Štandardy CEN, ETSI, ISO a odporúčania NBÚ

Ochrana dát a súkromia v cloudových službách (Normy & technológie pre riadenie a IT prevádzku)

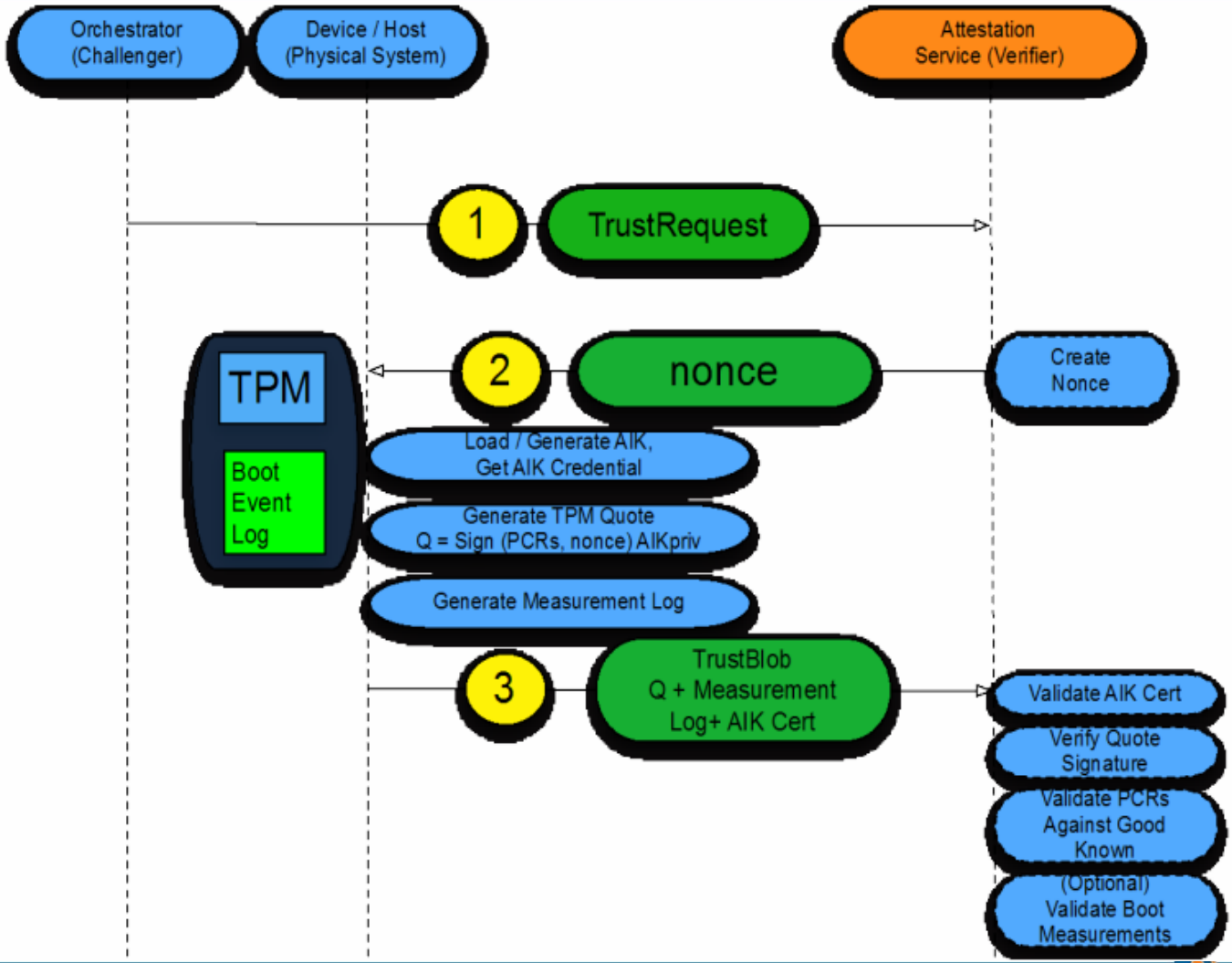
Štandardy CEN, ETSI, ISO a odporúčania NBÚ podporujúce služby podľa návrhu nariadenia Európskeho parlamentu a Rady o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu.

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

Riešenie identity v CLOUD pomocou asymetrických kľúčov

Skratky: Trusted Platform Module (TPM), Platform Configuration Registers (PCRs), Attestation Identity Key (AIK) na vytvorenie digitálneho podpisu.

Obrázok z TRUSTED GEOLOCATION IN THE CLOUD: PROOF OF CONCEPT IMPLEMENTATION (NIST DRAFT)



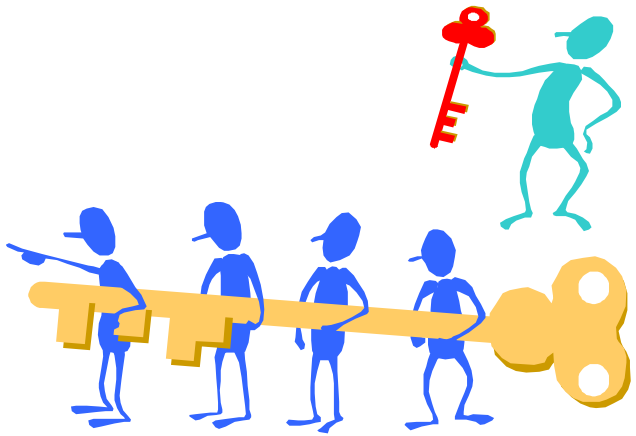
http://csrc.nist.gov/publications/PubsDrafts.html#

Súkromný kľúč – len pod kontrolou konkrétnej osoby alebo zariadenia

ETSI pripravuje štandard Cryptographic Suites for Secure Electronic Signatures (TS 119 312), ktorý bude obsahovť potrebné informácie o algortimoch využívajúcich asymetrický kľúčový pár a o funkciách na tvorbu odtlačku (hash).

