Spôsoby uvádzania identity osôb zabezpečujúcich hodnovernosť a ochranu elektronických údajov pomocou elektronickej pečate alebo elektronickým podpisom

eFOCUS

Štátom spravovaná identita osôb a orgánov verejnej moci v kvalifikovaných certifikátoch

Ing. Peter Rybár, Sekcia IBEP, Národný bezpečnostný úrad SR
http://www.nbusr.sk/ e-mail: podatelna@nbusr.sk

Novela zákona č. 215/2002 Z. z. o elektronickom podpise

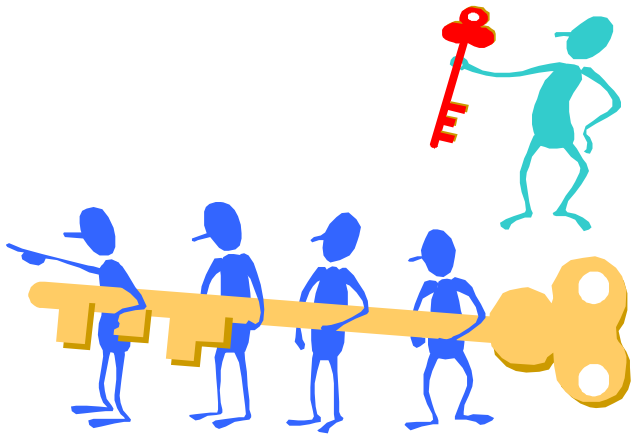
Zákon o e-Governmente novelizoval zákon č. 215/2002 Z. z. o elektronickom podpise, ktorý upravuje vzťahy vznikajúce v súvislosti s vyhotovovaním a používaním **elektronického podpisu** a **elektronickej pečate**, práva a povinnosti **fyzických osôb** a **právnických osôb** pri používaní elektronického podpisu a elektronickej pečate, hodnovernosť a ochranu elektronických dokumentov podpísaných elektronickým podpisom alebo opatrených elektronickou pečaťou.

http://www.nrsr.sk/web/Default.aspx?sid=zakony/zakon&MasterID=4500

Súkromný kľúč – len pod kontrolou konkrétnej osoby alebo zariadenia

Rovnako ako novela aj návrh nariadenia Európskeho parlamentu a Rady o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu definuje elektronickú pečať pre nefyzickú osobu: **Elektronická pečať** (seal) má zabezpečiť pôvod a neporušenosť elektronických údajov. Vyhotovenie elektronickej pečate (seal): odtlačok z elektronických údajov sa **uzamkne súkromným kľúčom. Odomknúť** odtlačok je možné len s párovým **verejným kľúčom**. Čo jeden kľúč zamkne, to odomkne len druhý kľúč z páru.

- **Súkromný kľúč** na uzamknutie odtlačku elektronického dokumentu má **len tvorca elektronickej pečate.**
- **Verejný kľúč** na odomknutie odtlačku a porovnanie s odtlačkom kópie elektronického dokumentu **je pre overovateľov** v kópiách **verejne dostupný.**
- Overenie - overovateľ porovnáva oba odtlačky elektronického dokumentu.



http://www.nbusr.sk/sk/elektronicky-podpis/overovanie.1.html

Uloženie súkromného kľúča na vyhotovenie elektronickej pečate a el. podpisu

SmartCards

USB Token

Pamäťová karta s čipom

SIM (SIM Toolkit – PKI enabled)

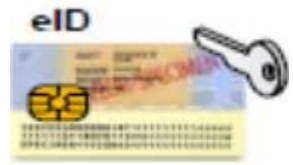
Čip na matičnej doske

Disk/pamäť PC/mobil

HSM

Disk servera














http://www.nbusr.sk/sk/elektronicky-podpis/certifikacia-produktov-pre-zep.1.html

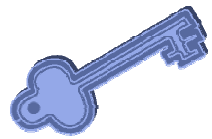
Zaručená elektronická pečať

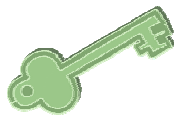
§ 4a

Zaručená elektronická pečať

Zaručená elektronická pečať je elektronická pečať, ktorá musí spĺňať podmienky podľa § 3a a zároveň

- je vyhotovená pomocou **súkromného kľúča**, ktorý je určený výlučne na vyhotovenie zaručenej elektronickej pečate,
- možno ju vyhotoviť len s použitím **bezpečného zariadenia na vyhotovovanie elektronickej pečate**,
- spôsob jej vyhotovovania umožňuje spoľahlivo určiť informačný systém, ktorej právnickej osobe alebo orgánu verejnej moci zaručenú elektronickú pečať vyhotovil,
- na verejný kľúč patriaci k súkromnému kľúču použitému na vyhotovenie zaručenej elektronickej pečate je vydaný **kvalifikovaný systémový certifikát**.





Na vyhotovenie zaručenej elektronickej pečate a ZEP

SmartCards

USB Token

Pamäťová karta s čipom

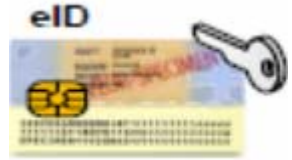
SIM (SIM Toolkit – PKI enabled)

Čip na matičnej doske

Disk/pamäť PC/mobil

HSM

Disk servera



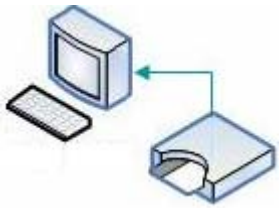
Pre ZEP - len ak je čip certifikovaný ako SSCD

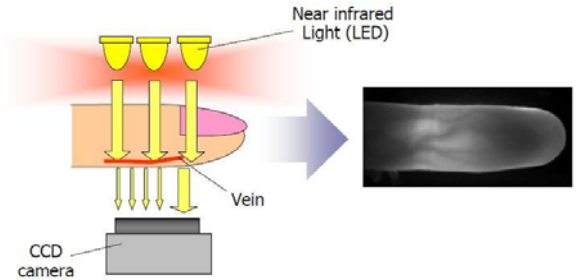
HSM nie je pre ZEP

Pre kv. pečať - HSM certifikovaný spolu s prostredím, v ktorom sa používa

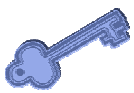
http://www.nbusr.sk/sk/elektronicky-podpis/certifikacia-produktov-pre-zep.1.html

