



První certifikační autorita, a.s. (I. CA) was founded at the beginning of November 2001. The use gained in implementation and operation of the project of commercial providing of sophisticated services in the Czech Republic is one of the determining factors for high quality services.

The most important step forward was a completion of accreditation process in sense of Law 227/2000 about electronic signature and cohering edicts. The Office for Personal Data Protection conferred I. CA a certificate of accreditation provider of certification services in the Czech Republic with effectiveness since 10th of May 2002. In 2006 I. CA get certificate of accreditation provider of certification services in the Slovak Republic Law 215/2002 about electronic signature too.

In both countries I. CA provide time stamp services, advanced electronic signature services too.

# eIDAS

## Position on the Market

Our company is currently the biggest provider of certification services in the Czech and Slovak Republic. Demands of clients are met through an infrastructure of so-called registration authorities, recently having expanded the number of 400 in count. Their spread over the whole territory of the country is a notable competitive advantage. These contacting offices thus provide optimum accessibility of our products and services.

The quantity of certificates issued in the Czech Republic is also unmatched. Their number has reached six-digit numbers. These competitive advantages enable the company to continuously develop its product portfolio as well as improve quality of services provided.

## Smart Cards & Devices Forum 2016

### Mgr. Dagmar Bosáková

A digital certificate is a technical personal identity card, it even contains similar set of information. First of all, it explicitly connects physical and electronic identities.

Validity of certificates is limited and is among the information contained in the certificate. This value is of paramount importance. Developments in performing power of computer technology has chances, however remote, of breaking of protocols and algorithms could in long-term void the reliability of digital certificates. Regularly issued certificates bear six-month validity. Validity of a certificate can be nullified even during the period if required e.g. by disclosure of private key of the certificate.

Nullified certificate is registered in the list of nullified certificates (CRL). The list of void certificates is therefore a set of published nullified certificates with unique serial numbers of void



# Nařízení eIDAS



## **Nařízení Evropského parlamentu a Rady č. 910/2014 ze dne 23. července 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**

Je účinné ve všech členských státech přímo, nebude „implementováno“ žádným českým právním předpisem. Doplněno bude českým adaptačním zákonem.

Rozdíl oproti směrnici č. 1999/93/ES, která byla implementována zákonem č. 227/2000 Sb., o elektronickém podpisu.

[http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L\\_.2014.257.01.0073.01.ENG](http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG)

# Nařízení eIDAS – oblasti úpravy



1. Elektronická identifikace
2. Elektronický dokument
3. Služby vytvářející důvěru – poskytovatelé služeb vytvářejících důvěru

Kvalifikované služby vytvářející důvěru poskytované kvalifikovanými poskytovateli služeb vytvářejících důvěru (dosud „akreditovaní poskytovatelé“)

# E-identifikace, e-dokument



## E-identifikace

V ČR připravuje ministerstvo vnitra – na eOP s čipem bude uložen identifikační certifikát pro přístup ke službám eGovernmentu.

Cílový stav: přístup ke službám přes hranice členských států.

## E- dokument

„Elektronickému dokumentu nesmějí být upírány právní účinky a nesmí být odmítán jako důkaz v soudním a správním řízení pouze z toho důvodu, že má elektronickou podobu.“

nařízení eIDAS

# Služby vytvářející důvěru



- Vydávání
  - kvalifikovaných certifikátů pro elektronické podpisy
  - kvalifikovaných certifikátů pro elektronické pečeti
- Kvalifikovaná služba **ověřování**
  - platnosti kvalifikovaných elektronických podpisů / uchování
  - platnosti kvalifikovaných elektronických pečetí / uchování
- Kvalifikovaná služba **vydávání kvalifikovaných elektronických časových razítek**
- Kvalifikovaná služba **vydávání kvalifikovaných certifikátů pro autentizaci internetových stránek**
- Kvalifikovaná služba **elektronického doporučeného doručování**