Elektronická pečať (seal) má zabezpečiť pôvod a neporušenosť elektronických údajov. Vytvorenie 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

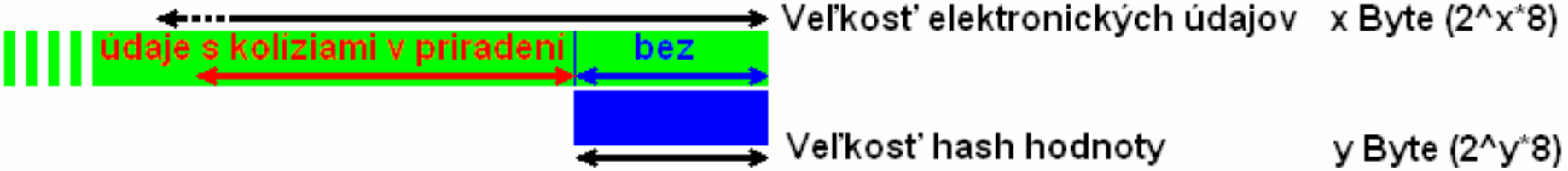
Výhody a obmedzenia odtlačku hash

ETSI štandard TS 119 312 Cryptographic Suites bude obsahovať aj informácie o funkciách na tvorbu odtlačku (hash).

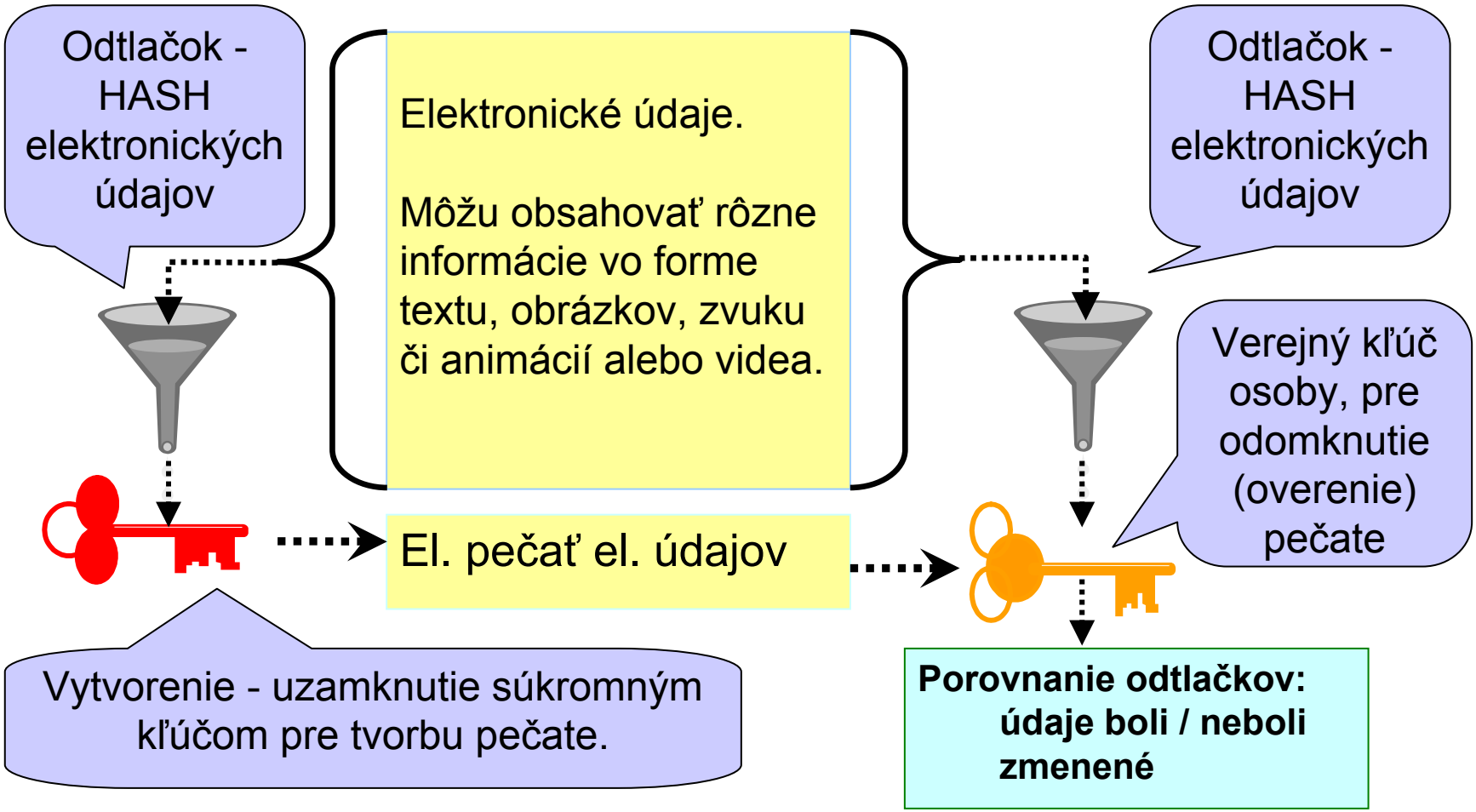
Niektoré vlastnosti hash funkcie:

- elektronickým údajom rôznej veľkosti priraďuje konštantne veľké údaje,
- je to kolízna funkcia ale nesmie byť známy algoritmus na nájdenie kolízie,
- urýchľuje identifikáciu elektronických údajov z ktorých sa hash hodnota vypočíta ale hash hodnota nie je jednoznačná na identifikovanie údajov a je potrebné počítať s dohľadávaním pri vzniku kolízií.

Zjednodušený príklad: Veľkosť elektronických údajov 2Byte (2^16 bitov = 65536 informácií) a veľkosť hash hodnoty 1Byte (2^8 bitov = 256 informácií) potom iba **256** priradení je **jednoznačných** a máme 65536 – 256 = **65280 kolízií**. Pri skutočnej veľkosti hash hodnoty je to analogické.