Ochrana súkromného kľúča pred zneužitím inou osobou





bioPKI
service



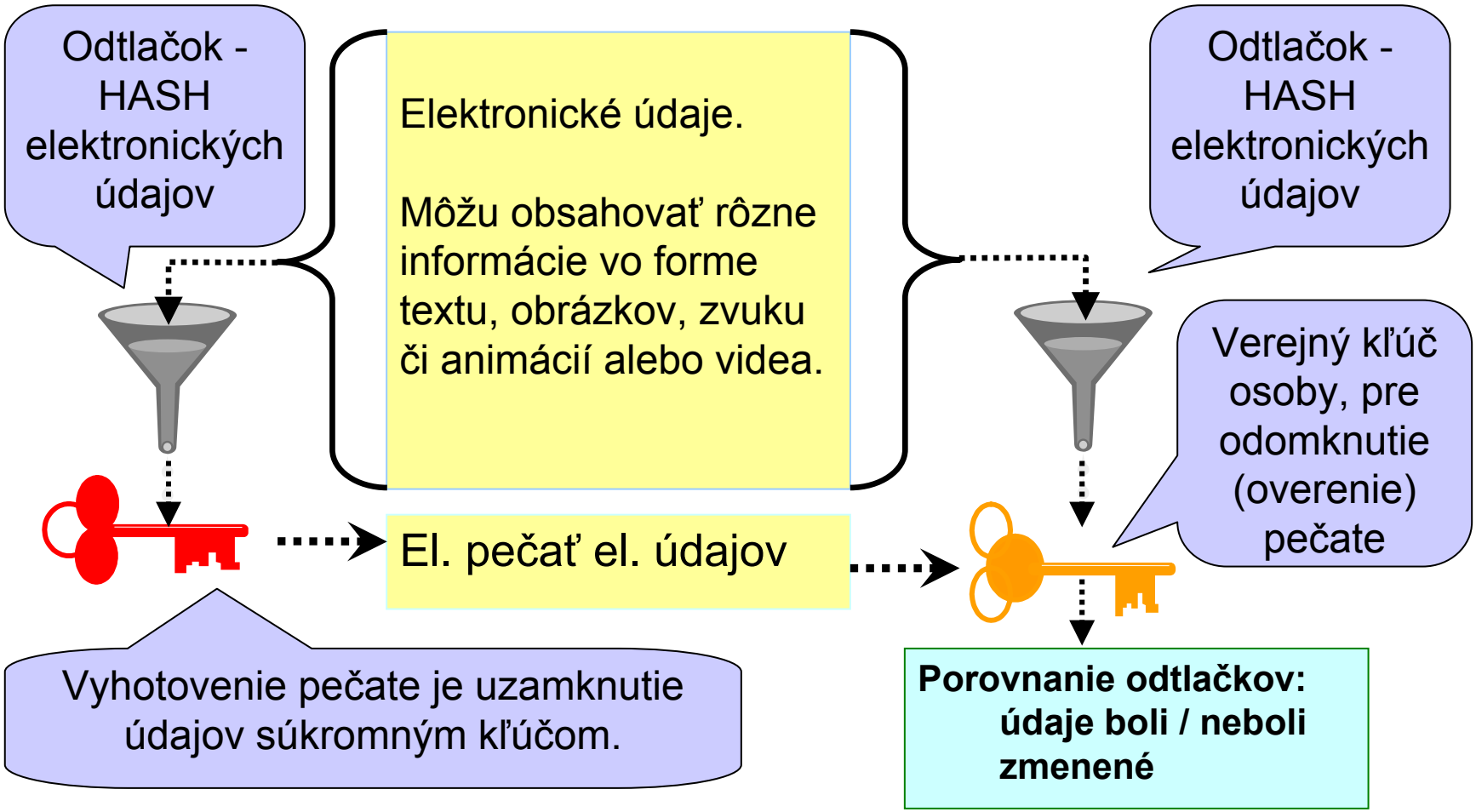
HSM

ISO/IEC DIS 17839-1
Biometric System-on-Card

ISO/IEC 24787:2010
Identification cards -- On-card biometric comparison

http://www.nbusr.sk/sk/elektronicky-podpis/certifikacia-produktov-pre-zep.1.html

Zapečatenie a overenie elektronickej pečate (seal) elektronických údajov

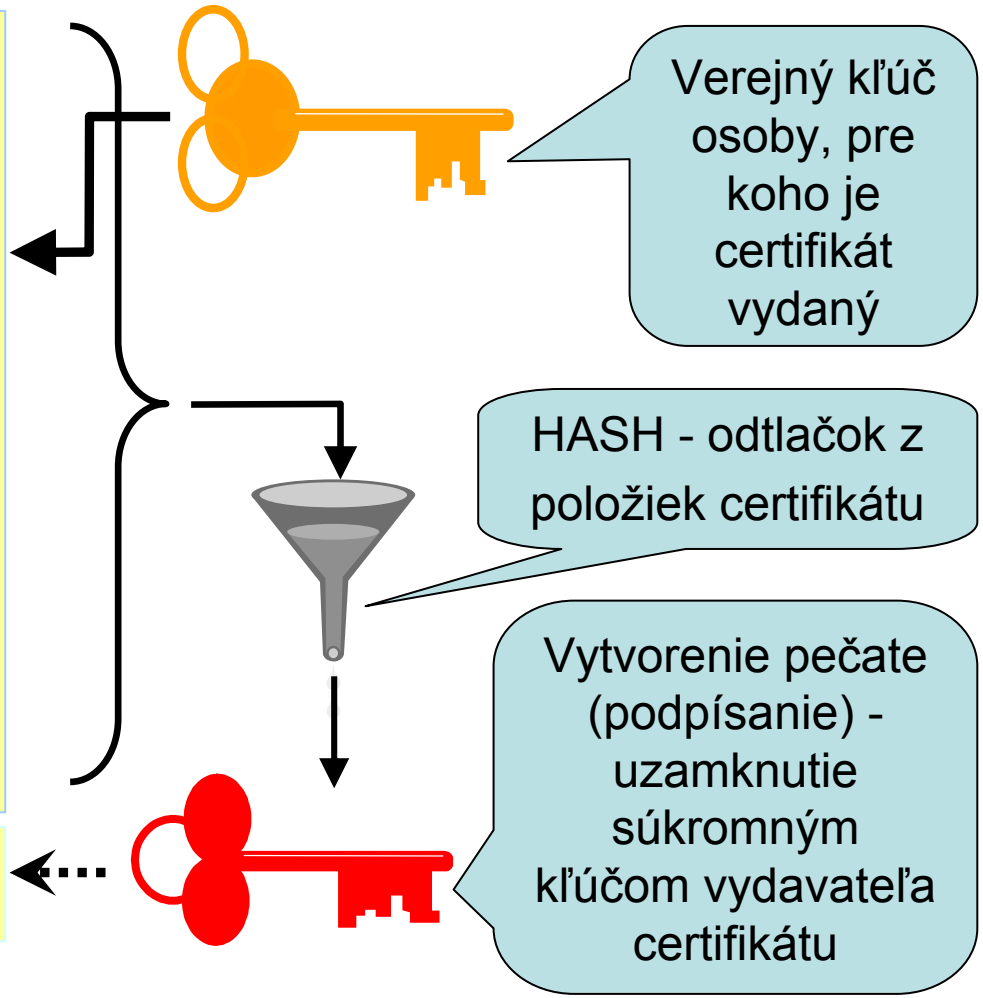


http://www.nbusr.sk/sk/elektronicky-podpis/overovanie.1.html

Obsah certifikátu podľa odporúčania ITU-T Rec. X.509|ISO/IEC 9594-8 a ETSI TS 119 412-2 Annex B.1 Identifikátor fyzickej osoby (pôvodne NBÚ štandard)

- Meno držiteľa súkromného kľúča – **subjekt** obsahuje aj rodné číslo / číslo pasu / číslo občianskeho preukazu
- **Verejný kľúč**
- Meno vydavateľa - CA
- Sériové číslo
- Čas odkedy a dokedy je možné certifikát používať
- Ďalšie voliteľné položky
  - certificatePolicies
  - subjectKeyIdentifier
  - AuthorityKeyIdentifier
  - CRL Distribution Points
  - ...