# Zachování kontinuity služeb



- **Vydávání kvalifikovaných certifikátů pro elektronické podpisy – pokračuje od 1. 7. 2016, I.CA se stává podle nařízení eIDAS kvalifikovaným poskytovatelem pro tuto službu.**
- **Kvalifikované certifikáty vydané do 30. 6. 2016 zůstávají platné po dobu, na kterou byly vydány.**
- **Zahájení poskytování dalších kvalifikovaných služeb je podmíněno provedením posouzení shody (auditem).**
- **Audit mohou provádět pouze k tomu oprávněné subjekty, které teprve budou určeny Českým institutem pro akreditaci (ČIA).**

nařízení eIDAS

# Právní úprava v České republice



## Nařízení eIDAS doplní

- **český adaptační zákon: zákon o službách vytvářejících důvěru pro elektronické transakce**

návrh – 2. čtení v PSP od 24. 5., sněmovní tisk č. 763, mj. zruší zákon č. 227/2000 Sb., o elektronickém podpisu

- **změnový zákon: zákon, kterým se mění některé zákony v souvislosti s přijetím zákona o službách vytvářejících důvěru pro elektronické transakce .....**

návrh – 2. čtení v PSP od 24. 5., sněmovní tisk č. 764

# Zachování kontinuity služeb - ČR



Český adaptační zákon řeší mimo jiné přechod od stávajícího právního stavu k novému podle nařízení eIDAS, a to v oblastech, ve kterých dosud neexistovala „evropská“ právní úprava.

Reaguje na zásadu, že jakákoliv služba může mít označení „kvalifikovaná“ až po provedení auditu.

Například současná kvalifikovaná časová razítka po 1. 7. 2016:

- do provedení auditu, max. 2 roky – **časová elektronická razítka vydaná kvalifikovaným poskytovatelem** (např. I.CA)
- po provedení auditu – **kvalifikovaná elektronická časová razítka.**



# Kvalifikovaný elektronický podpis



- Pouze „kvalifikovaný elektronický podpis“ má právní účinek rovnocenný vlastnoručnímu podpisu.

nařízení eIDAS

- Kvalifikovaný elektronický podpis založený na kvalifikovaném certifikátu vydaném v jednom členském státě se uznává jako kvalifikovaný elektronický podpis ve všech ostatních členských státech.

nařízení eIDAS

- ZEP + kvalifikovaný certifikát + QESigCD

# Požadavky na QESigCD



- Nestačí, aby pouze čip byl hodnocen na EAL 4+ podle Common Criteria.
- Aby prostředek mohl být prohlášen za SSCD či QESigCD, musí být osazen kombinací certifikovaného čipu a appletu, tj. **certifikace musí být provedena pro kombinaci konkrétního čipu a appletu.**

# Doložení požadavků na QESigCD



Doložení, že prostředek je bezpečným prostředkem podle eIDAS, je možné:

a) dokladem o provedeném hodnocení prostředku podle standardu CWA 14169 – Secure signature-creation device (do července 2014) na úroveň EAL4+, a to **licencovanou zkušební laboratoří** na shodu s jedním z těchto dokumentů:

- [Protection Profile - Secure Signature-Creation Device Type 1, Version 1.05 \(BSI-PP-0004-2002\)](#)
- [Protection Profile - Secure Signature-Creation Device Type 2, Version 1.04 \(BSI-PP-0005-2002\)](#)
- [Protection Profile - Secure Signature-Creation Device Type 3, Version 1.05 \(BSI-PP-0006-2002\)](#)

b) dokladem o provedeném hodnocení prostředku (od července 2014) podle standardu EN 419 211 – Protection profiles for secure signature creation device) na úroveň EAL4 augmented with AVA\_VAN.5, a to **licencovanou zkušební laboratoří** na shodu s jedním z těchto dokumentů:

- [EN 419 211-2 \(BSI-CC-PP-0059-2009\)](#)
- [EN 419 211-3 \(BSI-CC-PP-0075-2012\)](#)
- [EN 419 211-4 \(BSI-CC-PP-0071-2012\)](#)
- [EN 419 211-5 \(BSI-CC-PP-0072-2012\)](#)
- [EN 419 211-6 \(BSI-CC-PP-0076-2013\)](#).

