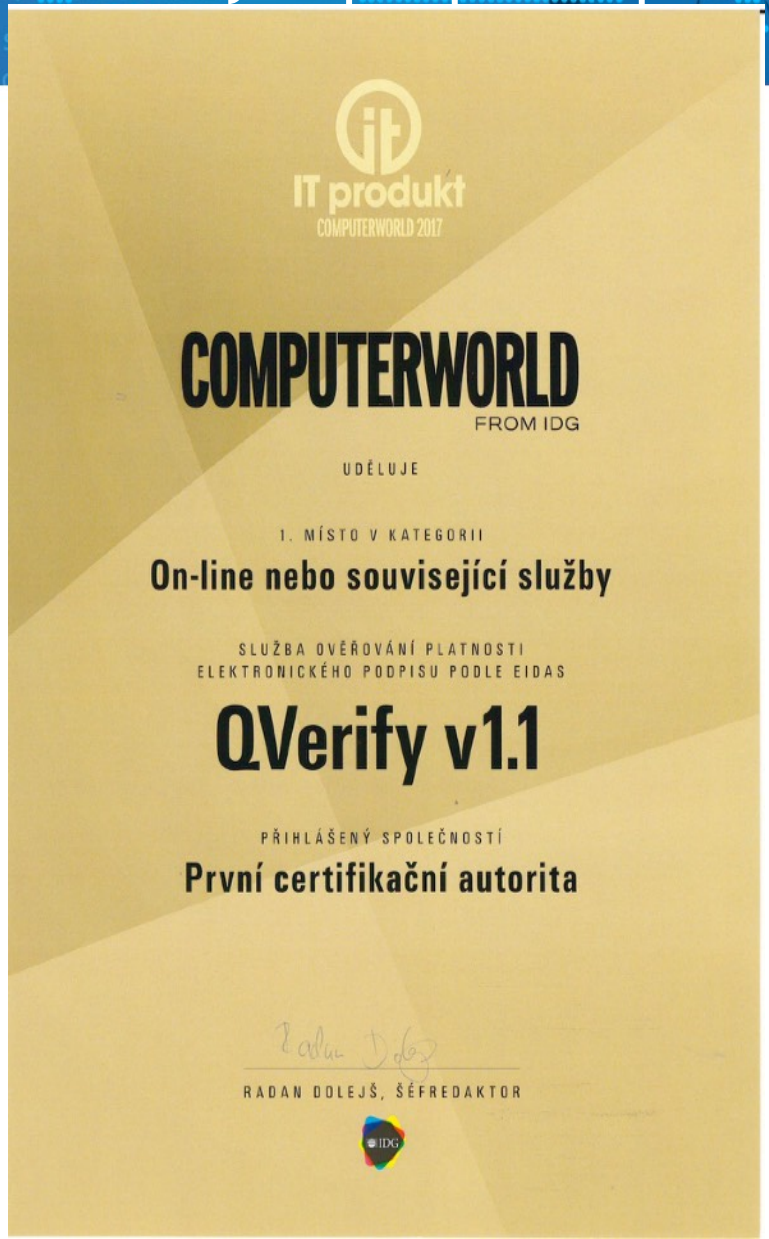
Účel služby

- zajištění právní jistoty ohledně platnosti podpisu/pečetě na straně spoléhající se strany – proto kvalifikovaná služba
- umožňuje, aby spoléhající se strany obdržely výsledek postupu ověření platnosti automatizovaným způsobem, který je spolehlivý, účinný a je opatřen zaručeným elektronickým podpisem nebo zaručenou elektronickou pečetí poskytovatele kvalifikované služby ověřování platnosti

I.CA nabízí službu I.CA QVerifyTL

Oceněna časopisem ComputerWorld jako IT produkt roku 2017 v kategorii on-line služby.

Kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů a pečetí



Kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů a pečetí

Služba I.CA QVerify byla zařazena na seznam služeb vytvářejících důvěru rozhodnutím ministerstva vnitra v dubnu 2017.

Služba ověřovala formáty (dle Prováděcího rozhodnutí Komise (EU) č. 2015/1506 :

- XAdES B
- PAdES B
- CAdES B

V březnu 2018 byla služba rozšířena o formáty T, tj. s časovým razítkem a o ověřování vůči LoTL EU.

Kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů a pečetí

V současné době ověřuje služba I.CA QVerifyTL podpisy a pečetě ve formátech:

- XAdES dle ETSI TS 103 171 v úrovni shody B, T a LT,
- PAdES dle ETSI TS 103 172 v úrovni shody B, T a LT,
- CAdES dle ETSI TS 103 173 v úrovni shody B, T a LT,
- XAdES dle ETSI EN 319 132-1 v úrovni shody B-B, B-T a B-LT
- PAdES dle ETSI EN 319 142-1 v úrovni shody B-B, B-T a B-LT
- CAdES dle ETSI EN 319 122-1 v úrovni shody B-B, B-T a B-LT
- ASiC - s

Kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů a pečetí

Certifikát č.: PCEB 19/02/01

tayllorcox.com
ensure your certification

Certifikát

Certifikační orgán TAYLLORCOX PCEB,
zřízený společností TAYLLORCOX s.r.o., institutem pro auditování, kontrolu a testování, uděluje tento certifikát společnosti

První certifikační autorita, a.s.
IČ: 264 39 395
Podvinný mlýn 2178/6
190 00, Praha 9 – Libeň, Česká republika

potvrzující, že kvalifikovaná služba vytvářející důvěru

QVerify, verze 1.1

pro ověřování platnosti kvalifikovaných elektronických podpisů a kvalifikovaných elektronických pečetí je v souladu s:

Nařízením Evropského Parlamentu a Rady (EU) č. 910/2014, článkem 5, článkem 13, článkem 15, článkem 19, článkem 24, článkem 32, článkem 33 a článkem 40.

Tento certifikát je vydáván v souladu s požadavky certifikačního schématu definovaného normou ČSN ETSI EN 319 403 v2.2.2 ve spojení s DKP verze 2.

Datum certifikace: 05.02.2019
Certifikát platí do: 05.02.2021

Ing. Radek Nedvěd
ředitel certifikačního orgánu

V 3239

Místo a datum vydání certifikátu: Praha, 05.02.2019

Certifikát byl vystaven společností TAYLLORCOX s.r.o.
Na Florenci 1055/35, Staré Město - Praha 1, CZ 110 00, info@tayllorcox.com, www.tcox.cz
Pro ověření platnosti tohoto certifikátu volejte: +420 222 553 101
Member of: TAYLLORCOX UK Ltd. 75 King William St., EC4N, London, United Kingdom, info@tayllorcox.com

Kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů a pečetí

Pro klienty, jež měli problém s prostupností a dostupností přes proxy soustavu do Internetu, byla služba rozšířena o variantu I.CA QverifyProxy.

V klientském prostředí běží služba I.CA QverifyProxy, která poskytuje do vnitřní sítě webové rozhraní. Všechny počítače využívající službu ověřování komunikují pouze s touto službou a prostupy do Internetu tudíž nepotřebují. Prostupy do I.CA má povolen pouze ten server, na kterém služba I.CA QverifyProxy běží.

Kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů a pečetí

Ověřování ZFO a S/MIME formátů, jež neodpovídají eIDAS

Služba umožňuje ověřit platnost podpisu/pečetě obálky datové zprávy ISDS formátu ZFO jako CAdES formát (celý ZFO soubor bez předchozího parsování).

Služba nepodporuje ověření podpisů/pečetí obsahujících atribut specifikující použitou podpisovou politiku (PP). V případě vložení ZFO na vstup ověření je kompletní obsah datové zprávy považován čistě za podepisovaná data, a to včetně příloh. Nedochází tedy k prohledávání příloh uvnitř ZFO a jejich případnému ověřování - volající aplikace musí příslušnou přílohu z obálky ZFO extrahovat a do služby pro ověření poslat zvlášť.

Kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů a pečetí

Ověřování ZFO a S/MIME formátů, jež neodpovídají eIDAS

Služba byla doplněna o nekvalifikovanou nadstavbu pro ověřování platnosti uznávaných elektronických podpisů e-mailových zpráv formátu S/MIME. 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 obsahuje informace o typu podpisového certifikátu, vydavateli, době jeho platnosti, zda je certifikát na QESCD, revokaci, atd.