Zapečatenie a overenie elektronickej pečate (seal) elektronických údajov

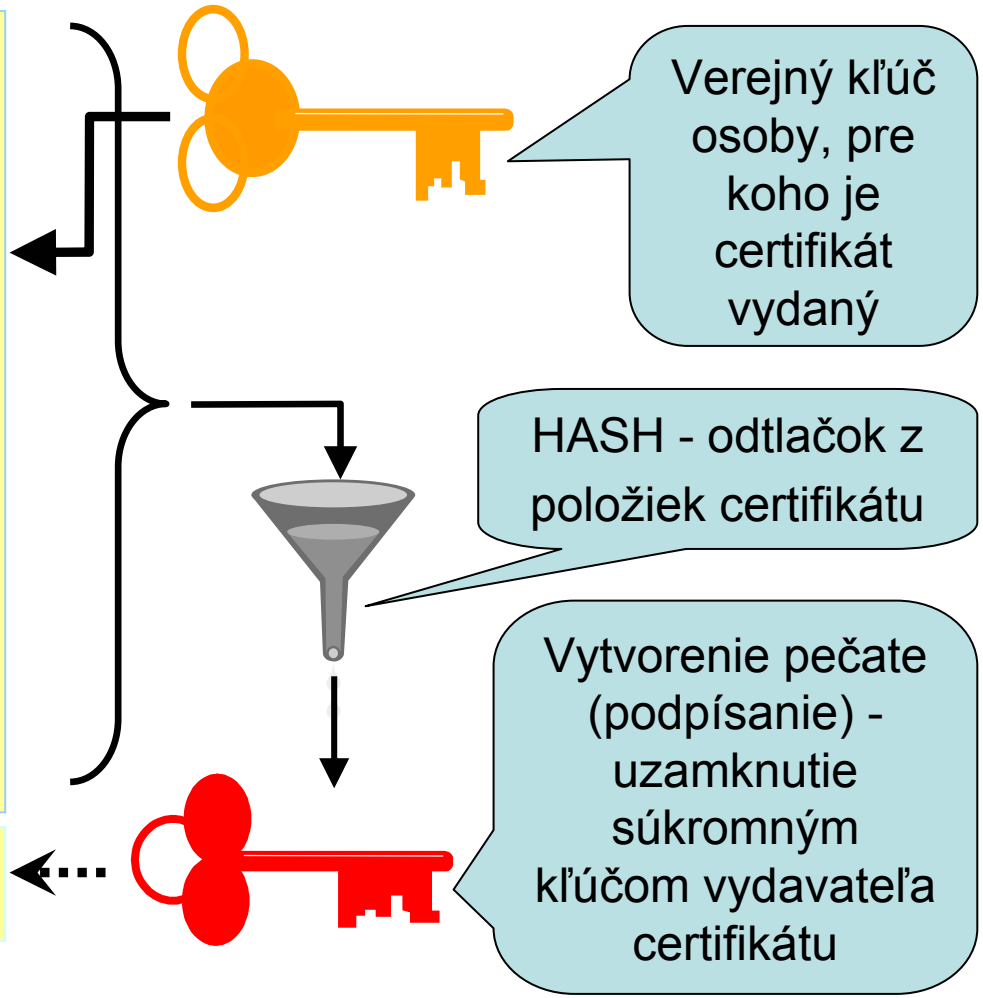


http://www.nbusr.sk/sk/elektronicky-podpis/overovanie.1.html

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)

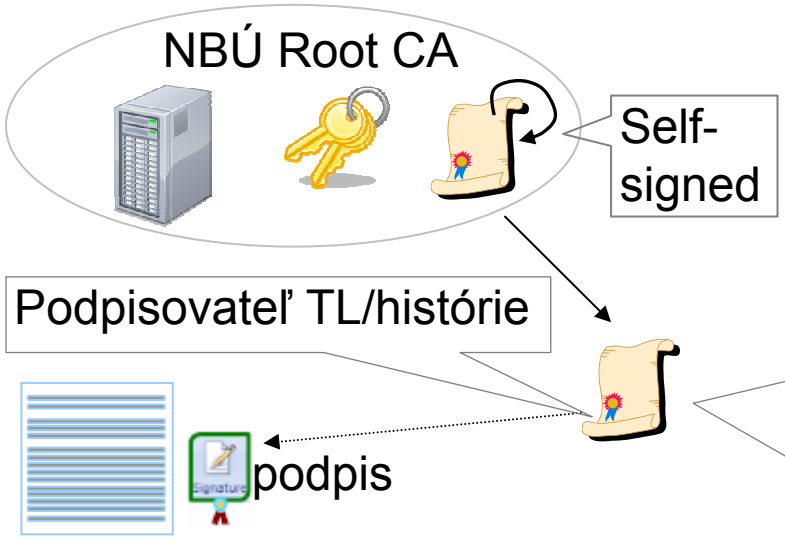
- Meno držiteľa súkromného kľúča – **subjekt** obsahuje aj rodné číslo / číslo pasu / číslo občianskeho preukazu
- **Verejný kľúč**
- Meno vydavateľa - CA
- Sériové číslo
- Čas odkedy a dokedy je možné certifikát používať
- Ďalšie voliteľné položky
  - certificatePolicies
  - subjectKeyIdentifier
  -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