Podpis/pečať certifikátu



http://www.nbusr.sk/sk/elektronicky-podpis/standardy-nbu.1.html

Identifikátor fyzickej alebo nefyzickej osoby podľa pracovnej verzie ETSI EN 319 412-1

Natural person semantics identifier

The three initial characters have the following defined values:

"**PAS**" for identification based on passport number.

"**IDC**" for identification based on national identity card number.

"**PNO**" for identification based on (national) personal number (national civic registration number).

"**TIN**" Tax Identification Number according to the European Commission – Tax and Customs Union (http://ec.europa.eu/taxation_customs/tin/tinByCountry.html).

Two characters according to local definition within the specified country and name registration authority, identifying a national scheme that is considered appropriate for national and European level, followed by the character ":" (colon).

Other initial character sequences are reserved for future amendments of the present document.

Legal person semantics identifier

"**VAT**" for identification based on a national value added tax identification number.

"**NTR**" for identification based on an identifier from a national trade register.

EXAMPLES:

"PASSK-P3000180", "IDCBE-590082394654" and "EI:SE-200007292386".

"VATBE-0876866142" and "EI:SE-5567971433".

http://docbox.etsi.org/ESI/Open/Latest_Drafts/

Zákon o e-Governmente novelizoval zákon č. 215/2002 Z. z. o elektronickom podpise

§ 5 Používanie elektronického podpisu a elektronickej pečate

(1) V styku s orgánmi verejnej moci sa používa elektronický podpis, zaručený elektronický podpis, elektronická pečať alebo zaručená elektronická pečať.

(2) 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**.

(3) Ak sa v styku s orgánmi verejnej moci používa **zaručená elektronická pečať**, *kvalifikovaný systémový certifikát* musí byť vydaný akreditovanou certifikačnou autoritou a musí obsahovať **názov a identifikačné číslo pôvodcu pečate**.

http://www.nrsr.sk/web/Default.aspx?sid=zakony/zakon&MasterID=4500

Mandátny certifikát podľa zákona č. 215/2002 Z. z. o elektronickom podpise

V § 7 odseky 3 až 8 znejú:

(3) Mandátny certifikát je kvalifikovaný certifikát vydaný fyzickej osobe, oprávnenej zo zákona alebo na základe zákona konať za inú osobu alebo orgán verejnej moci alebo v ich mene, alebo osobe, ktorá vykonáva činnosť podľa osobitného predpisu [2b)] alebo vykonáva funkciu podľa osobitného predpisu [2c)] (ďalej len „**mandatár**"). Mandátny certifikát okrem požiadaviek podľa odseku 1 obsahuje

a) identifikačné údaje mandatára,

b) identifikačné údaje orgánu verejnej moci alebo osoby, za ktorú alebo v mene ktorej mandatár koná (ďalej len „**mandant**"),

c) identifikačné údaje orgánu verejnej moci alebo osoby, u ktorej mandatár vykonáva činnosť podľa osobitného predpisu,[2b)] alebo vykonáva funkciu podľa osobitného predpisu,[2c)]

d) označenie oprávnenia podľa § 10a ods. 2 písm. a).

(4) Mandátnym certifikátom preukazuje mandatár oprávnenie konať za alebo v mene mandanta, konať ako orgán verejnej moci alebo oprávnenie vykonávať činnosť alebo funkciu podľa odseku 3.

http://www.nrsr.sk/web/Default.aspx?sid=zakony/zakon&MasterID=4500

Obsah mandátneho certifikátu X.509, ktorý je kvalifikovaný a vydaný fyzickej osobe

Subject:	
Ján Janovič	- commonName(2.5.4.3)
Firma a.s.	- organizationName(2.5.4.10)
PNOSK-7704167689	- serialNumber(2.5.4.5)
MANDANT Ivan Vzdialený	- commonName(2.5.4.3)
MANDANT Ostrov a.s.	- organizationName(2.5.4.10)
PNOSK-MANDANT 6405067689	- serialNumber(2.5.4.5)
SK	- countryName(2.5.4.6)
Issuer:	
SK	- countryName(2.5.4.6)
Bratislava	- localityName(2.5.4.7)
Disig a.s.	- organizationName(2.5.4.10)
ACA-307-2007-2	- organizationalUnitName(2.5.4.11)
CA Disig	- commonName(2.5.4.3)

Serial Number: **0100199**
Valid From: **21.11.2013 17:06:13** UTC Valid To: **21.12.2014 17:06:13** UTC
Public Key Algorithm Identifier: **RSA Public Key Size: 2048**
Rozšírenia Certifikátu:
certificatePolicies

OBJECT IDENTIFIER 1.3.158.36061701.99.**345** označenie oprávnenia podľa § 10a ods. 2 písm. a).

uNotice Skrátený názov pre dané oprávnenie, ktoré ustanovujú všeobecne záväzné právne predpisy, a ak to nie je možné, musí byť totožné s názvom, ktorý pre dané oprávnenie určuje platný interný predpis orgánu verejnej moci alebo inej osoby, za ktorú alebo v mene ktorej sa oprávnenie vykonáva.

CPS URL http://www.disig.sk/_pdf/informacieMandatu**345**.pdf Odkaz na dokument pravidiel na výkon cert. Činností, v ktorom ACA uvedie ako plní požiadavky pri vydaní mandátu uvedené na stránke NBÚ v CP obsahujúcom zoznam mandátov.

Kvalifikovaný systémový certifikát podľa zákona č. 215/2002 Z. z. o el. podpise

V § 7 odseky 3 až 8 znejú:

(8) Kvalifikovaný systémový certifikát je kvalifikovaný certifikát, ktorý vydala akreditovaná certifikačná autorita právnickej osobe alebo orgánu verejnej moci a v ktorom je uvedené, že ide o kvalifikovaný systémový certifikát.

http://www.nrsr.sk/web/Default.aspx?sid=zakony/zakon&MasterID=4500

Obsah kvalifikovaného systémového certifikátu X.509

Subject:

Podateľňa	- commonName(2.5.4.3)
Firma a.s.	- organizationName(2.5.4.10)
ICOSK-12312345	- serialNumber(2.5.4.5)
Bratislava	- localityName(2.5.4.7)
SK	- countryName(2.5.4.6)

Issuer:

SK	- countryName(2.5.4.6)
Bratislava	- localityName(2.5.4.7)
Disig a.s.	- organizationName(2.5.4.10)
ACA-307-2007-2	- organizationalUnitName(2.5.4.11)
CA Disig	- commonName(2.5.4.3)

Serial Number: **0100189**
Valid From: **21.11.2013 17:06:13** UTC Valid To: **21.12.2014 17:06:13** UTC
Public Key Algorithm Identifier: **RSA Public Key Size: 2048**
Rozšírenia Certifikátu:
qcStatements
OBJECT IDENTIFIER 0.4.0.1862.1.1 etsiQcsCompliance
certificatePolicies
OBJECT IDENTIFIER 1.3.158.36061701.0.0.0.1.2.2 Certifikát vydaný podľa slovenskej legislatívy
OBJECT IDENTIFIER 1.3.158.36061701.xx.xx označenie, že sa jedná o kvalifikovaný systémový certifikát.
uNotice Kvalifikovaný systémový certifikát podľa zákona č. 215/2002 Z. z.
CPS URL http://www.disig.sk/_pdf/infoOVydaniKvalifikovanehoSystemovehoCrt.pdf Odkaz na dokument pravidiel na výkon cert. činností, v ktorom ACA uvedie ako plní požiadavky CP pri vydaní kvalifikovaného systémového certifikátu.

