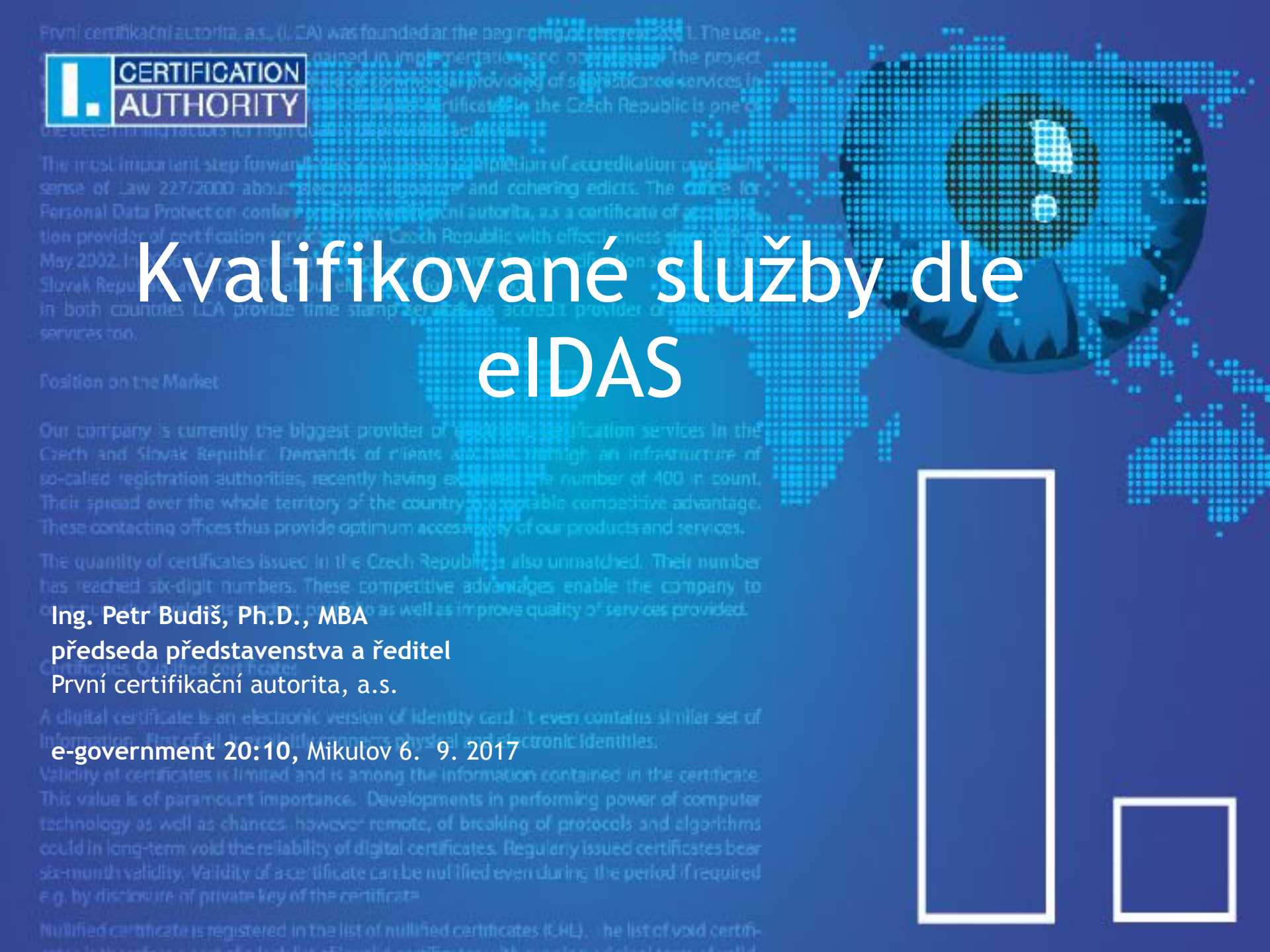


Kvalifikované služby dle eIDAS

Ing. Petr Budiš, Ph.D., MBA
předseda představenstva a ředitel
První certifikační autorita, a.s.

e-government 20:10, Mikulov 6. 9. 2017

Kvalifikované služby dle eIDAS

Název mého vystoupení je Kvalifikované služby dle eIDAS.