Podpis/pečať certifikátu



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

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



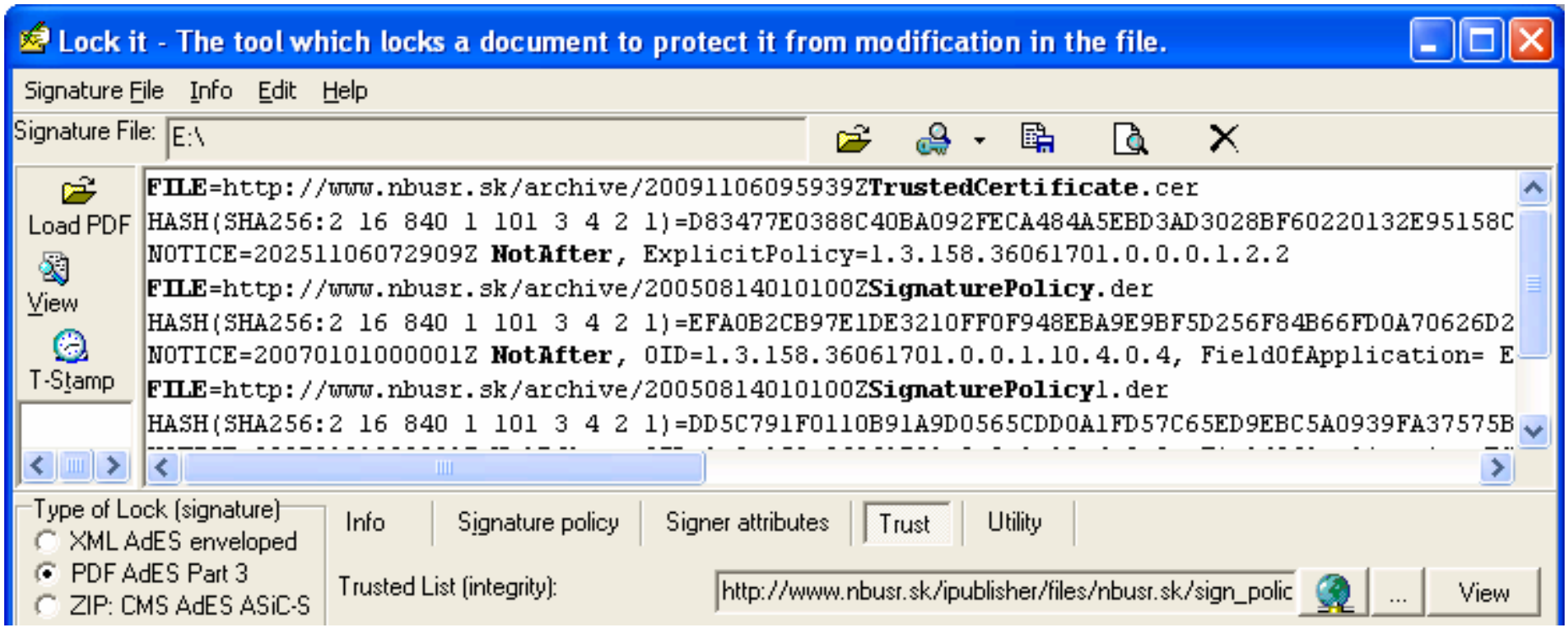
ako Signature Policy Authority

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 exspirované 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 exspirované 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.

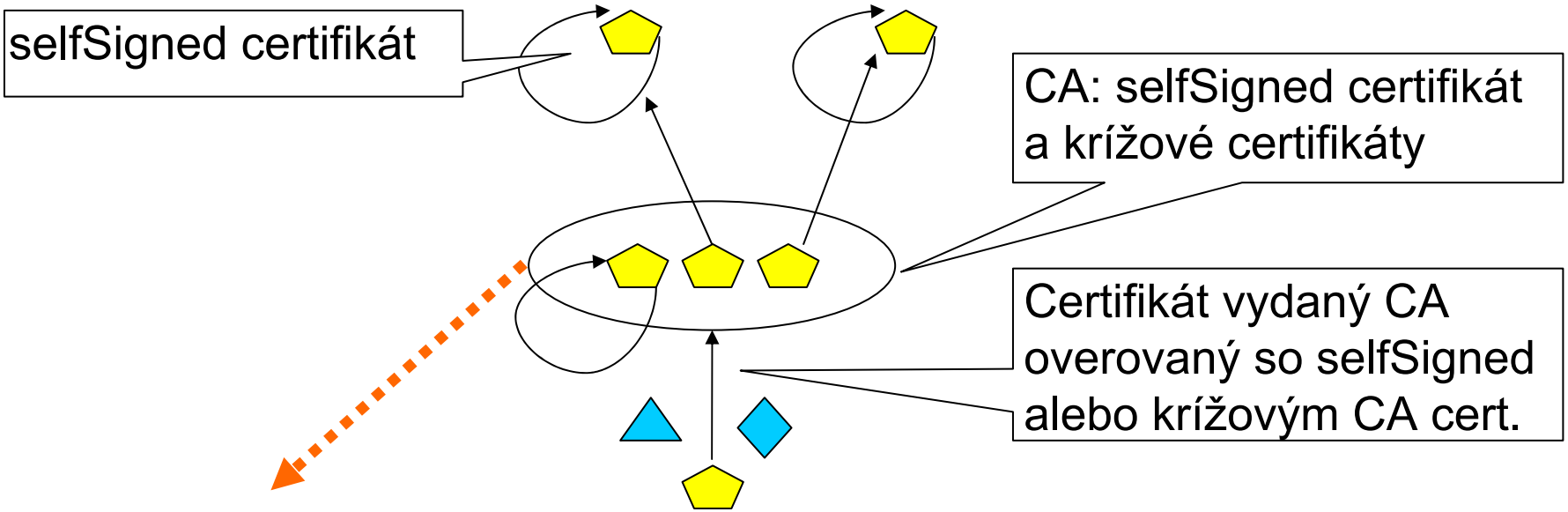
http://www.nbusr.sk/sk/elektronicky-podpis/podpisove-politiky.1.html

História a aktuálne dôveryhodné certifikáty NBÚ a EÚ a podpisové politiky



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

Jedna alebo viacej certifikačných ciest cez krížové certifikáty a samy sebou podpísané certifikáty certifikačných autorít (CA)

