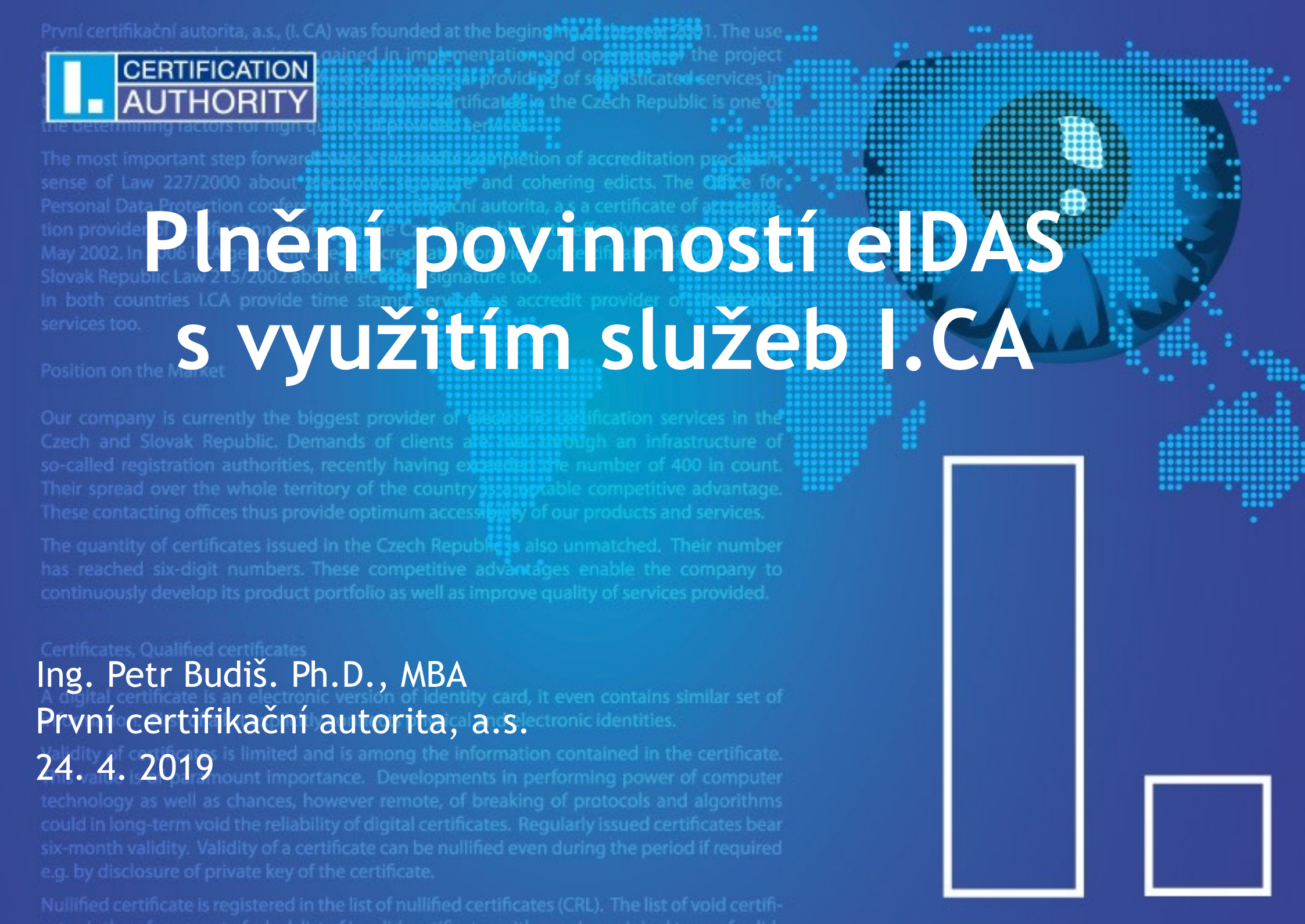


Plnění povinností eIDAS s využitím služeb I.CA

Ing. Petr Budiš. Ph.D., MBA
První certifikační autorita, a.s.
24. 4. 2019

Evropské nařízení a český zákon

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 (zkráceně: **nařízení eIDAS**)

Účinnost od 1. 7. 2016

Zákon o službách vytvářejících důvěru pro elektronické transakce (č.297/2016 Sb.)