O jaké služby se tedy jedná?

Jednak o tradiční služby:

- Vydávání **kvalifikovaných certifikátů pro elektronický podpis**
- Vydávání **elektronických časových razítek.**

Kvalifikované služby dle eIDAS

A dále o nové služby:

- Vydávání **kvalifikovaných certifikátů pro elektronické pečetě**
- **Ověřování platnosti kvalifikovaných elektronických podpisů a pečetí**
- **Uchovávání kvalifikovaných elektronických podpisů a pečetí**
- Vydávání **kvalifikovaných elektronických časových razítek**
- Vydávání **kvalifikovaných certifikátů pro autentizaci internetových stránek.**

Kvalifikované služby dle eIDAS

A ještě o služby, jež eIDAS ve vlastním textu výslovně neupravuje, ale v preambuli je uvádí jako perspektivní:

- **Podepisování prostřednictvím mobilního telefonu** a **podepisování v cloudech**
- **Vytváření elektronického podpisu na dálku.**

Kvalifikované služby dle eIDAS

Poskytování kvalifikovaných služeb podle eIDAS je podmíněno **provedením auditu a posouzení ze strany orgánu dohledu**.

Pro vydávání **kvalifikovaných certifikátů pro elektronický podpis** bylo nutné předložit orgánu dohledu nejpozději do 30.6. Zprávu o posouzení shody.

To I.CA učinila 31.5.2017 a počátkem srpna obdržela sdělení MV, že neshledalo žádné neshody s požadavky nařízení eIDAS a zákona č. 297/2016 Sb.

I.CA tak může i nadále bez prodlevy vydávat kvalifikované certifikáty pro elektronický podp

Kvalifikované služby dle eIDAS

Dále I.CA 2.6. požádala orgán dohledu o udělení statutu kvalifikované služby vytvářející důvěru pro služby:

- **Vydávání kvalifikovaných certifikátů pro elektronické pečetě**
- **Vydávání kvalifikovaných elektronických časových razítek.**

Správní rozhodnutí MV o udělení statutu obou kvalifikovaných služeb obdržela I.CA dne 15.8. a ihned se vzdala práva na odvolání, proto správní rozhodnutí nabylo právní moci dne 16.8. a téhož dne byly obě služby uveřejněny v důvěryhodném seznamu služeb vytvářejících důvěru vedeném podle čl. 22 eIDAS na https://tsl.gov.cz se statutem „***granted***“.

Kvalifikované služby dle eIDAS

První službou, které byl v ČR udělen statut kvalifikované služby vytvářející důvěru, je služba

Ověřování platnosti kvalifikovaných elektronických podpisů

a pečetí I.CA QVerify.

Kvalifikované služby dle eIDAS

V současné době tak I.CA poskytuje čtyři kvalifikované služby vytvářející důvěru dle eIDAS:

1. **Vydávání kvalifikovaných certifikátů pro elektronický podpis**
2. **Vydávání kvalifikovaných certifikátů pro elektronické pečetě**
3. **Vydávání kvalifikovaných elektronických časových razítek**
4. **Ověřování platnosti kvalifikovaných elektronických podpisů a pečetí.**

.

Kvalifikovaná služba ověřování platnosti elektronických podpisů a pečetí

Podrobněji ke službě ověřování platnosti kvalifikovaných elektronických podpisů a pečetí I.CA QVerify.

Službu jsme začali vyvíjet počátkem roku 2015.

Posouzení shody bylo provedeno v prosinci 2016 společností DX PCEB (první audit první nové služby dle eIDAS v ČR) pro elektron a v únoru 2017 rozšířeno pro elektronické pečetě.

Certification no.: PCER 17/02/01

tayllorcox.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

Kvalifikovaná služba ověřování platnosti elektronických podpisů a pečetí

V únoru 2017 požádala I.CA Ministerstvo vnitra o udělení statusu kvalifikované služby vytvářející důvěry, v březnu se uskutečnilo jednání se zástupci MV k představení služby a předání dokumentace.