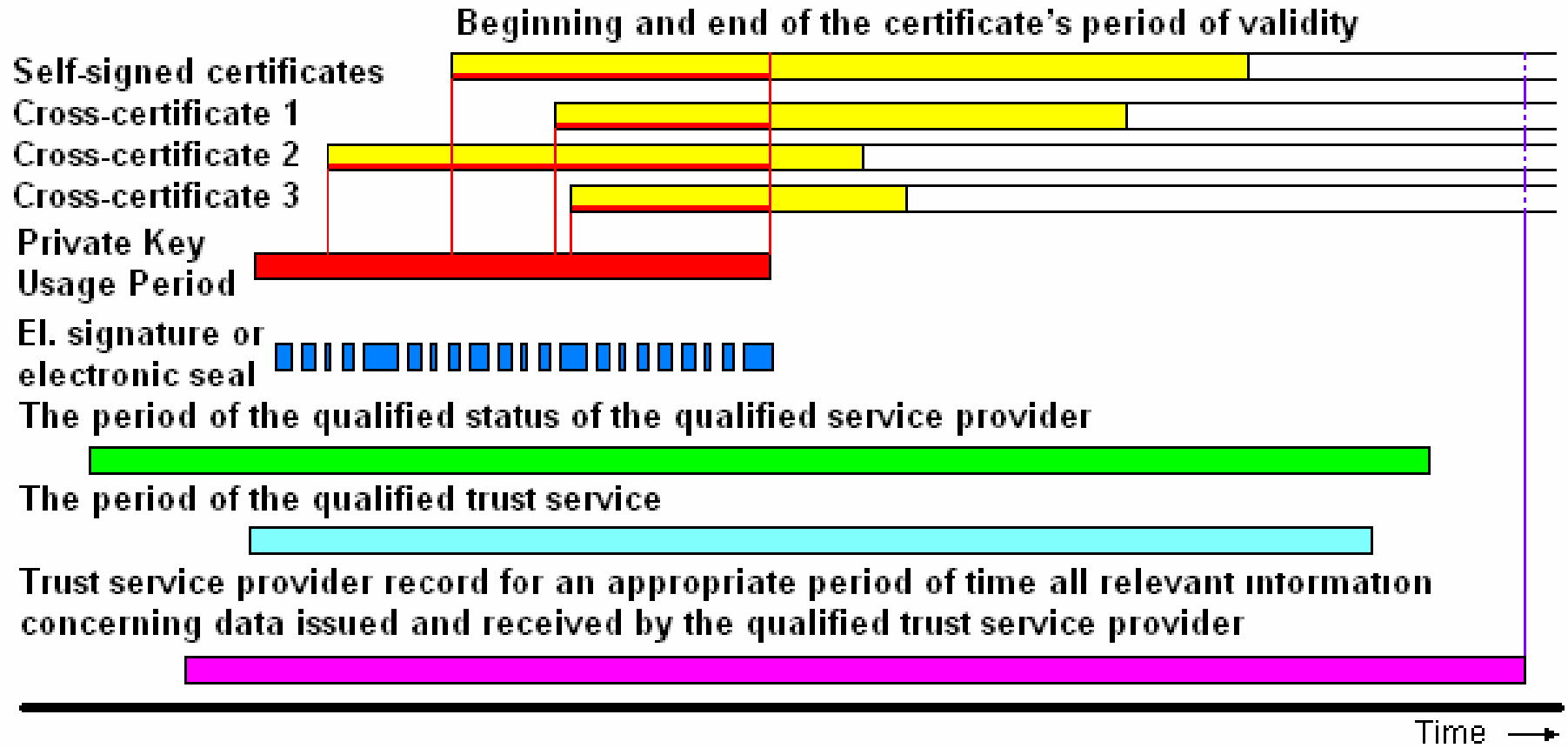


Jeden privátny kľúč vo viacerých certifikátoch (selfSigned alebo krížové CA certifikáty). Certifikáty môžu mať rôzne intervaly použitia na overenie pečatí - podpisov než je interval použitia súkromného kľúča. Interval definuje ITU-T Rec. X.509 v kapitole 8.2.2.5 ako voliteľný.

```
PrivateKeyUsagePeriod  ::=  SEQUENCE {
  notBefore [0] GeneralizedTime OPTIONAL,
  notAfter [1] GeneralizedTime OPTIONAL }
```


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

Periódy pre krížové certifikáty a samy sebou podpísané certifikáty CA



http://www.etsi.org/index.php/technologies-clusters/technologies/security/electronic-signature

Nariadenie Európskeho parlamentu a Rady o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu

- Cieľom tohto nariadenia je posilniť dôveru pri elektronických transakciách na vnútornom trhu umožnením bezpečnej a plynulej realizácie elektronických interakcií medzi podnikmi, občanmi a verejnými orgánmi, čím sa zvýši efektivita verejných a súkromných služieb online, elektronického podnikania a elektronického obchodu v Únii.
- Rada vyzvala Komisiu, aby prispela k digitálnemu jednotnému trhu vytvorením vhodných podmienok pre vzájomné uznávanie kľúčových prostriedkov naprieč hranicami, ako je **elektronická identifikácia, elektronické dokumenty, elektronické podpisy a elektronické doručovacie služby**, a pre interoperabilné služby elektronickej verejnej správy v celej Európskej únii.
- S cieľom posilniť dôveru ľudí vo vnútorný trh a podporiť používanie dôveryhodných služieb a produktov by sa mali zaviesť pojmy **kvalifikované dôveryhodné služby** a **kvalifikovaný poskytovateľ dôveryhodných služieb** so zámerom uviesť požiadavky a povinnosti na zabezpečenie **vysokej úrovne bezpečnosti** akýchkoľvek používaných alebo poskytovaných **kvalifikovaných** dôveryhodných **služieb** a **produktov**.

Nariadenie Európskeho parlamentu a Rady o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu

- Keď sa pri transakcii vyžaduje kvalifikovaná elektronická **pečať právnickej osoby**, rovnako akceptovateľný by mal byť aj **kvalifikovaný** elektronický **podpis** splnomocneného **zástupcu** právnickej osoby.
- **Elektronické pečate** slúžia ako dôkaz, že elektronický dokument vydala právnická osoba a zabezpečujú istotu, pokiaľ ide o pôvod a neporušenosť dokumentu.
- Týmto nariadením by sa malo zaručiť **dlhodobé uchovávanie informácií**, t. j. právna platnosť elektronického podpisu a elektronických pečatí počas rozšírených období, pričom by sa malo zaručiť, aby sa mohli overiť bez ohľadu na budúce technologické zmeny.
- Popri autentifikácii dokumentu vydaného právnickou osobou sa **elektronické pečate** môžu používať aj na **autentifikáciu** akéhokoľvek digitálneho majetku právnickej osoby, napríklad softvérového kódu, serverov.