Účinnost od 19. 9. 2016

Seznam kvalifikovaných služeb I.CA

Kvalifikované služby	Zahájení poskytování na základě posouzení MV
Vydávání kvalifikovaných certifikátů pro elektronické podpisy	03/2002
Kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů a pečetí	04/2017
Vydávání kvalifikovaných certifikátů pro elektronické pečetě	08/2017
Vydávání kvalifikovaných elektronických časových razítek	08/2017
Vydávání kvalifikovaných certifikátů pro autentizaci internetových stránek	02/2018

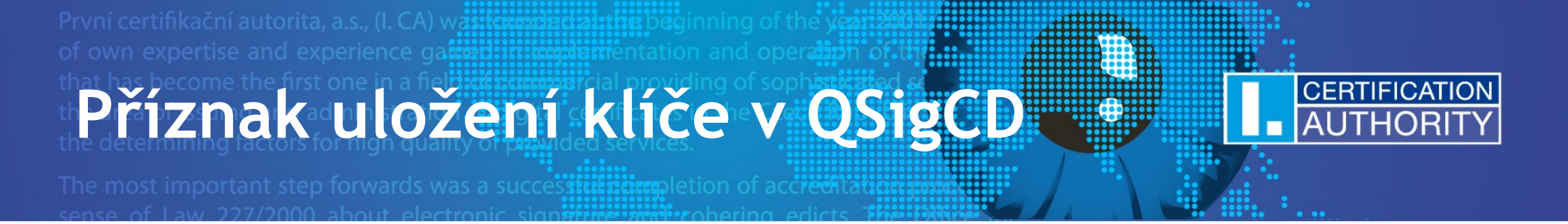
Služba poskytovaná kvalifikovaným poskytovatelem

Vytváření kvalifikovaných elektronických pečetí na dálku	06/2018

Kvalifikovaný certifikát pro e-podpis

Uložení soukromého klíče	Vytvořený typ elektronického podpisu	Určen pro právní jednání státu/ vůči státu (dle zákona č. 297/2016 Sb.)	Rovnocenný vlastnoručnímu podpisu (dle eIDAS)
PC	Zaručený e-podpis založený na kvalifikovaném certifikátu	N/A	ne
Čipová karta, která není QSigCD (často zaměstnanecké karty)	Zaručený e-podpis založený na kvalifikovaném certifikátu	N/A	ne
QSigCD – Starcos 3.5, dodavatel I.CA	Kvalifikovaný elektronický podpis	A/A	ano
QSigCD – dodavatel stát prostřednictvím eOP	Kvalifikovaný elektronický podpis	A/A	ano

Příznak uložení klíče v QSigCD



I.CA vydá kvalifikovaný certifikát pro elektronický podpis s příznakem uložení na bezpečném prostředku, tj. pro vytváření **kvalifikovaného elektronického podpisu**, výhradně

- v případě, kdy je soukromý klíč generován v čipu čipové karty Starcos 3.5, kterou uživateli I.CA dodá.
- v případě eOP.

V obou případech se jedná o QSigCD.

V ostatních případech může být vydán kvalifikovaný certifikát pro elektronickou pečeť bez tohoto příznaku, k použití pro vytváření **zaručeného e-podpisu založeného na kvalifikovaném certifikátu**.

Poznámka: Kvalifikovaný elektronický podpis nebo zaručený e-podpis založený na kvalifikovaném certifikátu = souhrnně podle zákona č. 297/2016 Sb. „uznávaný elektronický podpis“. Nařízení eIDAS tento pojem nezná.

Komerční certifikáty a TWINS

I.CA nadále vydává **komerční certifikáty**, které jsou určené pro autentizaci a šifrování. Nejčastěji jsou vydávány ve dvojici s kvalifikovaným certifikátem – obchodní název **„TWINS“**.

TWINS na čipové kartě Starcos 3.5 je v současné době velmi vyhledávaným produktem I.CA. Oblíbená je verze **plug-in** (vylamovací čip ve čtečce čipových karet). **ČK Starcos 3.5 je QSigCD a je způsobilá pro vytváření kvalifikovaných elektronických podpisů.**

Starcos 3.0 a 3.5 - QSigCD

Reakce uživatelů na povinnosti podle eIDAS a zákona č. 297/2016 Sb., zejména veřejnoprávní podepisující, ale i finanční instituce a zdravotnická zařízení:

Typ	Nárůst počtu vydaných ČK Starcos v roce 2017 proti roku 2016	Nárůst počtu vydaných ČK Starcos v roce 2018 proti roku 2016
ČK klasické, včetně duálních	199 %	328 %
ČK plug-in a token	127 %	155 %

