

# **Má elektronický podpis identifikovat podepsanou osobu?**

## **A pokud ano: jak?**

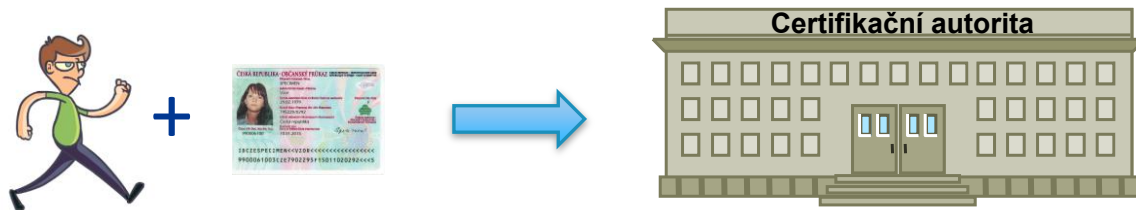
Jiří Peterka

nezávislý konzultant a publicista

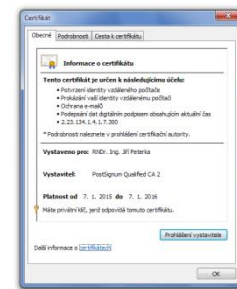
pedagog na MFF UK

# jak funguje (uznávaný) el. podpis?

- pro vystavení kvalifikovaného certifikátu se musíte dostavit osobně
- a předložit certifikační autoritě (CA) své osobní doklady



- důsledek:
  - vydavatel certifikátu (CA) zná vaši identitu
- otázka:
  - „kolik“ ze svých znalostí vaší identity má CA přenést do certifikátu?



# co je v silách el. podpisu?

- upřesnění:
  - bavíme se o uznávaném el. podpisu (a komunikaci s veř. správou)
    - od 1.7.2016: půjde o kvalifikovaný el. podpis (nařízení 910/2014: eIDAS)

- princip fungování:

- identita (fyzické) osoby je zjištěna dostatečně spolehlivě a přesně
  - jednorázově, při žádosti o vydání kvalifikovaného certifikátu (provádí CA)
  - může být přenesena (vložená) do certifikátu
- certifikát je veřejný a je připojen ke každému el. podpisu
  - důsledek: jednoznačná informace o identitě držitele certifikátu může být k dispozici spoléhající se straně (příjemci podepsaného dokumentu)
    - a za správnost identifikace ručí certifikační autorita



- důsledek:

- **uznávaný el. podpis může mít „stejnou sílu“ jako úředně ověřený (vlastnoruční) podpis**



# srovnání „síly“ různých podpisů

	Vlastnoruční	Ověřený (vlastnoruční)	Uznávaný (kvalifikovaný) el. podpis
Existence podpisu	<b>ANO</b>	<b>ANO</b>	<b>ANO</b>
Identifikace podepsané osoby	<b>NE</b>	<b>ANO</b> (znovu při každém podpisu)	<b>ANO</b> (jednorázově, při vydání certifikátu)
Pravost / neodmítnutelnost	<b>NE</b>	<b>ANO</b> (ručí za to ověřující)	<b>ANO</b> (dáno technicky/asymetr. kryptogr.)

- vlastnoruční podpis
  - nezajišťuje (vždy) identifikaci podepsané osoby
    - z „klikyháku“ nic nepoznáme
      - není předepsána podoba podpisu
  - ověření (pravosti) musí provádět (písmo)znalec
    - je to drahé, dělá se až při sporu



„klikyhák“

# zásadní otázky

- má být (uznávaný) elektronický podpis postaven na roveň
  - a. ověřenému (vlastnoručnímu) podpisu?
  - b. vlastnoručnímu podpisu?

Situace:	Uznávaný el. podpis odpovídá:
dnes v ČR	není definováno (v praxi: vlastnoručnímu, ale jsou výjimky)
dnes na Slovensku	ověřenému podpisu (je-li připojeno časové razítko)
od 1.7.2016 (nařízení 910/2014, eIDAS)	vlastnoručnímu podpisu

- jiná otázka:
  - **má el. podpis vůbec sloužit k identifikaci podepsané osoby?**
    - část „lidí kolem el. podpisů“ se domnívá, že NE
      - je to konzistentní s tím, že vlastnoruční podpis také nezajišťuje identifikaci podepsané osoby (viz „z klikyháku nepoznáme nic“)

# jak to řeší na Slovensku?

- vkládají do certifikátu rodné číslo držitele
- přitom: certifikát je (musí být) veřejný !!!
  - pokud má být veřejný i podepsaný dokument



§ 5 zákona č. 215/2002 Sb. (o elektronickom podpise):

Ak sa v styku s orgánmi verejnej moci používa zaručený elektronický podpis, kvalifikovaný certifikát musí byť vydaný akreditovanou certifikačnou autoritou a musí obsahovať rodné číslo držiteľa certifikátu.

