Zkušenosti s poskytováním služeb dle eIDAS

Ing. Petr Budiš, Ph.D., MBA
generální ředitel I.CA
4. 9. 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 poskytovatelů v ČR

číslo	Kvalifikovaní poskytovatelé služeb vytvářejících důvěru	Kvalifikované služby	Zahájení poskytování
1.	První certifikační autorita, a. s., IČO 26439395, Podvinný mlýn 2178/6, PSČ 190 00 Praha 9	Vydávání kvalifikovaných certifikátů pro elektronické podpisy (před účinností Nařízení (EU) č. 910/2014 se jednalo o službu vydávání kvalifikovaných certifikátů); Kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů a pečetí; Vydávání kvalifikovaných certifikátů pro elektronické pečetě; Vydávání kvalifikovaných elektronických časových razítek; Vydávání kvalifikovaných certifikátů pro autentizaci internetových stránek.	03/2002 04/2017 08/2017 08/2017 02/2018
2.	Česká pošta, s. p., IČO 47114983, Politických vězňů 909/4, PSČ 225 99 Praha 1	Vydávání kvalifikovaných certifikátů pro elektronické podpisy (před účinností Nařízení (EU) č. 910/2014 se jednalo o službu vydávání kvalifikovaných certifikátů); Vydávání kvalifikovaných certifikátů pro elektronické pečetě; Vydávání kvalifikovaných certifikátů pro autentizaci internetových stránek; Vydávání kvalifikovaných elektronických časových razítek.	09/2005 08/2017 08/2017 08/2017
3.	eldentity a. s., IČO 27112489, Vinohradská 184/2396, PSČ 130 00 Praha 3	Vydávání kvalifikovaných certifikátů pro elektronické podpisy (před účinností Nařízení (EU) č. 910/2014 se jednalo o službu vydávání kvalifikovaných certifikátů). Vydávání kvalifikovaných elektronických časových razítek Vydávání kvalifikovaných certifikátů pro elektronické pečetě	08/2005 01/2018 02/2018
4.	Software602 a. s., IČO 63078236, Hornokrčská 703/15, PSČ 140 00 Praha 4	Kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů a pečetí; Kvalifikovaná služba uchování kvalifikovaných elektronických podpisů a pečetí.	06/2017 06/2017
5.	Správa základních registrů, IČO 72054506, Na vápence 915/14, PSČ 130 00 Praha 3	Vydávání kvalifikovaných certifikátů pro elektronické podpisy; Vydávání kvalifikovaných certifikátů pro elektronické pečetě; Vydávání kvalifikovaných elektronických časových razítek	05/2019
6.	SEFIRA spol. s r.o., IČO 62907760, Antala Staška 2027/77, PSČ 140 00 Praha 4	Kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů a pečetí.	08/2019

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 elektronický podpis bez tohoto příznaku, k použití pro vytváření **zaručeného e-podpisu založeného na kvalifikovaném certifikátu.**

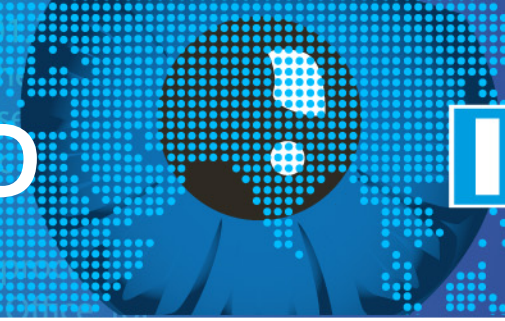
Poznámka: Kvalifikovaný elektronický podpis nebo zaručený e-podpis založený na kvalifikovaném certifikátu = souhrnně podle zákona č. 297/2016 Sb. „uznávaný elektronický podpis“. Nařízení eIDAS tento pojem nezná.

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, zdravotnická zařízení a další subjekty:

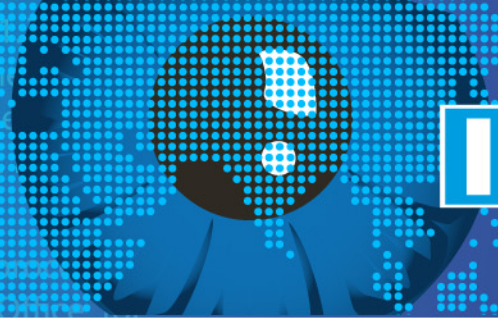
Typ	Nárůst počtu vydaných ČK Starcos v roce 2017 proti roku 2016	Nárůst počtu vydaných ČK Starcos v roce 2018 proti roku 2016
ČK klasické, včetně duálních	199 %	328 %
ČK plug-in a token	127 %	155 %

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 (serverové)	83 % nárůst počtu vydaných certifikátů mezi roky 2015 – 2018.

eOP jako QSigCD



I.CA umožňuje vydávání kvalifikovaných certifikátů pro elektronický podpis, kdy je soukromý klíč generován a uložen 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 srpna 2019 41 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**.