§ 10b Register systémových certifikátov zákona č. 215/2002 Z. z. o el. podpise

(1) Register systémových certifikátov je informačným systémom verejnej správy, 1) ktorého správcom je úrad.

(2) V registri systémových certifikátov vedie úrad zoznam kvalifikovaných systémových certifikátov, ktoré boli vydané orgánu verejnej moci, ako aj údaj o tom, že takýto kvalifikovaný systémový certifikát bol zrušený.

(3) Úrad zapíše do registra systémových certifikátov kvalifikovaný systémový certifikát na žiadosť orgánu verejnej moci, ktorému bol vydaný. Orgán verejnej moci, ktorému bol vydaný kvalifikovaný systémový certifikát zapísaný v registri systémových certifikátov, je povinný oznámiť úradu zrušenie tohto certifikátu bezodkladne potom, ako k zrušeniu dôjde.

(4) Úrad je povinný každý deň vydať zoznam platných kvalifikovaných systémových certifikátov podľa odseku 2 a zverejniť ho na svojom webovom sídle.

(5) Zoznam platných kvalifikovaných systémových certifikátov podľa odseku 4 platí 24 hodín od jeho vydania a kvalifikovaný systémový certifikát uvedený v zozname sa považuje za platný počas celej doby platnosti zoznamu, ak sa nepreukáže opak.

(6) Ak je kvalifikovaný systémový certifikát zrušený, úrad to bezodkladne oznámi správcovi alebo prevádzkovateľovi modulu úradnej komunikácie,2a)

http://www.nrsr.sk/web/Default.aspx?sid=zakony/zakon&MasterID=4500

Zoznam kvalifikovaných systémových certifikátov

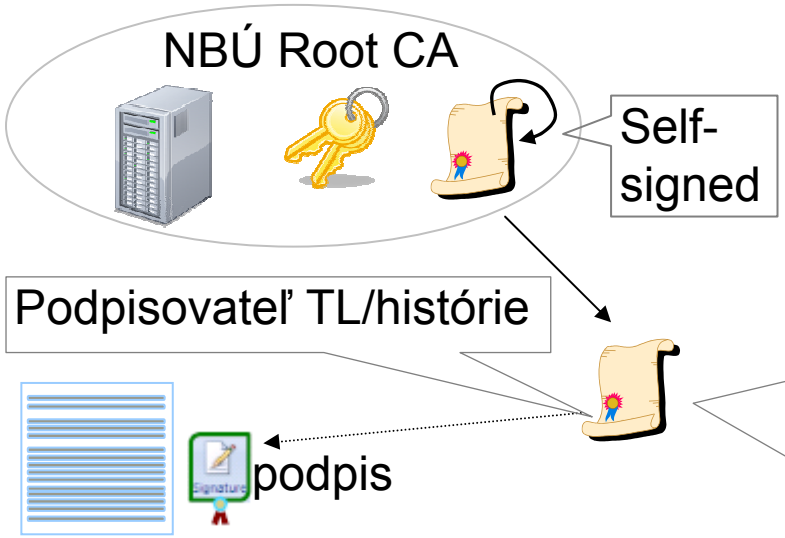
Úrad zverejňuje na svojom webovom sídle podpísaný:

1. Zoznam platných kvalifikovaných systémových certifikátov
2. Úplný zoznam kvalifikovaných systémových certifikátov (platné, zrušené a expirované pre dlhodobé overenie)

FILE=http://www.nbusr.sk/ksc/**20040114163833Z**.cer
HASH(SHA256:2 16 840 1 101 3 4 2 1)=6FBF021174831BE8B5889C9077F7BD6CDB
NOTICE=**20060114155622Z** NotAfter, **ICO**SK=12312345
FILE=http://www.nbusr.sk/ksc/**20040114163833Z**1.cer
HASH(SHA256:2 16 840 1 101 3 4 2 1)=2E95158C00DDCE98B5889C9077F7BD6C38
NOTICE=**20060114155622Z** NotAfter **ICO**SK=31234590
FILE=http://www.nbusr.sk/ksc/**20050222161337Z**.cer
HASH(SHA256:2 16 840 1 101 3 4 2 1)=E17E8EC51F376C0371B45BBEB5BD84E0F
NOTICE=**20150222154357Z** NotAfter, **ICO**SK=131583606
FILE=http://www.nbusr.sk/ksc/**20091106095939Z**.cer
HASH(SHA256:2 16 840 1 101 3 4 2 1)=D83477E0388C40BA092FECA484A5EBD38F
NOTICE=**20251106072909Z** NotAfter, **OSI**SK=11583606172

http://www.nrsr.sk/web/Default.aspx?sid=zakony/zakon&MasterID=4500

NBÚ – podpisovateľ histórie zverejňuje bezpečné algoritmy vo forme podpisovej politiky a dôveryhodné certifikáty