Pole	Hodnota
Sériové číslo	00 a3 20 40
Algoritmus podpisu	sha256RSA
Podpisový algoritmus hash	sha256
Vystaviteľ	I.CA - Accredited Provider of ...
Platnosť od	12. ledna 2012 11:19:16
Platnosť do	11. ledna 2013 11:19:16
Subjekt	PNOSK 6505046955, ICA - 10...
Veřejný klíč	RSA (2048 Bits)

SERIALNUMBER = PNOSK 6505046955  
SERIALNUMBER = ICA - 10149876

E =  
O = MANDAT CONSULTING, k.s.  
CN =  
C = SK

Ministerstvo vnútra  
(SK) zverejňuje  
certifikáty úradníkov

rodné číslo držiteľa

SERIALNUMBER = PNOSK 6505046955  
SERIALNUMBER = ICA - 10149876

Ing. Vladimír Ďuračková, ...  
www.mv.gov.sk/durackova\_2013

Ministerstvo vnútra  
Slovenskej republiky

Sekcie MV SR

Úvodná stránka MV SR | Verejná správa

Yerejná správa / Živnostenské podnikanie / ZEP / Trenčanský kraj / Okresný úrad Prievidza | Ďuračková 2013

Ing. [redacted]

Okresný úrad Bánovce nad Bebravou | Okresný úrad Nové Mesto nad Váhom | Okresný úrad Považská Bystrica | Okresný úrad Prievidza | Okresný úrad Trenčín

Vydavateľ: C = CZ, CN = I.CA - Qualified Certification Authority, 09/2009, O = První certifikační autorita, a.s., OU = I.CA - Accredited Provider of Certification Services

Sériové číslo: 00 a3 1c c7

Algoritmus: RSA Encryption

Úvodná stránka  
Aktuálne informácie  
Publikácie  
Okresné úrady  
Odborová organizácia  
Voľby a referendum  
Výškový program ISO

Subjekt: C = SK, CN = OPRAVNENIE 1 JRM, O = MANDANT Ministerstvo vnútra Slovenskej republiky, O = Okresný úrad Prievidza, O = SN = ICA - 10340639, SN = IDCSR-EB610133, SN = NTRSK-00151866, SN = NTRSK-MANDANT 00151866, SN = PNOSK-6260047090

SN = PNOSK 6260047090

# současný stav v ČR

- „tuzemský“ kvalifikovaný certifikát (pro uznávaný podpis):
  - musí obsahovat údaje, které umožňují jednoznačnou identifikaci

§11 odst. 3 zákona č. 227/2000 Sb.: Uznávaným elektronickým podpisem se rozumí  
a) zaručený elektronický podpis založený na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb a **obsahujícím údaje, které umožňují jednoznačnou identifikaci podepisující osoby**

- o jaké údaje se jedná?
  - to říká vyhláška č. 212/2012 – ale špatně !!!!

údaj, který umožňuje jednoznačnou identifikaci podepisující osoby, se uvádí ve struktuře desetimístného čísla v desítkové soustavě v rozsahu 1 100 100 100 až 4 294 967 295.

- neříká, co má toto číslo znamenat – jaký identifikátor to má být
  - když si do certifikátu napíšu 1 111 111 111, bude to OK (ale k ničemu) !!

# současná praxe v ČR

- do certifikátů se vkládá IK MPSV
  - přímo v CN (eIdentity)
  - v ASCII kódu v jiné položce (I.CA a PS)

Certifikát

Obecné Podrobnosti Cesta k certifikátu

Zobrazit: <Vše>

Pole	Hodnota
Vystavitel	ACAEID2 - Qualified Issuing C...
Platnost od	17. srpna 2011 17:11:34
Platnost do	17. srpna 2012 17:11:34
<b>Subjekt</b>	<b>MPSV-1680937599, jiri@peter...</b>
Veřejný klíč	RSA (2048 Bits)
Identifikátor klíče předmětu	ec 58 ab ea 3a fe fb 5b fb 12 ...
Zásady certifikátu	[1]Certifikační zásady:Identifik...
Základní omezení	Typ předmětu=Koncová entita

SERIALNUMBER = MPSV-1680937599  
E = jiri@peterka.cz  
CN = RNDr. Ing. Jiří Peterka  
OU = Clients  
O = eIdentity a.s.  
C = CZ