Pozn: 100% = rok 2016

Trendy ve vydávání certifikátů

Typ certifikátu	Vývoj v letech 2015 - 2018
Kvalifikované certifikáty pro e-podpis	37 % nárůst počtu vydaných certifikátů mezi roky 2015 - 2018
(Kvalifikované) systémové certifikáty	Mezi roky 2015 a 2017 nárůst o 36 %, v roce 2018 už mírný pokles ve prospěch kvalifikovaných certifikátů pro elektronické pečetě. Uvítali bychom, kdyby náhrada systémových certifikátů za certifikáty pro pečetě nebo za KSC probíhala rychleji.
Komerční certifikáty (osobní)	29 % nárůst počtu vydaných certifikátů mezi roky 2015 - 2018
Komerční technologické certifikáty	83 % nárůst počtu vydaných certifikátů mezi roky 2015 – 2018.

eOP jako QSigCD

I.CA umožňuje vydávání kvalifikovaných certifikátů pro elektronický podpis s generováním a uložením soukromého klíče v čipu eOP.

Zájem není velký, neboť

- velká část kvalifikovaných certifikátů pro elektronický podpis je vydávána jako tzv. zaměstnanecké certifikáty, tj. v certifikátu je uveden název zaměstnavatele. Pro tento účel je eOP zcela nevhodný – OP je „osobní“, nikoliv „zaměstnanecký“.
- podle zákona č. 297/2016 Sb. pro komunikaci občanů se státem, tedy pro „osobní“ kontakt, postačí kvalifikovaný certifikát s uložením soukromého klíče v paměti PC a není tedy nezbytné použít QSigCD.

Celkem bylo vydáno od října 2018 do současnosti 22 ks kvalifikovaných certifikátů do e-OP.

Kvalifikované certifikáty pro e-pečeť

I.CA vydává ve variantě uložení soukromého klíče

- v QSealCD, tj. v prostředku pro vytváření **kvalifikovaných elektronických pečetí,** který I.CA sama spravuje.

  Jedná se o službu **vzdáleného vytváření kvalifikovaných elektronických pečetí jménem pečetící osoby** (tj. vzdálené pečetění) - **I.CA RemoteSeal**.

  Od uvedení služby do rutinního provozu, tj. v období 09/2018 – 03/2019 bylo vydáno/vytvořeno 750 tisíc elektronických pečetí. Další klienti jsou ve fázi testování služby.

- v prostředku (na serveru) klienta pro vytváření **zaručených elektronických pečetí**. Tyto certifikáty často postupně nahrazují (kvalifikované) systémové certifikáty, které I.CA na žádost klientů stále ještě vydává. Staly se však komerčními certifikáty.

Kdy je nezbytné nahradit značku pečetí

- E-značku nelze použít v případech, kdy právní předpis stanoví povinnost použít zaručenou/uznávanou/ kvalifikovanou elektronickou pečeť.

- Elektronickou pečetí může dokument opatřit pouze **původce dokumentu** – pozor při příjmu elektronických dokumentů.

  nařízení eIDAS

- Kvalifikovaný certifikát pro elektronickou pečeť nelze vydat na fyzickou osobu, ale pouze na **právnickou osobu**.

  nařízení eIDAS

Vydávání certifikátů I.CA

- **Veřejné registrační autority** (VRA) – 30 provozoven po celé ČR, nabízejí služby všem zájemcům, kteří splní požadavky Certifikační politiky.
- **Klientské registrační autority** (KRA) – provozují klienti na základě smlouvy s I.CA jejím jménem, a to pro potřeby své organizace.
- Bylo zřízeno téměř tisíc jednotlivých pracovišť. Zastoupeny jsou především banky, úřady a nemocnice. Jsou provozovány také na Slovensku, ve Švýcarsku a v Bulharsku.
- **Mobilní registrační autority** (MRA) – provozuje I.CA a nabízejí některé VRA I.CA. Na žádost klienta I.CA zajišťuje výjezdy v rámci celé Evropy.

Ověřování platnosti podpisů a pečetí

Kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů a pečetí – I.CA QVerify

- Zajištění právní jistoty ohledně platnosti podpisu na straně spoléhající se strany – proto nově podle nařízení eIDAS **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.
- Služba je určena především klientům, kteří přijímají velké objemy elektronicky podepsaných/opečetěných e-dokumentů, se zřetelem na nezbytnost následného dokazování platnosti podpisu/pečetě. I.CA provádí průměrně 1,4 milionů ověření měsíčně. Velmi jsme uvítali spolupráci s významnými producenty systémů spisových služeb.