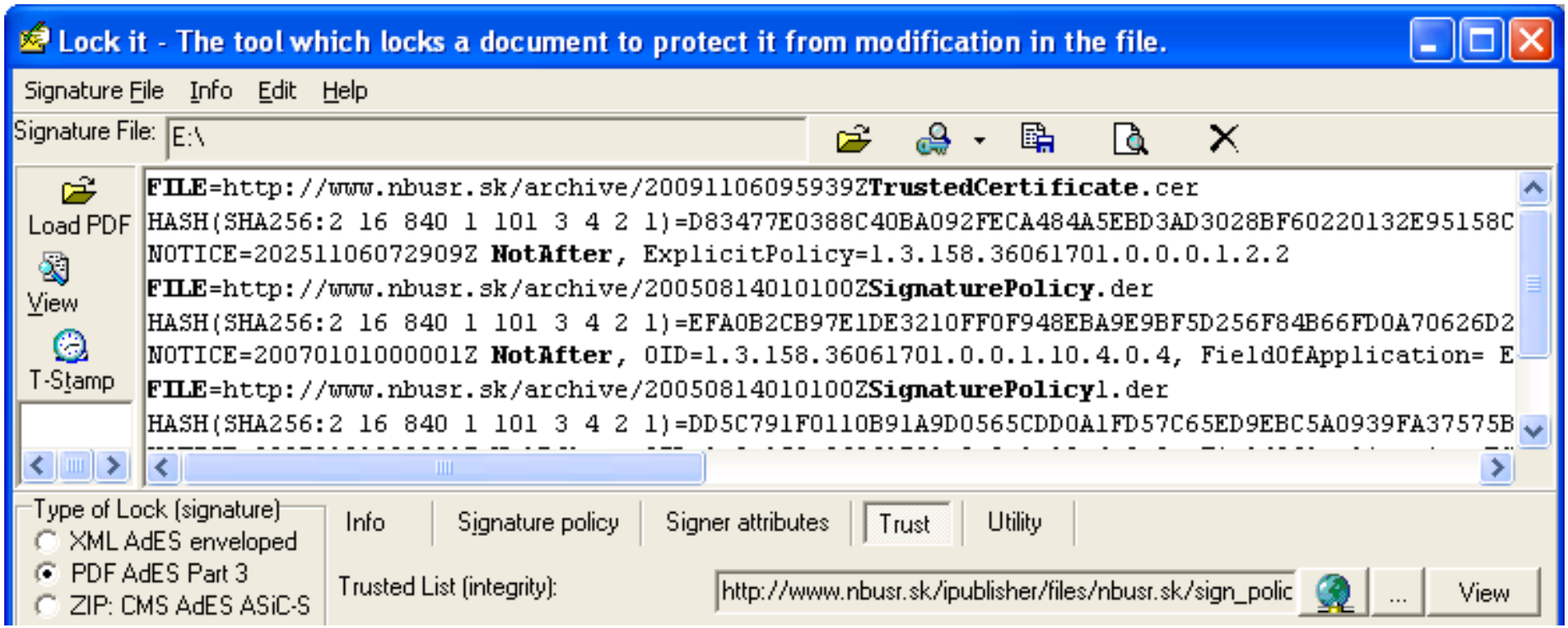
ako Signature Policy Authority

NBÚ Root CA vydáva priamo certifikát podpisovateľa TL a histórie s jednoznačným OID certifikačnej politiky pre identifikáciu tohto typu certifikátu. Zrušenie certifikátu nastáva pri skrátení doby použitia koreňového certifikátu NBÚ alebo skrátení použitia podpisovej politiky napríklad z dôvodu oslabenia bezpečnosti algoritmov.

Podpísaný zoznam koreňových NBÚ certifikátov a podpisových politík obsahuje:
- Aktuálny NBÚ Root CA certifikát a všetky expirované NBÚ Root CA certifikáty s potenciálne skrátenou dobou použitia self-signed NBÚ Root CA certifikátov.
- Aktuálne schválené podpisové politiky (schválené NBÚ ako policy authority) a všetky expirované podpisové politiky s potenciálne skrátenou dobou použitia.
- Hash hodnoty a URL na NBÚ Root certifikáty a podpisové politiky.
- Hash hodnoty a URL na certifikáty Komisie na overenie LOTL EÚ Komisie.

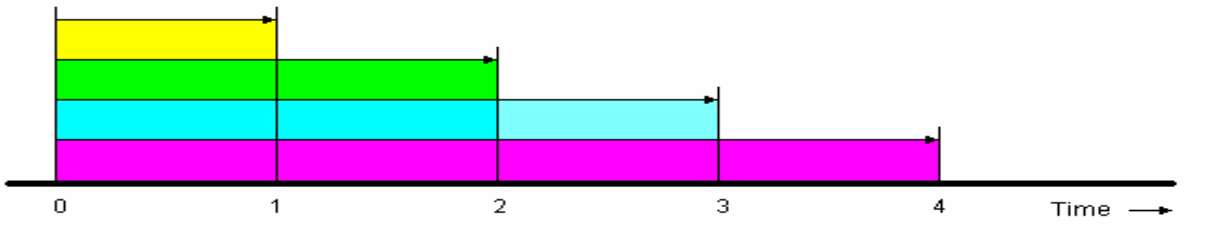
http://www.nbusr.sk/sk/elektronicky-podpis/podpisove-politiky.1.html

História a aktuálne dôveryhodné certifikáty NBÚ a EÚ a podpisové politiky



http://www.nbusr.sk/sk/elektronicky-podpis/podpisove-politiky.1.html

Časová os kritických momentov pri používaní certifikátov X.509

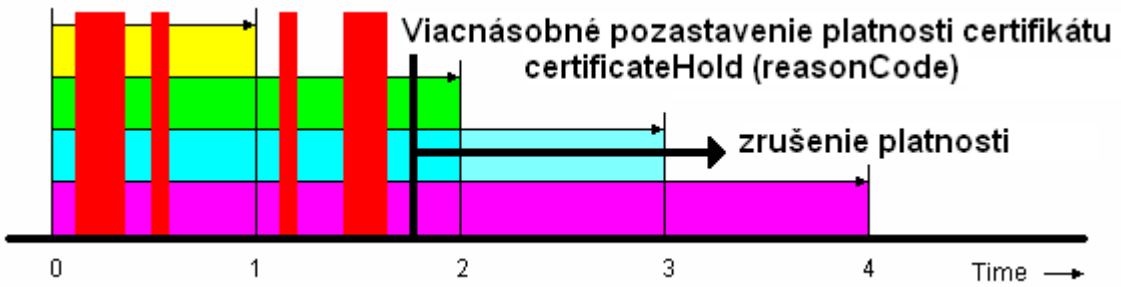


Dôležité časové momenty:

0. Čas zapečatenia elektronických údajov (seal).
1. Čas vytvorenia archívneho formátu zapečatených údajov, ktorý obsahuje všetky potrebné údaje na dlhodobé overenie.
2. Čas expirovania certifikátu (pečate), po ktorom nemusia existovať informácie na overenie platnosti.
3. Čas ukončenia väčšiny povinností certifikačnej autority(CA). Vymazanie archivovanej dokumentácie súvisiacej s vydávanými certifikátmi (§ 14 zákona 215/2002 Z. z.). Certifikačná autorita **nie je** po tomto čase zodpovedná za **spojenie identity** tvorcu pečate vlastniaceho súkromný kľúč s verejným kľúčom vo forme certifikátu, ktorý CA vydala pre tvorcu pečatí s daným kľúčom.
4. Koniec cyklického archívneho pečiatkovania elektronického podpisu pre zabezpečenie podpisu pred útokmi (kompromitácia kľúčov alebo prelomenie použitých algoritmov).

http://www.itu.int/rec/T-REC-X.509

Časová os viacnásobného pozastavenia a zrušenia platnosti certifikátu X.509



Pozor na pozastavenie platnosti certifikátu! SK legislatíva pre ZEP a niektoré systémy **nepovoľujú použitie certificateHold,** ale nový ETSI štandard to povoľuje. Ak je táto možnosť povolená, potom pre potreby auditu je potrebná analýza všetkých CRL počas celej doby použitia certifikátu, lebo transakcie vytvorené v čase, keď je certifikát v stave Hold, sa považujú za neplatné!

Aktuálne CRL a OCSP poskytuje len posledný stav certifikátu. Z toho dôvodu sa pre spätné overovanie alebo dlhodobé podpisy zakazuje používanie certificateHold, lebo tento stav je možné len komplikovane overiť. Pripravované nariadenie rovnako **zakazuje obnovenie platnosti certifikátu**!

ETSI EN 319 411 Policy and security requirements for Trust Service Providers issuing certificates; (tieto politiky umožňujú pozastavenie platnosti!)