Neuplatní se poslední odstavec bodu 1. čl. 13 nařízení eIDAS (důkazní břemeno), neboť nejde o kvalifikovanou službu, byť je poskytována kvalifikovaným poskytovatelem.

Kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů a pečetí

Ověřování ZFO a S/MIME formátů, jež neodpovídají eIDAS

Při ověřování platnosti podpisu/pečetě obálky datové zprávy formátu ZFO i e-mailové zprávy formátu S/MIME 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 podpisové politiky skončí s indikací INDETERMINATE/POLICY_PROCESSING_ERROR a ověření S/MIME kvůli chybějícímu atributu SigningCertificate skončí s indikací INDETERMINATE/SIG_CONSTRAINTS_FAILURE, proces ověřování musí být ukončen.

Kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů a pečetí

Povinnost ověřit platnost podpisu přijatého elektronického dokumentu definuje:

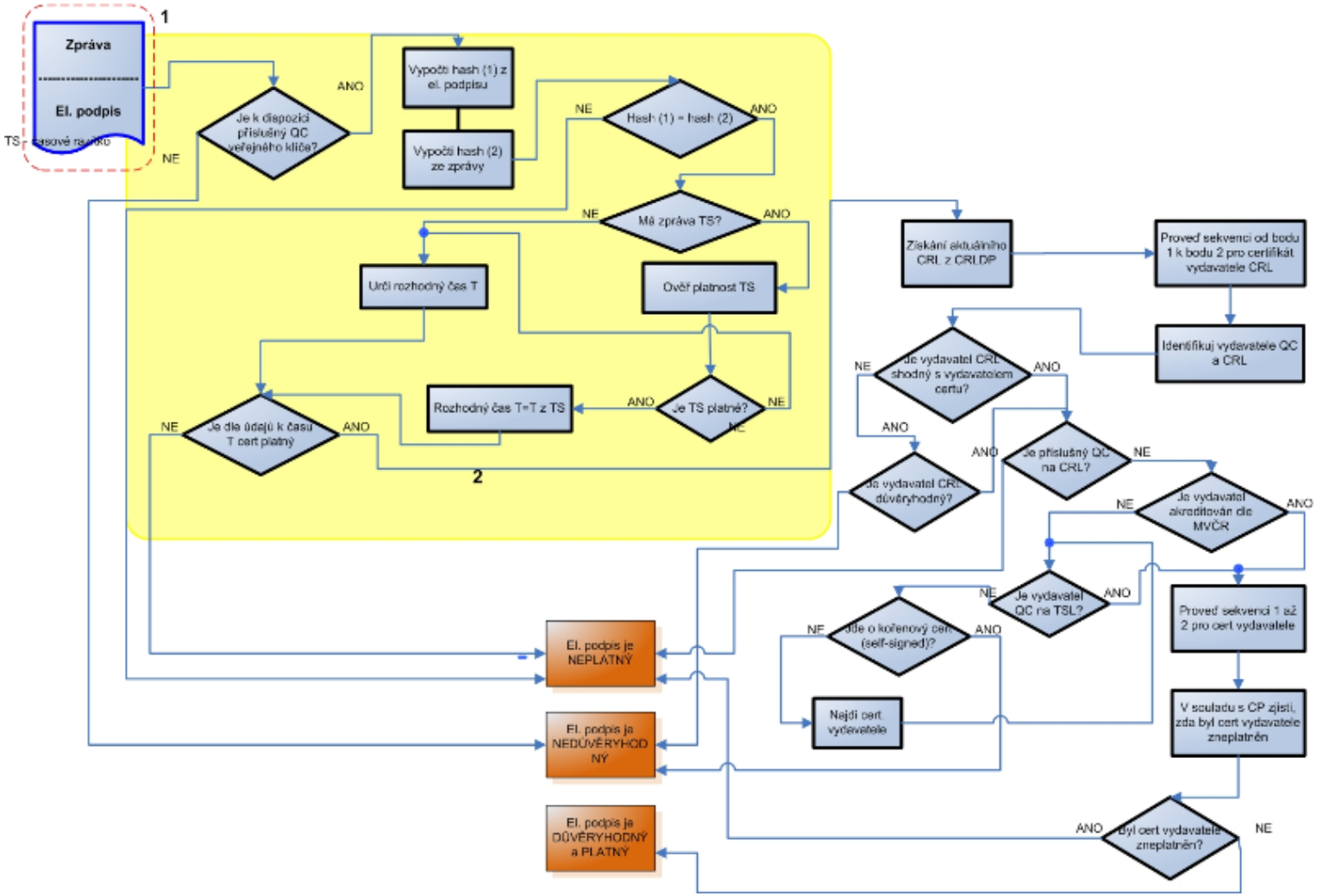
1. eIDAS v čl. 32
2. zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce v § 12
3. Vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby, ve znění pozdějších předpisů, v § 4 odst. 4-7 (v současné době probíhající novelizace nemění povinnosti veřejnoprávního původce zaznamenat výsledek ověření).

Kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů a pečetí

Stručný popis postupu ověřování platnosti elektronického podpisu (pečetě přiměřeně).

- Kontrola integrity dat (výpočet hashe z podepsaných dat, porovnání s hashem z podpisu).
- Zjištění, zda je dokument podepsán kvalifikovaným certifikátem vydaným kvalifikovaným poskytovatelem. *Dotaz na TSL*.
- Je certifikát platný? Nebyl zneplatněn? *Dotaz na OCSP či CRL*.
- Sestavení certifikační cesty k důvěryhodné kotvě
- Jedná se o podporovaný typ formátu podpisu (PAdES, CAdES, XAdES, Asic)?
- Jaký je legislativní typ podpisu?
- Stanovení času ověření: časové razítko/předaný čas ověření/čas přijetí požadavku
- Opakování podle počtu podpisů a razítek
- Vyhodnocení jednotlivých podpisů a razítek.

Kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů a pečetí



Kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů a pečetí

Služba I.CA QVerifyTL je poskytována:

1. na základě přímého smluvního vztahu I.CA a klienta
2. prostřednictvím dodavatelů spisových služeb (Gordic spol. s r.o., VERA, spol. s r.o.)

Kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů a pečetí

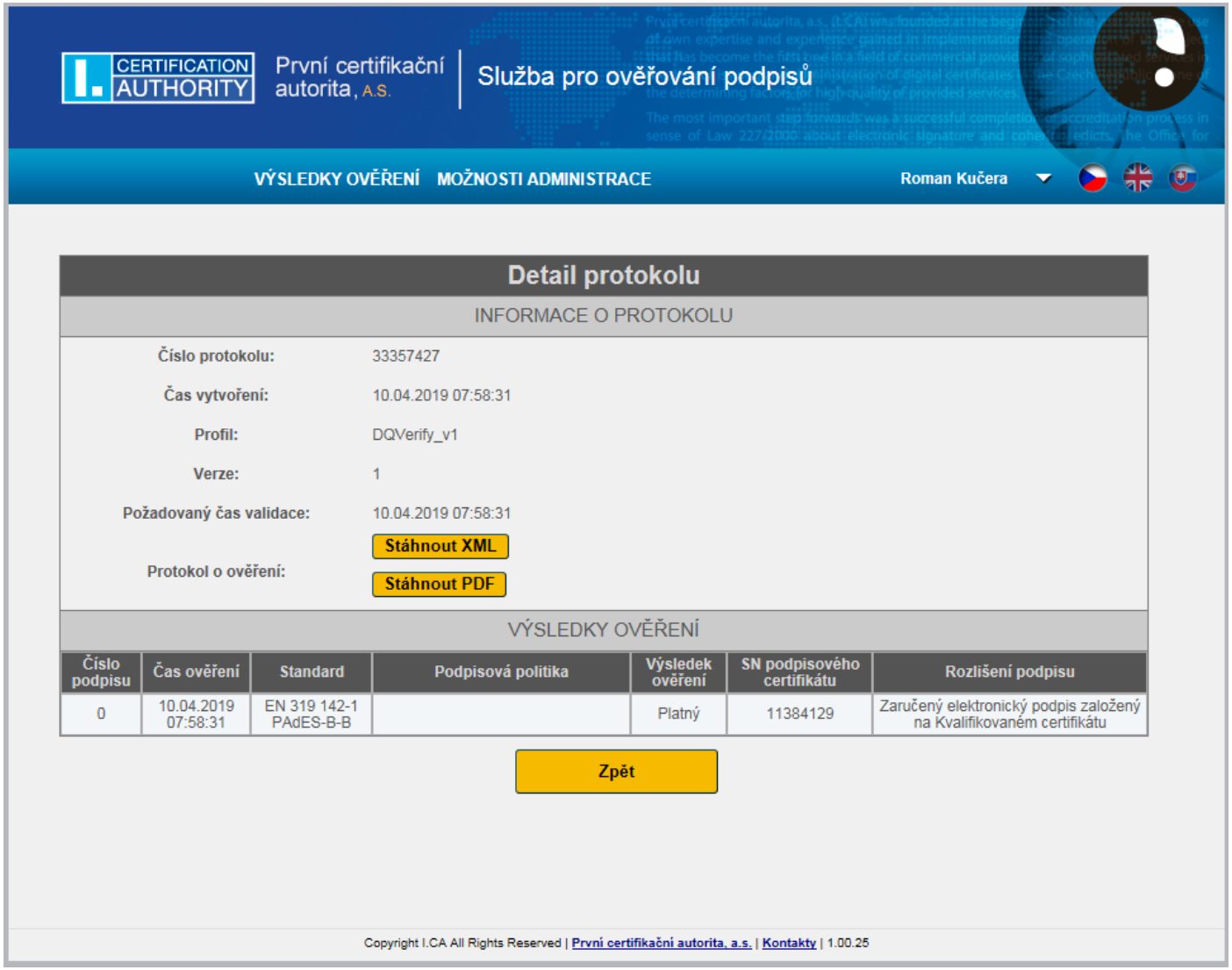
Výstupem služby je:

- Stav ověření (platný/neplatný podpis/nelze ověřit, důvod, proč nelze ověřit), čas, ke kterému se ověřovalo, zdroj času (časové razítko, čas obdržení požadavku, parametr zadaný uživatelem), data, na základě kterých bylo ověření provedeno (číslo CRL, OCSP odpověď), hash ověřovaných dat, informace o kvalifikovanosti certifikátu, zda je uložen na QESigCD/QESealCD …