Právní úprava ověřování

Veřejnoprávní původci mají povinnost ověřovat platnost elektronických podpisů u přijatých elektronických dokumentů dle § 4 odst. 4) až 7) vyhlášky č. 259/2012 Sb., o podrobnostech výkonu spisové služby.

Novela této vyhlášky č. 85/2019 Sb. s účinností od 07/2019 i nadále tuto povinnost stanoví, a to následovně:

Veřejnoprávní původce je povinen zaznamenat:

„g) výsledek, datum a čas ověření platnosti uznávaného elektronického podpisu, uznávané elektronické pečetě, uznávané elektronické značky, kvalifikovaného elektronického časového razítka a certifikátů, na nichž jsou založeny, a

h) číslo seznamu zneplatněných certifikátů, vůči kterému byla platnost certifikátu ověřována, nebo způsob, jakým byla platnost certifikátu ověřována, nebylo-li seznamu zneplatněných certifikátů k ověření platnosti certifikátu užito.“.

QWAC

I.CA vydává **kvalifikované certifikáty pro autentizaci internetových stránek**

Qualified certificates for website authentication – de facto SSL certifikáty.

QWAC podle eIDAS - umožňuje autentizovat internetové stránky a spojuje je s fyzickou nebo právnickou osobou, jíž je certifikát vydán.

Právními předpisy není stanovena povinnost QWAC používat – mohlo by
v budoucnu být například povinné pro webové stránky orgánů státu.

QWAC a certifikační služby celkově nacházejí uplatnění ve službách finančních institucí.

Speciální služby pro finanční sektor

Služby pro splnění požadavků:

- směrnice EP a Rady (EU) 2015/2366 o platebních službách na vnitřním trhu (PSD2).
- zákona č. 370/2017 Sb., o platebním styku.

Služby:

- vydávání certifikátů – QC pro e-pečetě, QWAC dle eIDAS pro PSD2
- ověřování QC s atributy PSD2 – Služba I.CA WHITELIST

  Každá banka nebo finanční instituce vedoucí klientský účet musí kvalifikovaně ověřit platnost kvalifikovaného certifikátu přistupujícího TPP (Third Party Provider) navíc ověřit i platnost atributů PSD2.

Aktivní role I.CA ve službách pro finanční sektor

- I.CA počátkem roku 2018 zahájila jako jeden z prvních evropských kvalifikovaných poskytovatelů služeb vytvářejících důvěru vydávání kvalifikovaných certifikátů pro potřeby PSD2.

- Aktuálně se I.CA stala členem Open Banking Europe QTSP Working group, kde jsou diskutovány aktuální otázky v oblasti využívání kvalifikovaných certifikátů s atributy požadovanými PSD2.

Kvalifikovaný systém elektronické identifikace

Na základě zákona č. 250/2017 Sb., o elektronické identifikaci, má I.CA zájem stát se kvalifikovaným správcem kvalifikovaného systému elektronické identifikace, a to s kvalifikovaným prostředkem na úrovni záruky „vysoká“ podle prováděcího nařízení komise (EU) 2015/1502.

Kvalifikovaným prostředkem je kombinace komerčního identitního certifikátu s uložením privátního klíče na čipové kartě Starcos 3.5.

12.3.2019 získala I.CA audit tohoto systému a 15.3. podala žádost o udělení akreditace.

Získání akreditace není jednoduchou záležitostí, samotný audit splnění povinností eIDAS, zákona č. 250/2017 Sb. a dokumentu DKP IdP v.3 trval sice „jen“ měsíc, ale příprava zabrala 6 měsíců.

Kvalifikovaný systém elektronické identifikace

Dalším předpokladem akreditace je potvrzení, že systém elektronické identifikace umožňuje poskytnutí na služby národního bodu (ISVS provozovaný Správou základních registrů).

28.3.2019 obdržela I.CA dokumentaci pro testování napojení na národní bod.