- Part 2: Policy requirements for certification authorities issuing qualified certificates
- Part 3: Policy requirements for Certification Authorities issuing public key certificates

http://www.itu.int/rec/T-REC-X.509

Podmienka z ITU-T Rec. X.509|ISO/IEC 9594-8 pri rušení platnosti certifikátu

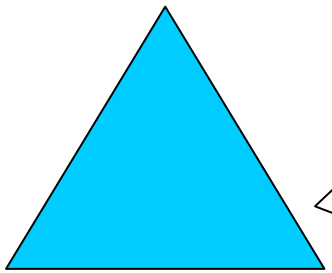
Čas, kedy CA zruší certifikát, nesmie predchádzať čas vydania aktuálneho (naposledy vydaného) CRL alebo OCSP (položka **thisUpdate** v CRL alebo OCSP).

To znamená, že nie je možné spätné zrušenie certifikátu pred časom uvedeným v položke thisUpdate z posledného CRL alebo OCSP. Vďaka tomu stačí nájsť alebo počkať na CRL alebo OCSP s hodnotou času v thisUpdate, ktorá je po čase ku ktorému overujeme. Potom sme si istí, že stav certifikátu sa k tomuto času už nezmení.

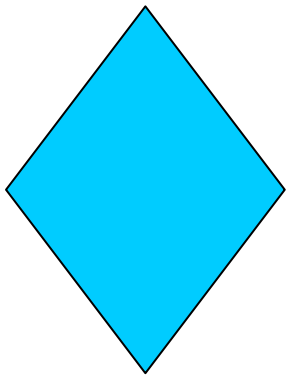
Nariadenie požaduje po zrušení certifikátu vydať do 10 minút CRL alebo umožniť OCSP, kde rozdiel času medzi zrušením certifikátu a časom z **thisUpdate** takéhoto CRL alebo OCSP je do 10 minút.

http://www.itu.int/rec/T-REC-X.509

Časový interval pre CRL a OCSP

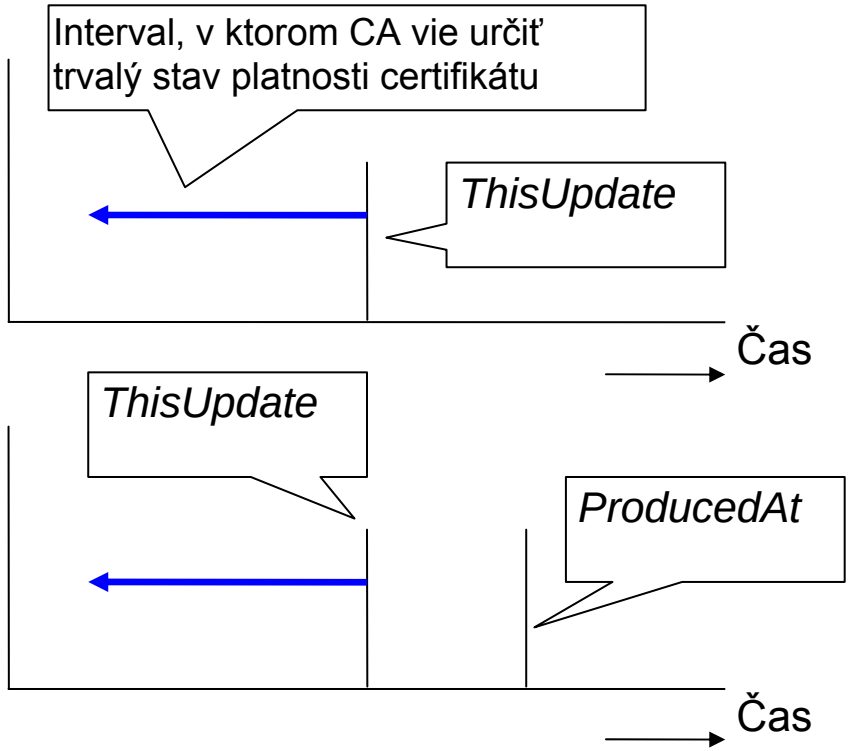


CRL: platnosť podpisovateľa CRL? ***ThisUpdate*** (Koniec intervalu pre overenie platnosti certifikátu)



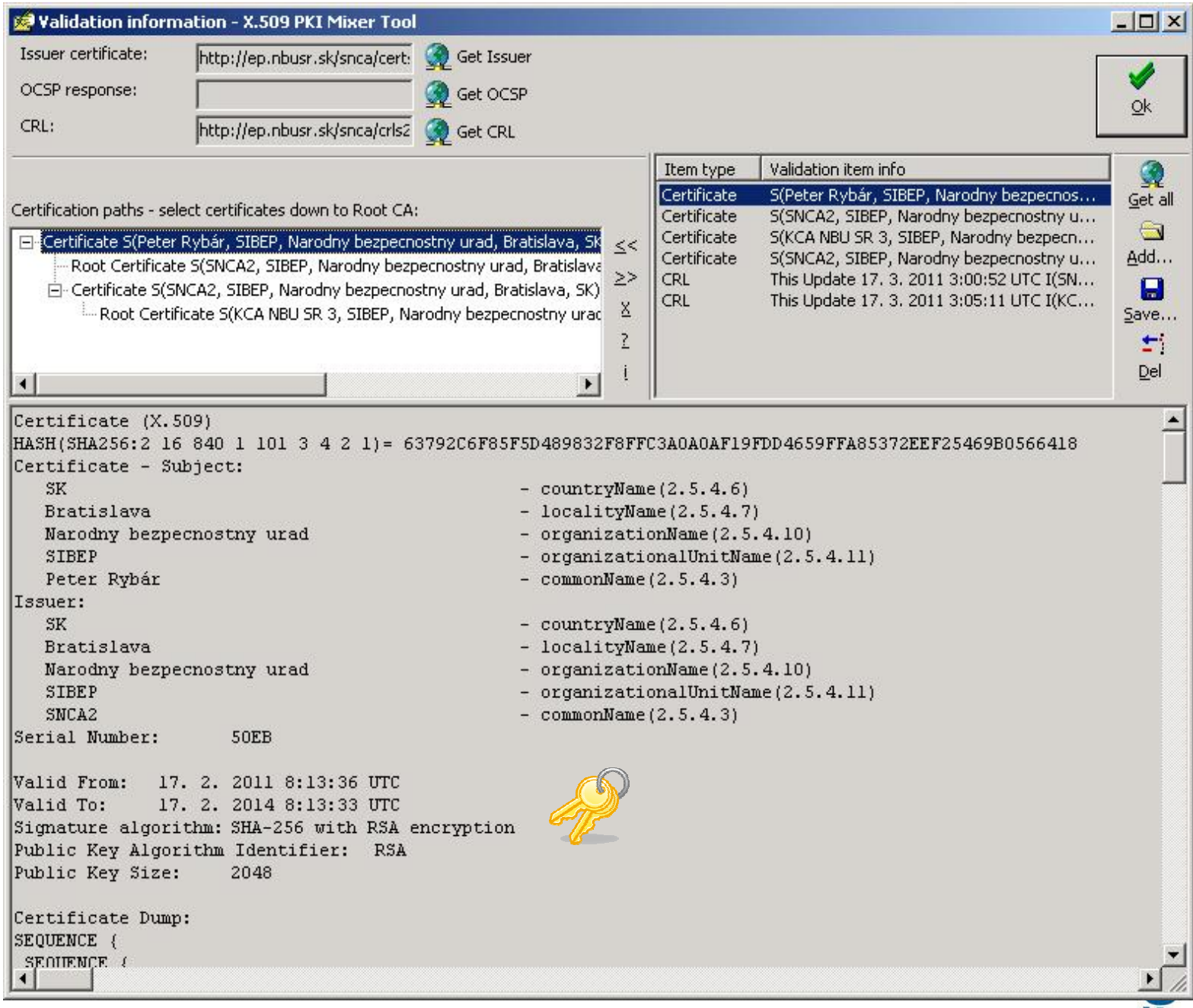
OCSP: ***ProducedAt*** čas podpisu OCSP?