Rozhodnutí MVČR o zařazení na důvěryhodný seznam služeb vytvářejících důvěru vedený podle čl. 22 eIDAS obdržela I.CA 27.4.2017 a dne 28.4.2017 byla služba I.CA QVerify uveřejněna se statusem „granted“ [redacted]://tsl.gov.cz.

Kvalifikovaná služba ověřování platnosti elektronických podpisů a pečetí

Jde o první službu hodnocenou jako kvalifikovaná podle eIDAS v ČR; současně s touto službou získala I.CA též status kvalifikovaného poskytovatele služeb vytvářejících důvěru v souvislosti se službou I.CA QVerify.

Kvalifikovaná služba ověřování platnosti elektronických podpisů a pečetí

Nejedná se o službu ověřování platnosti certifikátu, ale elektronického podpisu!

Při ověřování platnosti certifikátu se ověřuje pouze:

- Jeho platnost (nebyl zneplatněn?) *Dotaz na OCSP či CRL*
- Jde o kvalifikovaný certifikát?
- Ověření platnosti nadřízeného a kořenového certifikátu. *Dotaz na CRL či OCSP.*

Kvalifikovaná služba ověřování platnosti elektronických podpisů a pečetí

V rámci EU se jedná o třetí kvalifikovanou službu ověřování platnosti elektronických podpisů a pečetí.

První kvalifikovanou službou je služba Certum QES
Asseco Data Systems S.A., Polsko, zprovozněnou a k

Druhou službou je TrustWeaver Signature Validation Service, Švédsko, zařazenou na seznam v prosinci 2016.

Kvalifikovaná služba ověřování platnosti elektronických podpisů a pečetí

Služba Certum QESValidationQ se od služby I.CA QVerify výrazně liší:

- Jde o webovou službu, kde je nutné vložit celý dokument
- Druhou možností je zaslat dokument e-mailem
- Ověřovány jsou formáty CAdES, PAdES, XAdES a ASiC baseline profile dle starších norem ETSI TS 103 171 až 103 174 z roku 2012, resp. 2013.

Zajímavé je, že služba byla hodnocena dle eIDAS ještě před účinností eIDAS, tj. před 1.7.2016 (certifikát TÜV je z 17.6.2016), kdy ještě nemohlo být schváleno polské národní akreditační schéma.

Nařízení (EU) 2016/679 – General Data Protection Regulation, Nařízení o ochraně osobních údajů, účinné od 25.5.2018.

Kvalifikovaná služba ověřování platnosti elektronických podpisů a pečetí

Je vůbec nutné při přijetí elektronického dokumentu jeho podpis ověřovat?

Určitě, je to přece stejné jako u papírového dokumentu, také musíme vědět, zda podepsala správná osoba (vlastnoruční/úředně ověřený podpis).

Je tedy přirozené, že je nutné ověřit a následně doložit, že tento úkon byl proveden právně správně,

existují minimálně další dva legislativní důvody:

1. eIDAS v čl. 32 definuje povinnost ověřovat platnost elektronického podpisu obecně; totéž v § 12 zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce (zaručený podpis a pečeť).
2. Vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby, tuto povinnost definuje pro veřejnoprávního původce dokumentu v § 4 odst. 4-7.

Kvalifikovaná služba ověřování platnosti elektronických podpisů a pečetí

Vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby, nebyla doposud novelizována v souladu s eIDAS a zákonem č. 297/2016 Sb.

Avšak ministerstvo vnitra vydalo v říjnu 2016 upravený „Metodický návod pro kontrolu výkonu spisové služby vedené prostřednictvím elektronického systému spisové služby u veřejnoprávních původců“.

Ten již aktualizován je a odkazuje na § 4 vyhlášky č. 259/2012 Sb.