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

Nové číslovanie v CEN a ETSI

Pre zabezpečenie jednoznačného identifikovania štandardov s ohľadom na ich neskoršie zmeny sa navrhla schéma:

DD L19 xxx-z

Kde:

- DD identifikuje typ štandardu (SR, TS, TR a EN)
- L identifikuje organizáciu 0-3 ETSI, 4 CEN
  - 019 ETSI Special Reports (SR)
  - 119 ETSI Technical Specification (TS) a Technical Report (TR)
  - 219 ETSI Standard (ES) a ETSI Guide (EG)
  - 319 ETSI European Norm (EN)
  - 419 CEN Technical Specification (TS) a European Norm (EN)
- 19 identifikuje sériu štandardov súvisiacich s eSignatures
- xxx identifikuje sériové číslo (000 to 999):
  - kde **X**xx identifikuje oblasť (0-generic; 1-Signature Creation and Validation; 2-Signature Creation Devices; 3-cryptographic suites; 4-Trust Service Providers supporting eSignatures; 5-Trust Application Service Providers; 6-Trust Service Status Lists Providers);
  - kde x**X**x identifikuje podoblasť a 0 je vyhradená pre všeobecnú;
  - kde xx**X** identifikuje typ dokumentu (0-Guidance; 1-Policy and Security Requirements; 2-Technical Specifications; 3-Conformity Assessment; 4- Testing Compliance and Interoperability).
- -z identifikuje dokumenty skladajúce sa z viacerých častí (multi-part documents).

http://www.cen.eu/ http://portal.etsi.org/portal/server.pt/community/ESI/307

Niektoré pripravované štandardy CEN a ETSI

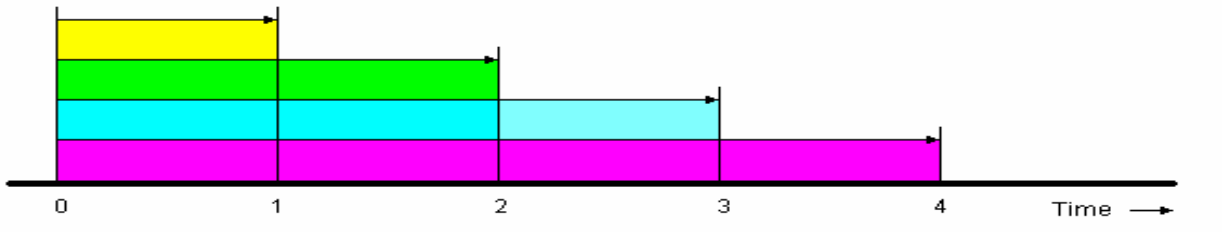
- **CEN prEN 14170/419111** Protection profiles for signature creation and verification application (PP-SCA/SVA)
  - Part 1: Introduction to the European Norm
  - Part 2: Signature creation application - Core PP
  - Part 3: Possible extensions
  - Part 4: Signature verification application - Core PP
  - Part 5: Signature verification application - Possible extensions
- **CEN prEN 14169/419211** parts 1 to 6 Protection Profiles for secure signature creation devices (PP-SSCD)
  - Part 1: Overview, Part 2: Device with key generation, Part 3: Device with key import, Part 4: Extension for device with key generation and trusted communication with certificate generation application, Part 5: Device with key generation and trusted communication with signature creation application, Part 6: Device with key import and trusted communication with signature creation application
- CEN prTS 14167/419221 parts 1 to 5 Security requirements for trustworthy systems managing certificates for ES
  - 1: Security Requirements for Trustworthy Systems
  - 2: Cryptographic Module for CSP signing operations with backup - Protection profile (CMCSOB-PP)
  - 3: Cryptographic module for CSP key generation services - Protection profile (CMCKG-PP)
  - 4: Cryptographic module for CSP signing operations - Protection profile (CMCSO-PP)
  - 5/EN 419241: Security requirements for trustworthy systems supporting server signing
- CEN prEN 16248/419251 Protection Profile for Authentication Device (PP-DAUTH): parts 1 to 3
- CEN TS 419 241 Security Requirements for Trustworthy Systems Supporting Server Signing
- CEN EN 419 103 Conformity Assessment for Signature Creation and Validation (Applications and Procedures)
- CEN EN 419 231 Protection profile for trustworthy systems supporting time stamping
- CEN TR 419 200 Business Driven Guidance for Signature Creation and other related Devices
- CEN EN 419 103 Conformity Assessment for Signature Creation and Validation Applications and Procedures
- CEN TR 419 **010** Extended Rationalized structure including IAS (Identification, Authentication and Signature) standardization aspects

- ETSI EN 319 411-3, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates;Part 3: Policy Requirements for Certification Authorities issuing public key certificates.
- **ETSI EN 319 411-2**, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates.

- **ETSI TS 101 733**, Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)

http://www.cen.eu/ http://portal.etsi.org/portal/server.pt/community/ESI/307

Časová os kritických momentov pri používaní certifikátov X.509

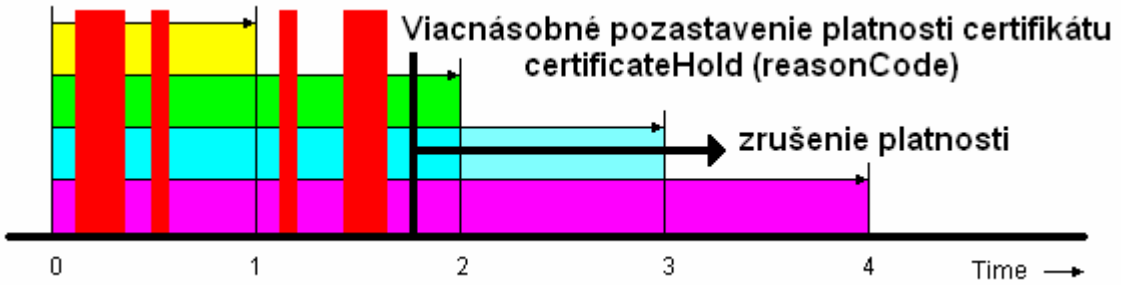


Dôležité časové momenty:

0. Čas zapečatenia elektronických údajov (seal).
1. Čas vytvorenia archívneho formátu zapečatených údajov, ktorý obsahuje všetky potrebné údaje na dlhodobé overenie.
2. Čas exspirovania 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

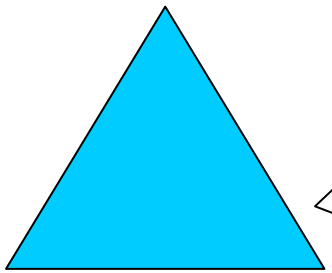
Čas, kedy CA zruší certifikát, nesmie predchádzať čas vydania aktuálneho (naposledy vydaného) CRL alebo OCSP (položka **thisUpdate** v CRL alebo OCSP).

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.

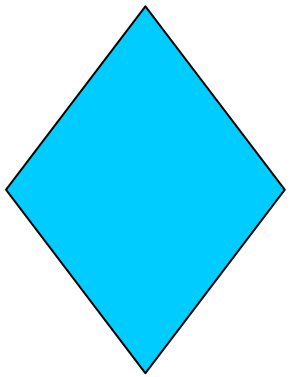
Nariadenie požaduje po zrušení certifikátu vydať do 10 minút CRL alebo umožniť OCSP, kde rozdiel času medzi zrušením certifikátu a časom z **thisUpdate** takéhoto CRL alebo OCSP je do 10 minút.

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

Časový interval pre CRL a OCSP

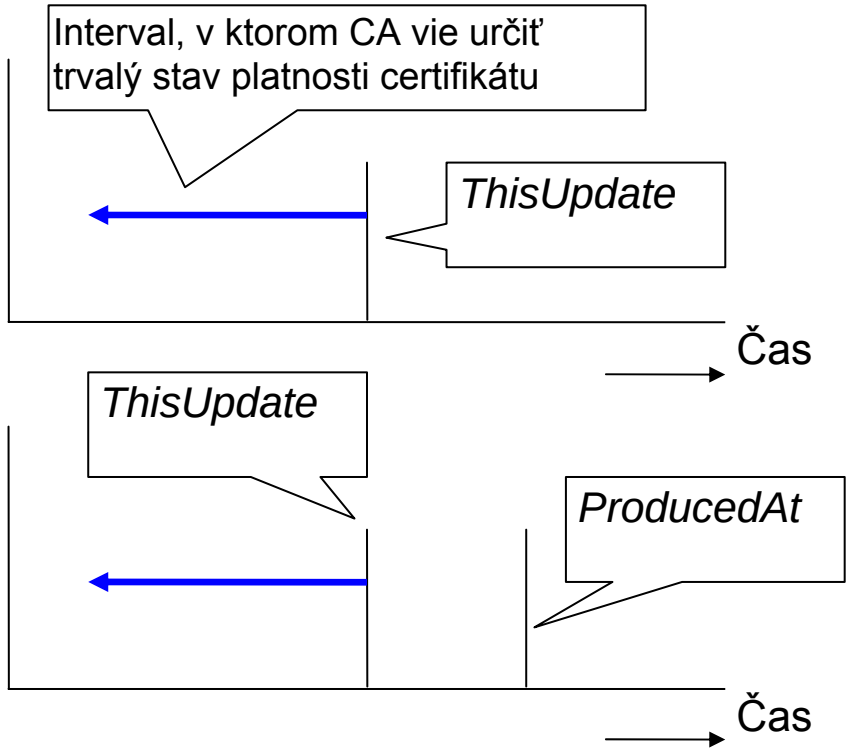


CRL: platnosť podpisovateľa CRL? ***ThisUpdate*** (Koniec intervalu pre overenie platnosti certifikátu)