Stav ověření má charakter:

- Podepsaného XML protokolu. Odpověď je odesílána on-line.
- Opečetěného PDF protokolu opatřeného časovým razítkem. Data pro generování protokolu jsou ukládána při generování xml protokolu, pdf protokol je následně k dispozici na vyžádání.

Kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů a pečetí



report_33357427.xml

Kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů a pečetí

Příklad pdf protokolu:

www.ICA.cz

PROTOKOL Č. 33357427

O OVĚŘENÍ PLATNOSTI KVALIFIKOVANÉHO ELEKTRONICKÉHO PODPISU A PEČETĚ

Identifikace ověřovaného dokumentu: Popis ICA QVerifyTL 19-02-19.pdf

PODPIS 1

Profil podpisu	EN 319 142-1 PAdES-B-B
Legislativní typ podpisu	Zaručený elektronický podpis založený na Kvalifikovaném certifikátu
Hash podepsaných dat	F569957F44724EC5572C6BC65AA681171009910943ODFE2630D6E7164FABFFB2
Čas ověření	10.04.2019 05:58
Zdroj ověření	CRL č. 12800
Sériové číslo certifikátu	11384129
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	04.05.2018 7:30:41 - 04.05.2019 7:30:41
CN certifikátu	Roman Kučera
Kvalifikovaný certifikát	Ano
Certifikát vydán na QESigCD	Ne
Výsledek ověření certifikátu	Platný
Výsledek ověření	Platný

Údaje jsou platné ke dni: 10.04.2019

Správnost tohoto ověření potvrzuje

První certifikační autorita, a. s.

Kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů a pečetí

Parametry prostředí:

Produkční:

24/7, SLA až 99,95 %, kapacita až 500 ověření/min (100 paralelních vláken).

Testovací:

24/7, SLA 99 %, kapacita až 60 ověření/min.

Parametry služby jsou škálovatelné.

Kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů a pečetí

Praktické zkušenosti z ostrého provozu

- Ostrý provoz byl zahájen v lednu 2017 pro ČSSZ
- V současné době službu odebírají:
  - ČSSZ cca 1,4 mil. ověření/měsíc
  - FN Plzeň cca 3 tis. ověření/měsíc
  - SFDI cca 1 tis. ověření/měsíc
  - VERA cca 15 tis. ověření/měsíc
    - Statutární město Jihlava
    - Město Železný Brod
    - Město Třebechovice pod Orebem
    - Město Chlumec nad Cidlinou
    - Město Rychnov nad Kněžnou
    - Město Bílovec
    - Město Mníšek pod Brdy

Kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů a pečetí

Praktické zkušenosti z ostrého provozu

- Jedná se o jednu z nejsložitějších on-line služeb I.CA z hlediska interpretace výsledku ověření – jak uživateli spisové služby sdělit výsledek ověření ve srozumitelné podobě
- To je úkolem dodavatele spisové služby, I.CA musí postupovat podle normy EN 319 102-1, a tomu odpovídá xml protokol
- Proto jsou jednání o implementaci služby s konkrétním zákazníkem náročnější.

Kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů a pečetí

Praktické zkušenosti z ostrého provozu

Nejčastější omyly zákazníků:

- Služba ověří platnost jednotlivých podpisů/razítek a shrne výsledek
  - Ověřuje se platnost jednotlivých podpisů bez vzájemné návaznosti
- Služba ověří právní platnost dokumentu
  - Nikoli, služba je podpůrným technickým nástrojem pro následné rozhodnutí.

Praktické zkušenosti z ostrého provozu

Největší problémem z hlediska interpretace zůstává formát podpisu PAdES

- Vyskytuje se velké množství podpisů ve formátu PAdES-Basic, které aktuální normě ETSI EN 319 142 nevyhovují
- Je to dáno staršími aplikacemi, které jsou používány
  - Podání je ve smyslu správního řádu v pořádku, z pohledu eIDAS nikoli
- Proto byl zvolen kompromis – podpis je vyhodnocen jako nepodporovaný (chyba 2007) s výsledkem nelze ověřit, ale protokol obsahuje informace o platnosti certifikátu, zda jde o QC, zda byl vydán na QESigCD. – tedy informace nutné pro rozhodnutí o přijetí podání a zahájení zpracování.

Kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů a pečetí

Praktické zkušenosti z ostrého provozu

- Počet komerčních certifikátů, jež byly zaměňovány pro podpis, klesá stejně jako podpisy certifikáty interní CA
- Zvyšuje se počet připojených časových razítek (povinnost OVM podle zákona č. 297/2016 Sb.)
- Stejně tak se zvyšuje počet kvalifikovaných elektronických podpisů při podáních vůči OVM (stačí zaručený podpis), nyní cca 15% .

Kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů a pečetí

Služba QVerify se vyvíjí a upravuje především na základě legislativy/technických norem.

To znamená stálé změny klientských knihoven i serverové části.

Např. aktuální ETSI TS 119 102–2 V1.2.1 (2019-02) specifikující strukturu validačního reportu.

Kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů a pečetí

Obchodní model

Komponenta I.CA instalovaná v prostředí klienta a volaná ze spisové služby je poskytovány zdarma, a to včetně maintenance a případné custemizace dle požadavků klienta. Veškeré úpravy vyvolané změnou legislativy či technických norem jsou taktéž zdarma.

Hrazena jsou jednotlivá ověření vždy podle počtu ověření za uplynulý kalendářní měsíc v příslušném pásmu jako součin ceny za 1 ověření a počtu ověření.

Jednotkové ceny se liší podle smluvně dohodnuté úrovně SLA a propustnosti.

Závěr

Děkuji za pozornost.

Roman Kučera

kucera@ica.cz

verify@ica.cz

www.ica.cz/Q-Verify