## SSCD - QESigCD



- SSCD (Secure Signature Creation Device) se stanou automaticky QESigCD (kvalifikovanými prostředky pro vytváření podpisů) podle eIDAS. **V ČR pouze I.CA pro Starcos 3.0 a 3.2.**
- Evropská komise bude zveřejňovat **seznam certifikovaných kvalifikovaných prostředků pro vytváření elektronických podpisů**, a to na základě hlášení členských států.

nařízení eIDAS

# Podepisování dokumentů OVM - ČR



Pokud podepisuje „veřejnoprávní podepisující“ (OVM) dokument, kterým právně jedná, použije

**kvalifikovaný elektronický podpis.**

ZEP + kvalifikovaný certifikát + QESigCD (kvalifikovaný prostředek pro vytváření elektronických podpisů), např. ČK Starcos 3.0.

Přechodné ustanovení: 2 roky, cca do 30. 6. 2018, je možné používat rovněž

**ZEP+ kvalifikovaný certifikát (bez QESigCD).**

# Opatřování časovými razítky - ČR



Pokud podepisuje „veřejnoprávní podepisující“ (OVM) dokument, kterým právně jedná, je povinen jej opatřit **kvalifikovaným elektronickým časovým razítkem.**

Přechodné ustanovení: 2 roky, cca do 30. 6. 2018, je možné používat rovněž

**elektronická časová razítka vydaná kvalifikovanými poskytovateli.**

**Povinnost nastává 1. 7. 2016!!!**

# Podepisování dokumentů určených OVM v ČR



Pokud se podepisuje dokument, kterým se právně jedná vůči veřejnoprávnímu podepisujícímu, použije se

**uznávaný elektronický podpis,**

tj.

- ZEP + kvalifikovaný certifikát (bez ČK), nebo
- kvalifikovaný elektronický podpis = ZEP + kvalifikovaný certifikát + QESigCD.

# Pečetění dokumentů



## e- značka *versus* e-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 **právníckou osobu**.

nařízení eIDAS



# Pečetění dokumentů OVM



Pokud pečetí „veřejnoprávní podepisující“ (OVM) dokument, kterým právně jedná, použije

**kvalifikovanou elektronickou pečeť.**

zaručená elektronická pečeť + kvalifikovaný certifikát pro elektronickou pečeť + QESealCD (kvalifikovaný prostředek pro vytváření elektronických pečetí).

# Pečetění dokumentů určených OVM



Pokud se pečetí dokument, kterým se právně jedná vůči veřejnoprávnímu podepisujícímu, použije se

**uznávaná elektronická pečeť,**

tj.

- elektronická pečeť + kvalifikovaný certifikát pro elektronickou pečeť, nebo
- kvalifikovaná elektronická pečeť = elektronická pečeť + kvalifikovaný certifikát pro elektronickou pečeť + QESealCD.

# Pečetění dokumentů



Přechodné ustanovení: 2 roky, cca do 30. 6. 2018, je možné k pečetění při právním jednání používat rovněž

**elektronickou značku + systémový certifikát vydaný akreditovaným/kvalifikovaným poskytovatelem**

(používá se dosud jako „uznávaná elektronická značka založená na kvalifikovaném systémovém certifikátu“)

nebo

**elektronickou pečeť + certifikát pro elektronickou pečeť vydaný kvalifikovaným poskytovatelem.**

# Poznámka k přechodným ustanovením



- Přechodná ustanovení českého adaptačního zákona jsou použitelná pouze v ČR.
- Dokumenty komunikované do jiných členských států musí splňovat požadavky nařízení eIDAS.

# Závěr

První certifikační autorita, a.s., (I. CA) was established at the beginning of the year 2000. It is a company of own expertise and experience gained in implementation and operation of the first one in a field of commercial providing of sophisticated services in the area of issuing and administration of digital certificates in the Czech Republic. The determining factors for high quality of provided services.

The most important step forwards was a successful completion of accreditation process in accordance with sense of Law 227/2000 about electronic signature and e-signing edicts.



[bosakova@ica.cz](mailto:bosakova@ica.cz)