Dostupný je na http://www.mvcr.cz/clanek/spisova-sluzba-metodiky.aspx

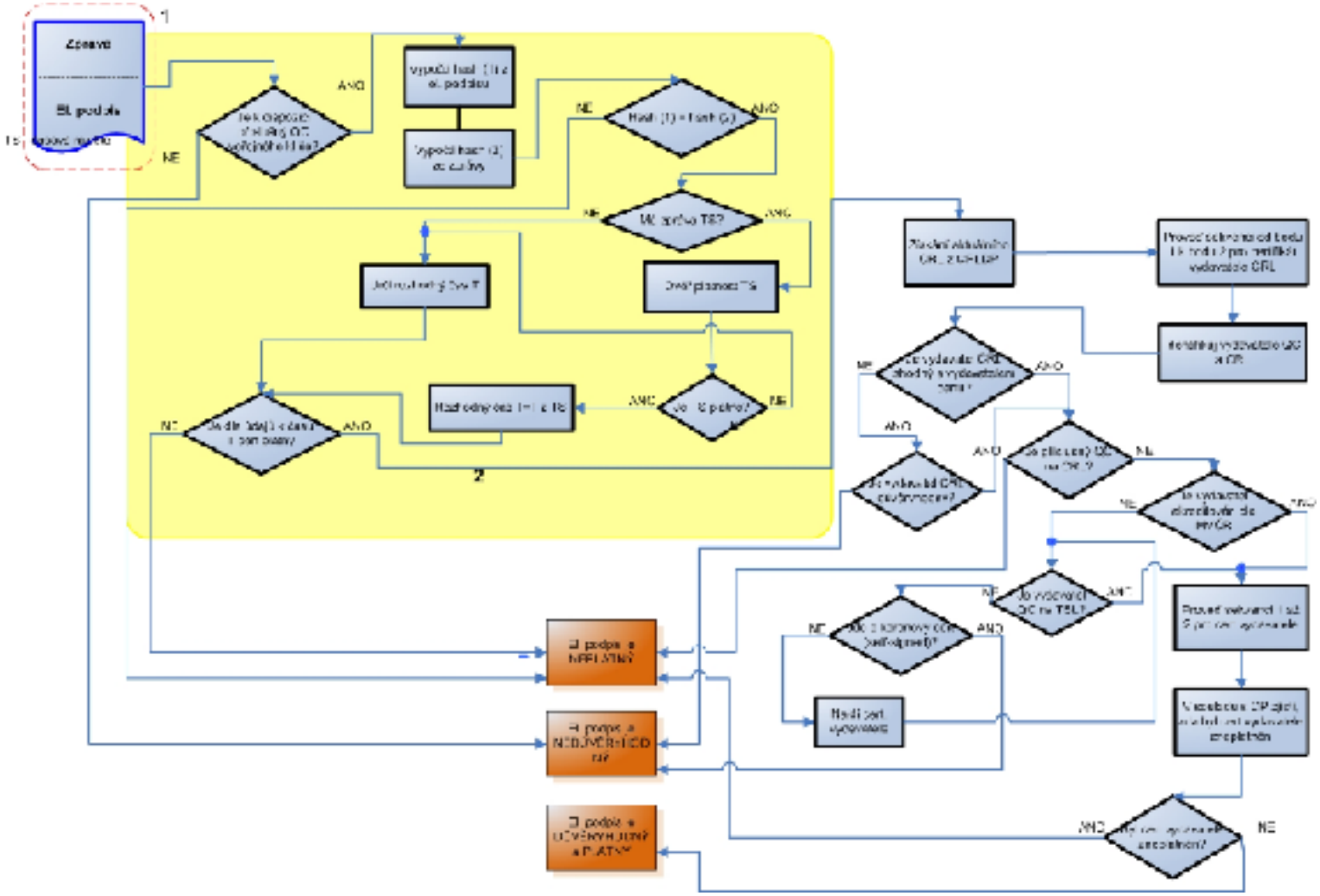
Pro veřejnoprávní původce je vyhláška závazná, pro ostatní lze použít přiměřeně návodně.

Kvalifikovaná služba ověřování platnosti 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)?
- Jaký je legislativní typ podpisu?
- Stanovení času ověření: obsahují předaná data čas ověření? Pokud ne, ověřuji k času přijetí požadavku.
- Opakování podle počtu podpisů
- Vyhodnocení jednotlivých podpisů.