IK MPSV v „plain text-u“

Certifikát

Obecné Podrobnosti Cesta k certifikátu

Zobrazit: Pouze přípony

Pole	Hodnota
<b>Alternativní název předmětu</b>	<b>Název RFC822=jiri@peterka.c...</b>
Základní omezení	Typ předmětu=Koncová entita...
Zásady certifikátu	[1]Certifikační zásady:Identifik...
Prohlášení kvalifikovaného c...	30 0a 30 08 06 06 04 00 8e 46...
Přístup k informacím autority	[1]Přístup k informacím autorit...
Identifikátor klíče autority	ID klíče=89 e8 4c df 8b 26 39 ...
Distribuční místa seznamu o...	[1]Distribuční místo CRL: Náze...
Identifikátor klíče předmětu	7c 5a 8c 21 c7 04 00 73 77 6a

Název RFC822=jiri@peterka.cz  
Jiný název:  
1.3.6.1.4.1.11801.2.1=13 0a 31 36 38 30 39 33 37 35 39 39  
Jiný název:  
Description=13 00

IK MPSV v ASCII kódu

v certifikátu je vždy uvedeno jméno a příjmení držitele (nebo pseudonym)



# znovu základní otázka:

---

- CA zná (zcela přesně) identitu držitele certifikátu
- ale: „jak moc“ má tuto identitu znát spoléhající se strana?
  - tj. příjemce podepsaného dokumentu
    - což může být i soukromá osoba (nebo privátní subjekt) !!!
- možnosti:
  - a. **nemusí ji znát vůbec** (a musí si poradit nějak jinak)
    - jako u vlastnoručního podpisu
      - ale proč se pak v certifikátu vůbec uvádí jméno a příjmení?
  - b. **zná ji „jen rámcově“**, a jednoznačně pouze „potenciálně“
    - zná jen jméno a příjmení (což nepostačuje pro jednoznačnou identifikaci)
    - další údaje o identitě (nutné k jednoznačné identifikaci) může získat:
      - OVM: může se kdykoli „zeptat“ na držitele IK MPSV
      - soukromá osoba, privátní subjekt: musí vyvolat soudní spor
        - soud se pak může „zeptat“ CA, komu certifikát vydala
  - c. **zná ji jednoznačně** („aktuálně“, nikoli jen „potenciálně“)

# nařízení 910/2014 (eIDAS)

---

- říká:
  - *„chci, aby kvalifikovaný el. podpis měl stejnou váhu jako vlastnoruční podpis“*
    - názor: je to krok zpět – způsobený tím, že některé členské země neznají ověřený (vlastnoruční) podpis
  - v kvalifikovaném certifikátu má být jméno (a příjmení) držitele
    - další položky tam mohou být, ale jen dobrovolně
      - nesmí být povinné, a celkový „efekt“ musí být stejný, jako když tam nejsou
- požaduje:
  - aby spoléhající se strana mohla ověřit (kvalifikovaný) el. podpis jako platný, musí jí být (řádně) poskytnuta unikátní data, identifikující držitele certifikátu (a tím i podepsanou osobu)

provided that ..... the unique set of data representing the signatory in the certificate is correctly provided to the relying party

# jak rozumět nařízení eIDAS?

---

- požaduje pro spoléhající se stranu „jednoznačnou identifikaci“, nebo jen „unikátní identifikátor“?
  - spíše jde o unikátní identifikátor (viz „a unique set of data ...“)
- požaduje „aktuální“ možnost jednoznačné identifikace, nebo jen „potenciální“ možnost (pro případ sporu)?
  - vypadá to spíše na „potenciální“ možnost
    - tedy v zásadě stejně, jako je to dnes
- jaké údaje má mít k dispozici spoléhající se strana?
  - jak konkrétně má vypadat onen „unique set of data“?
    - mají to být jiná data než ta, která jsou již obsažena v certifikátu?
      - možná interpretace: *certifikát může obsahovat něco jako IK MPSV (či AIFO nebo VIFO), ale nepovinně. Pokud jej neobsahuje, musí jej podepsaná osoba dodat spoléhající straně nějak jinak.*
    - protiargument: **pro potenciální identifikaci (při sporu, který řeší soud) postačuje sériové číslo certifikátu a identita vydavatele !!!!**

**děkuji za pozornost**

**Jiří Peterka**

<http://jiri.peterka.cz>

<http://www.earchiv.cz>

<http://www.bajecnysvet.cz>

<http://www.muzeuminternetu.cz>