ThisUpdate (Koniec intervalu pre overenie platnosti certifikátu)



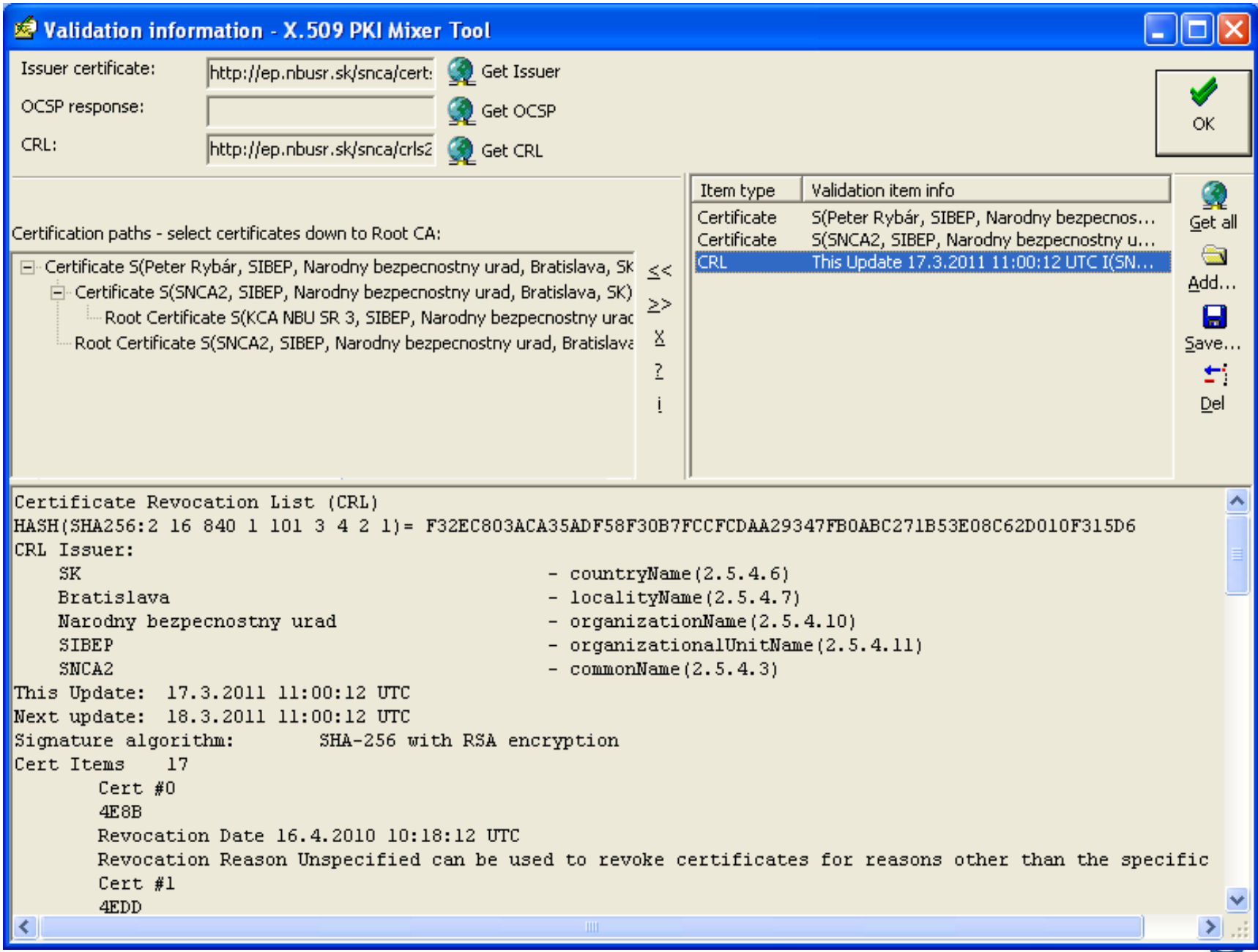
http://www.itu.int/rec/T-REC-X.509

X.509 Cer.