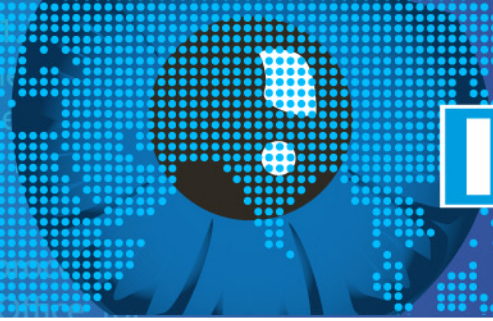
- v prostředku (na serveru) klienta pro vytváření **zaručených elektronických pečetí**. Tyto certifikáty často postupně nahrazují (kvalifikované) systémové certifikáty, které I.CA na žádost klientů stále ještě vydává. Staly se však komerčními certifikáty.

Služba vzdáleného pečetění

- POZOR!!! **Služby typu vytváření kvalifikovaných elektronických podpisů/pečetí na dálku nejsou a nemohou být kvalifikovanou službou vytvářející důvěru ve smyslu nařízení eIDAS,** proto nejsou uvedeny ve zveřejněném "Seznamu kvalifikovaných poskytovatelů služeb vytvářejících důvěru a poskytovaných kvalifikovaných služeb vytvářejících důvěru„.
- Ministerstvo vnitra jako orgán dohledu na žádost I.CA posoudilo službu I.CA RemoteSeal (před jejím spuštěním) a neshledalo rozpor oznámených změn v poskytování kvalifikované služby vytvářejících důvěru vydávání kvalifikovaných certifikátů pro elektronické pečetě s platnými právními předpisy upravující podmínky poskytování kvalifikovaných služeb vytvářejících důvěru. Toto zjištění oznámilo na svém webu.

Viz: https://www.mvcr.cz/clanek/oznameni-o-udeleni-souhlasu-s-poskytovanim-sluzby-vytvareni-kvalifikovanych-elektronickych-peceti-na-dalku-poskytovatel-prvni-certifikacni-autorita-a-s.aspx

1.000.000 pečetí vytvořených I.CA RemoteSeal



První milion vytvořených/odebraných kvalifikovaných pečetí na dálku byl zaznamenán v 06/2019.

Tato pečeť byla vytvořena prostřednictvím společnosti Gordic spol. s r.o. v rámci spisové služby GINIS.

Služba je nabízena jednak přímo, jednak prostřednictvím dodavatelů spisových služeb (integrace služby pečetění do spisové služby).

Spolupracující producenti systémů spisových služeb: Gordic spol. s r.o. (GINIS), VERA, spol. s r.o. (Radnice, Dimenze) a PilsCom, s.r.o., resp. S&T (AthenA). V jednání ICZ a.s. (e-spis).

Kdy je nezbytné nahradit značku pečetí

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

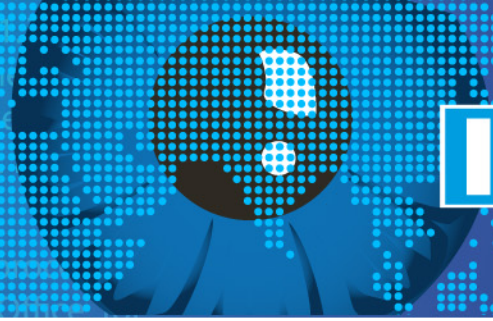
- Elektronickou pečetí může dokument opatřit pouze **původce dokumentu** – pozor při příjmu elektronických dokumentů.

  nařízení eIDAS

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

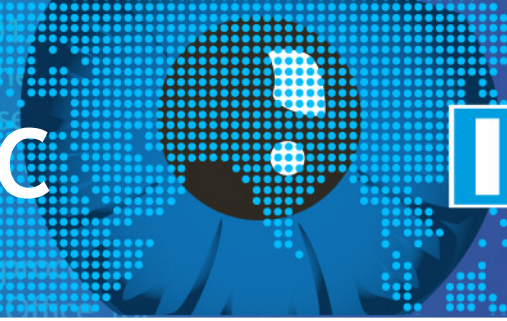
  nařízení eIDAS

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.