Kvalifikovaná služba ověřování platnosti elektronických podpisů a pečetí



Kvalifikovaná služba ověřování platnosti elektronických podpisů a pečetí

Služba I.CA QVerify představuje nadstavbu elektronické spisové služby/DMS a přináší nespornou právní výhodu v přenesení odpovědnosti za správné ověření platnosti elektronického podpisu a pečetě na třetí stranu, kvalifikovaného poskytovatele služeb vytvářejících důvěru.

Kvalifikovaná služba ověřování platnosti elektronických podpisů a pečetí

I.CA jako kvalifikovaný poskytovatel služeb vytvářejících důvěru je dle čl. 13 odst. 1 eIDAS odpovědný za případnou škodu:

Článek 13

Odpovědnost za škodu a důkazní břemeno

1. Aniž je dotčen odstavec 2, poskytovatelé služeb vytvářejících důvěru odpovídají za škodu, kterou úmyslně nebo z nedbalosti způsobí fyzické nebo právnické osobě nesplněním povinností podle tohoto nařízení.

Důkazní břemeno, pokud jde o úmysl nebo nedbalost nekvalifikovaného poskytovatele služeb vytvářejících důvěru, nese fyzická nebo právnická osoba uplatňující nárok na náhradu škody podle prvního pododstavce.

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.

Kvalifikovaná služba ověřování platnosti elektronických podpisů

Služba sestává:

Ověřování elektronického podpisu

- Kvalifikovaný elektronický podpis
- Uznávaný elektronický podpis

Ověřování elektronické pečetě

Kvalifikovaná služba

Ověřování elektronické značky

Důvodem je, že elektronické značky nebyly ve směrnici č. 93/1999 definovány, proto nejsou do eIDAS převzaty.

Kvalifikovaná služba ověřování platnosti elektronických podpisů

Technické řešení služby:

S ohledem na bezpečnostní hledisko, interní politiky a požadavky klientů je služba realizována jako řešení rozprostřené mezi klienta a I.CA (podepsaný dokument, jehož podpis ověřujeme, neopustí prostředí klienta).

Kvalifikovaná služba ověřování platnosti elektronických podpisů

Výpočet hashe z podepsaných dat

Získání podpisové struktury
(norma ETSI 102853)

Výsledek ověření
(norma ETSI 319102p.2)

Odeslání struktury podpisu (bez dat)

nebo časového razítka a hashe

Ověření podpisu, TSA/ATSA/ LTV

Generování Protokolu
(norma ETSI 102853)

Prostředí klienta

Prostředí I.CA

Kvalifikovaná služba ověřování platnosti elektronických podpisů a pečetí

Služba ve standardní podobě představuje:

- Klient v 32b a 64b verzi Javy a .NET
- Rozpoznávání legislativního typu podpisu (kvalifikovaný - uznávaný) a formátu podpisu
- Veškerá validační schémata
- Protokol v XML podepsán externím CAdES podpisem
- PDF verze protokolu v PDF/A verze 1.3 podepsána a opatřena časovým razítkem.

Kvalifikovaná služba ověřování platnosti elektronických podpisů a pečetí

Parametry prostředí pro jednoho klienta:

Produkční:

24/7, SLA až 99,95 % (nedostupnost 4 hod 22 min 48 s/ rok), kapacita až 500 ověření/min (100 paralelních vláken).

Testovací:

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

Služba QVerify pracuje v režimu 24/7 s průměrnou rychlostí 20-250 ověření/min při průměrně 60.000 ověření/24 hod.

Parametry služby jsou škálovatelné.

Kvalifikovaná služba ověřování platnosti elektronických podpisů a pečetí

Jaké formáty elektronického podpisu služba ověřuje:

Jsou to formáty elektronického podpisu definované Prováděcím rozhodnutím Komise (EU) č. 2015/1506:

- XAdES-B-B
- PAdES-B-B
- CAdES-B-B

Jedná se o značení dle ETSI EN 319 122, ETSI EN 319 142 a ETSI EN 319 132.