Základní povinnosti kvalifikovaného správce:

c) před prvním použitím prostředku pro elektronickou identifikaci v rámci kvalifikovaného systému ověří totožnost držitele prostřednictvím národního bodu,

d) zapíše identifikátor jím vydaného prostředku pro elektronickou identifikaci a úroveň záruky tohoto prostředku do národního bodu,

e) aktualizuje údaje v evidenci vydaných prostředků pro elektronickou identifikaci na základě upozornění správce národního bodu na změny údajů,

g) bez zbytečného odkladu zneplatní prostředek pro elektronickou identifikaci držitele, o kterém se prokazatelně dozvěděl, že zemřel nebo byl prohlášen za mrtvého,

h) bez zbytečného odkladu zneplatní prostředek pro elektronickou identifikaci na základě žádosti držitele, nebo na základě ohlášení držitele o zneužití nebo hrozícím nebezpečí zneužití prostředku pro elektronickou identifikaci,

i) při ukončení své činnosti zneplatní jím vydané prostředky pro elektronickou identifikaci,

j) oznámí správci národního bodu zneplatnění prostředku pro elektronickou identifikaci podle písmen g) až i).

Kvalifikovaný systém elektronické identifikace

Požadavkům odpovídá 6 testovacích scénářů, které v současné době I.CA analyzuje a připravuje do realizace.

Samozřejmě to znamená dopad na interní systémy I.CA a vývoj backoffice.

Proces je o to složitější, že I.CA je prvním žadatelem o akreditaci k působení jako kvalifikovaný správce kvalifikovaného systému elektronické identifikace v ČR.

Slovo „První“ v názvu společnosti tedy není náhodné.....

Kvalifikovaná elektronická časová razítka

I.CA vydává i nadále ve variantách

- **kvalifikovaná časová razítka**
- archivní kvalifikovaná časová razítka

Doba, po kterou může spoléhající strana elektronické časové razítko ověřit, je omezena platností certifikátu, na kterém je založen „podpis“ certifikační autority, kterým je časové razítko „podepsáno“. Platnost tohoto certifikátu je zpravidla 5 roky. Použití ATSA tuto dobu prodlužuje na cca 10 let.

Mezi roky 2015 až 2018 vzrostl počet odebraných časových razítek o 66 %.

Je zde zřejmý dopad naplnění povinnosti veřejnoprávních podepisujících a dalších povinných osob opatřovat kvalifikovanými časovými razítky elektronické dokumenty, kterými se právně jedná (podle zákona č. 297/2016 Sb.).

Význam nařízení eIDAS pro I.CA

- Možnost rozšířit portfolio kvalifikovaných služeb.
- Realizace nařízení eIDAS znamenala pro I.CA obchodní příležitost.
- Na druhé straně si realizace nařízení eIDAS vynutila velký objem vývojářských prací, potřebu úprav interních systémů, posílení HW v provozu, náklady spojené s audity a nezbytnost přijetí dalších odborných pracovníků.
- I.CA řeší četné požadavky na součinnost při nasazení služeb I.CA u jednotlivých klientů s ohledem na specifika jejich ICT prostředí.
- I.CA vynaložila nemalé prostředky do seznamování klientů i veřejnosti s principy eIDAS (odborné konference I.CA, aktivní účast na akcích jiných subjektů, četné konzultace s klienty a případně s jejich dodavateli, publikování odborných článků aj.).

Naše poznatky

- Přetrvává nezbytnost upřesnění/výkladu některých ustanovení nařízení eIDAS, a tedy stálého kontaktu s orgány EK, s ENISA a dalšími orgány EU a samozřejmě s pracovníky MV.
- Co nás trápí – problémy s používáním certifikátů v některých IS provozovaných státními institucemi. Uživatel se může domnívat, že tyto problémy jsou způsobeny certifikátem.
- Protože některé tyto systémy mají nedostatečný podpůrný aparát (funkční helpdesk, aktuální manuál), uživatelé se s žádostí o řešení obracejí na nás. Jsme však schopni jim pomoci pouze v omezené míře.

Co nás potěšilo

- Důvěra a spolupráce našich klientů při zavádění nařízení eIDAS do praxe. V mnoha případech až překvapivě hluboká znalost problematiky.
- Na základě prezentovaných čísel je zřejmé, že uživatelé naplňují ve velké míře požadavky nařízení eIDAS, i když podle našich poznatků výjimky ještě existují.
- I.CA byla v roce 2018 úspěšná v 75 % výběrových řízení, kterých se účastnila.
- I.CA byla svěřena mimořádná zakázka - Návrh řešení a realizace vydávání certifikátů pro bezpečnostní složky státu, tj. řešení k tomu určené speciální Národní certifikační autority.

Závěr

Děkuji za pozornost.

budis@ica.cz

www.ica.cz