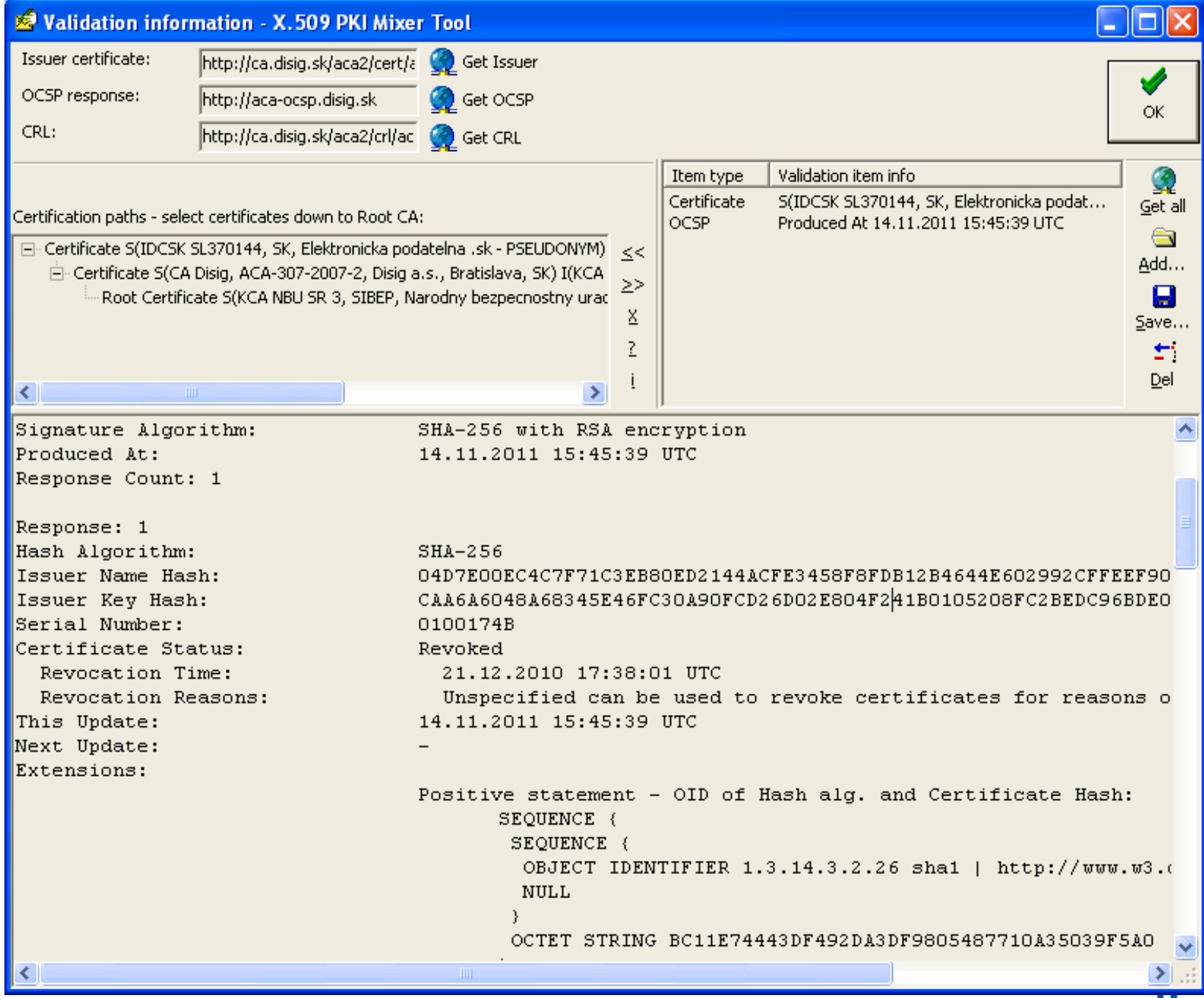
http://www.itu.int/rec/T-REC-X.509

CRL



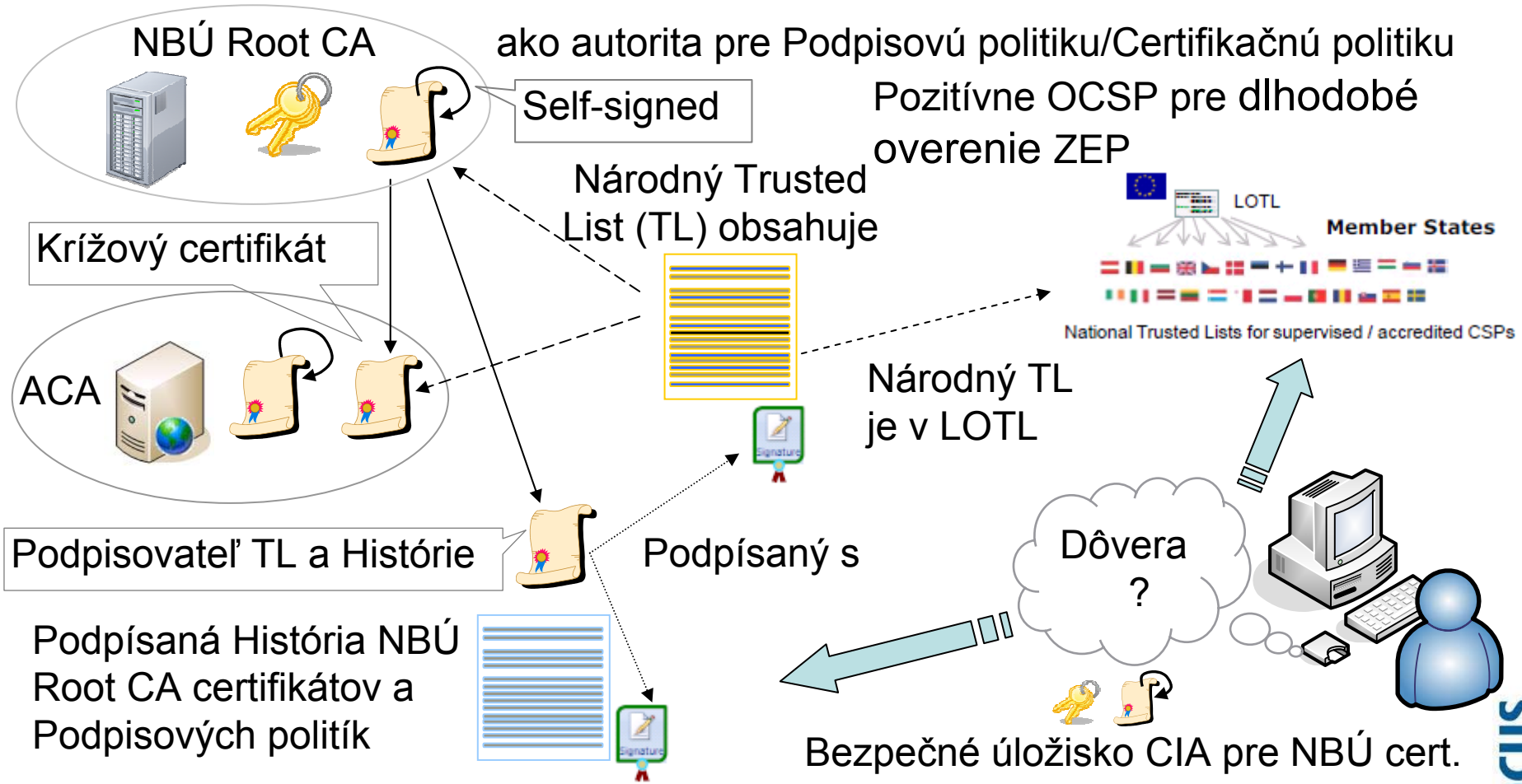
http://www.itu.int/rec/T-REC-X.509

OCSP



http://www.itu.int/rec/T-REC-X.509

Pre SK jeden kľúč NBÚ koreňovej CA pre dlhodobú dôveru v ZEP. V EÚ zoznam služieb.



http://ec.europa.eu/information_society/policy/esignature/eu_legislation/trusted_lists/

ETSI TS 119 612 V1.1.1 (2013-06) Trusted Lists - Skratky

- ACA — Akreditovaná Certifikačná Autorita
- LOTL — List Of The Lists – EÚ Komisiou zverejňovaný zoznam
- OID — Object Identifier
- CIA — Cryptographic Information Application, **EN 14890-1** obsahuje adresárový popis ISO/IEC 7816-15 (CIA) pre získanie dôveryhodných koreňových certifikátov a podpisovateľovho certifikátu zo smart karty podpisovateľom alebo **overovateľom**
- TSL — Trust Status List – dôveryhodný zoznam podľa ETSI
- TL — Trusted List (ako je definované v Rozhodnutí Komisie 2009/767/EC) – dôveryhodný zoznam podľa EÚ Komisie
- SP — Signature Policy – podpisová politika
- SSCD — Secure Signature Creation Device – certifikovaná karta

Ďakujem za pozornosť

Zdroje:
Interoperabilita – Národný profil na základe Rozhodnutia CD 2011/130/EU:
http://www.nbusr.sk/en/electronic-signature/verification/index.html
http://www.nbusr.sk/ipublisher/files/nbusr.sk/elektronicky-podpis/docs/interoperability-profile-intended-for-commission-decision-2011-130-eu-realization-pdf.pdf
http://www.nbusr.sk/en/electronic-signature/signature-policies/index.html

Aplikácia LockIt vytvorená pre NBÚ SR na podpisovanie NBÚ TL, histórie NBÚ Root CA a podpisových politík (v súčasnosti dostupná ako freeware a doplnená o podpisovanie PDF dokumentov, ZIP kontajnera elektronických dokumentov (ASiC-S), XML dokumentov).
http://lockitin.webnode.sk/products/produkt-1/

Ing. Peter Rybár e-mail: peter.rybar@nbusr.sk