Certifikáty založené na ECC



V rámci podpory nových technologií zahájila I.CA dne 15. 7. 2019 **vydávání certifikátů založených na ECC, tj. na eliptických křivkách.**

Vydávány jsou:

- Kvalifikované certifikáty pro elektronický podpis
- Kvalifikované certifikáty pro elektronickou pečeť
- Komerční certifikáty
- Komerční technologické (serverové) certifikáty.

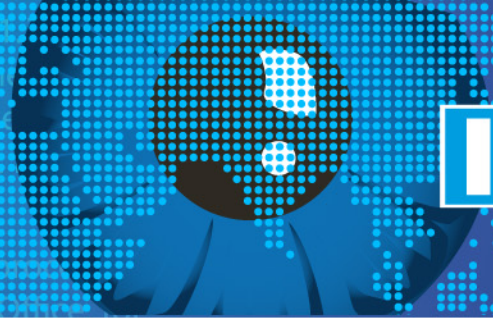
Stávajících i budoucích uživatelů certifikátů založených na algoritmu RSA se tato změna v dohledné době žádným způsobem nedotkne.

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 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, pečetí a časových razítek u přijatých elektronických dokumentů dle § 4 odst. 4) až 7) vyhlášky č. 259/2012 Sb., o podrobnostech výkonu spisové služby.

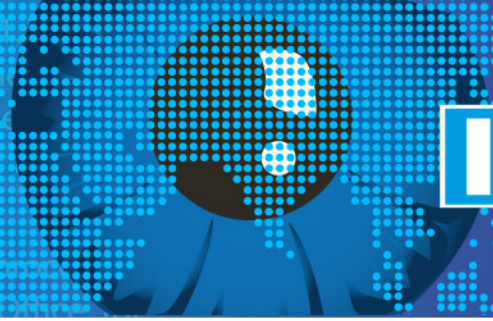
Novela této vyhlášky č. 85/2019 Sb. s účinností od 07/2019 i nadále tuto povinnost stanoví, a to následovně:

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.

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 let. 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.).

I.CA jako kvalifikovaný správce

Nařízení eIDAS

- služby vytvářející důvěru (certifikáty, razítka….)

- elektronická identifikace jako nástroj pro bezpečné a zaručené ověření totožnosti uživatele online služeb.

I.CA podala žádost MV o akreditaci jako **kvalifikovaný správce 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.

I.CA je v ČR prvním žadatelem o tuto akreditaci, příprava i realizace jsou technicky, finančně a časově velmi náročné.

eIdentifikace v ČR podle eIDAS

Prostředky pro elektronickou identifikaci - stát:

- **eOP** – poskytovatelem prostředku je stát, úroveň záruky vysoká
- **Jméno, heslo, SMS** – poskytovatelem je SZR, úroveň záruky značná

Poskytovateli služby jsou např. eRecept, ePortál ČSSZ, Portál občana.

Prostředky pro elektronickou komunikaci - komerční subjekty:

- **Starcos 3.5** – poskytovatelem prostředku bude I.CA, úroveň záruky vysoká

Předpokládanými poskytovateli služby budou zejména finanční instituce.

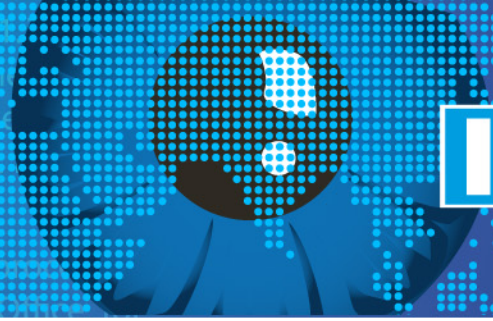
Význam nařízení eIDAS pro I.CA

- 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

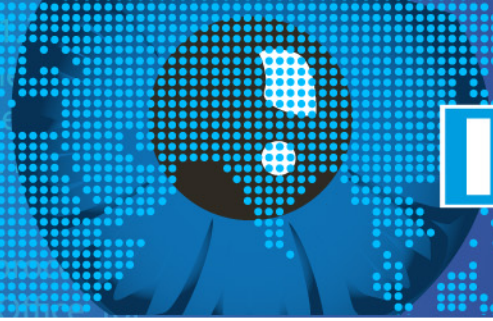
- Přetrvává nezbytnost upřesnění/výkladu některých ustanovení nařízení eIDAS, a tedy stálého kontaktu s orgány EK, s ENISA a dalšími orgány EU a samozřejmě s pracovníky MV.
- Co nás trápí – problémy s používáním certifikátů v některých IS provozovaných státními institucemi. Uživatel se může domnívat, 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 Správy základních registrů.

Závěr



Děkuji za pozornost.

budis@ica.cz

www.ica.cz