Mimo výše uvedených formátů služba pracuje i s formátem PAdES-Basic.

Kvalifikovaná služba ověřování platnosti 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 (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 …

Stav ověření má charakter:

- Podepsaného XML protokolu. Odpověď je odesílána on-line.
- Podepsaného PDF protokolu opatřeného časovým razítkem. Protokol je generován v nočních hodinách a je možné jej autentizovaně stáhnout a uložit.

Kvalifikovaná služba ověřování platnosti elektronických podpisů a pečetí

Praktické zkušenosti z provozu

- Stěžejním bodem implementace bylo, jak správně interpretovat výsledky ověření v krajních situacích (např. když byl certifikát nově vydán a ihned po podpisu dokumentu zneplatněn, když ještě nebylo vydáno CRL).

Kvalifikovaná služba ověřování platnosti elektronických podpisů a pečetí

Praktické zkušenosti z ostrého provozu

- Největší problémem pak 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 klienti používají
    - 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 elektronických podpisů a pečetí

Praktické zkušenosti z ostrého provozu

Zásadním problémem bylo, jak přistoupit k realitě adaptačního zákona na území ČR:

- Kvalifikovaná služba ověřuje kvalifikované elektronické podpisy
- Ale vzhledem k § 6 zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, by taková služba nebyla na území ČR využitelná – ve většině případů by muselo ověření skončit s výsledkem neplatný podpis
- Proto byla služba doplněna o nadstavbu ověřující i zaručený podpis a protokol doplněn o legislativní status podpisu (kvalifikovaný – zaručený).

Kvalifikovaná služba ověřování platnosti elektronických podpisů a pečetí

Praktické zkušenosti z ostrého provozu

- Interní systém I.CA musí garantovat vysokou dostupnost 24/7, stabilitu a průchodnost – požadavky na ověření jsou zasílány nepřetržitě
- Zpracování 1 požadavku trvá průměrně 0,8-1,5s
- Při přijetí požadavku je přiděleno jednoznačné číslo protokolu (vzestupná řada), kdyby došlo k chybě při ověřování, toto číslo se již nikdy nepoužije
- Nejvyšší počty ověření jsou během pracovní doby od cca 7:00 do 17:00 (ve špičkách cca 350/min)
- Nejnižší jsou naopak před půlnocí a od cca 03:00 do 05:00 (jednotky ověření/min)
- Měsíčně je ověřeno cca 1,5 mil. požadavků.

Kvalifikovaná služba ověřování platnosti elektronických podpisů a pečetí

Praktické zkušenosti z ostrého provozu

Problémem je též ukládání PDF protokolů

- Průměrná velikost 1 protokolu je cca 360 KB
- Při cca 1,5 mil. protokolů/měsíc jde o cca 540GB
- Ročně pak o cca 6,5TB.

- Je však možné PDF protokoly negenerovat, ale učinit tak až při požadavku na předání lidsky čitelné podoby.

Kvalifikovaná služba ověřování platnosti elektronických podpisů a pečetí

Praktické zkušenosti z ostrého provozu

- Vyskytuje se také podpis komerčním certifikátem vydaným kvalifikovaným poskytovatelem
- Nebo podpis certifikátem vydaným interní CA
- Pokud je připojeno časové razítko, nebývá vždy vyd kvalifikovaným poskytovatelem
- Pouze v cca 5 % případů se jedná o kvalifikovaný elektronický podpis.

Kvalifikovaná služba ověřování platnosti elektronických podpisů a pečetí

Služba QVerify není statická, musí se neustále vyvíjet a upravovat. To znamená stálé změny klientských knihoven i serverové části.

I.CA stále musí:

- Sledovat stav legislativy a obecného používání elektronického podpisu
- Sledovat aktualizaci technických norem
- Stav kryptografických algoritmů
- Trendy obecně v oblasti PKI

a podle toho službu ověřování upravovat.

Kvalifikovaná služba ověřování platnosti 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 z provozních prostředků 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.

Ing. Petr Budiš

budis@ica.cz

verify@ica.cz

www.ica.cz/Q-Verify