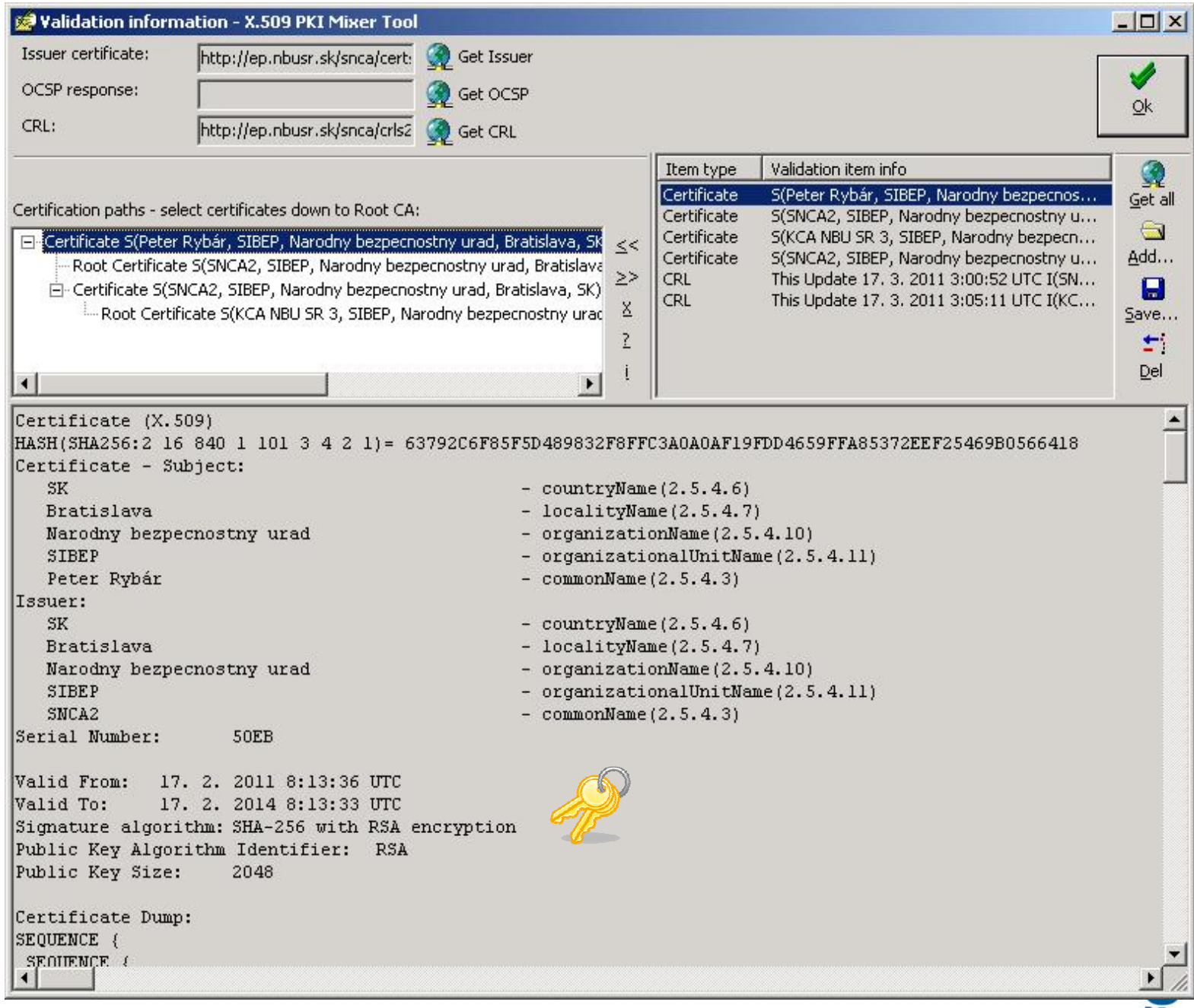
OCSP: ***ProducedAt*** čas podpisu OCSP?

ThisUpdate (Koniec intervalu pre overenie platnosti certifikátu)

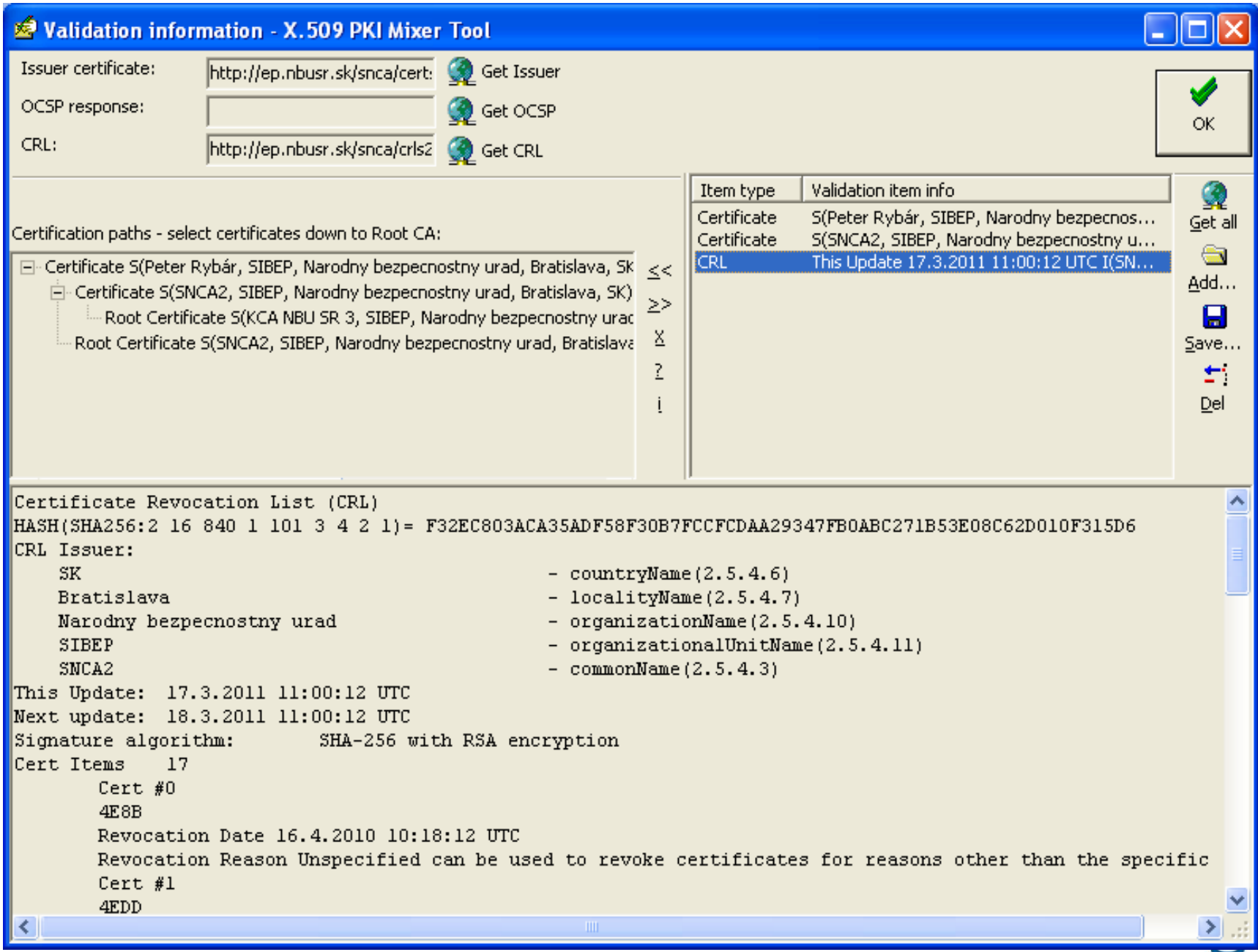


http://www.itu.int/rec/T-REC-X.509

X.509 Cer.

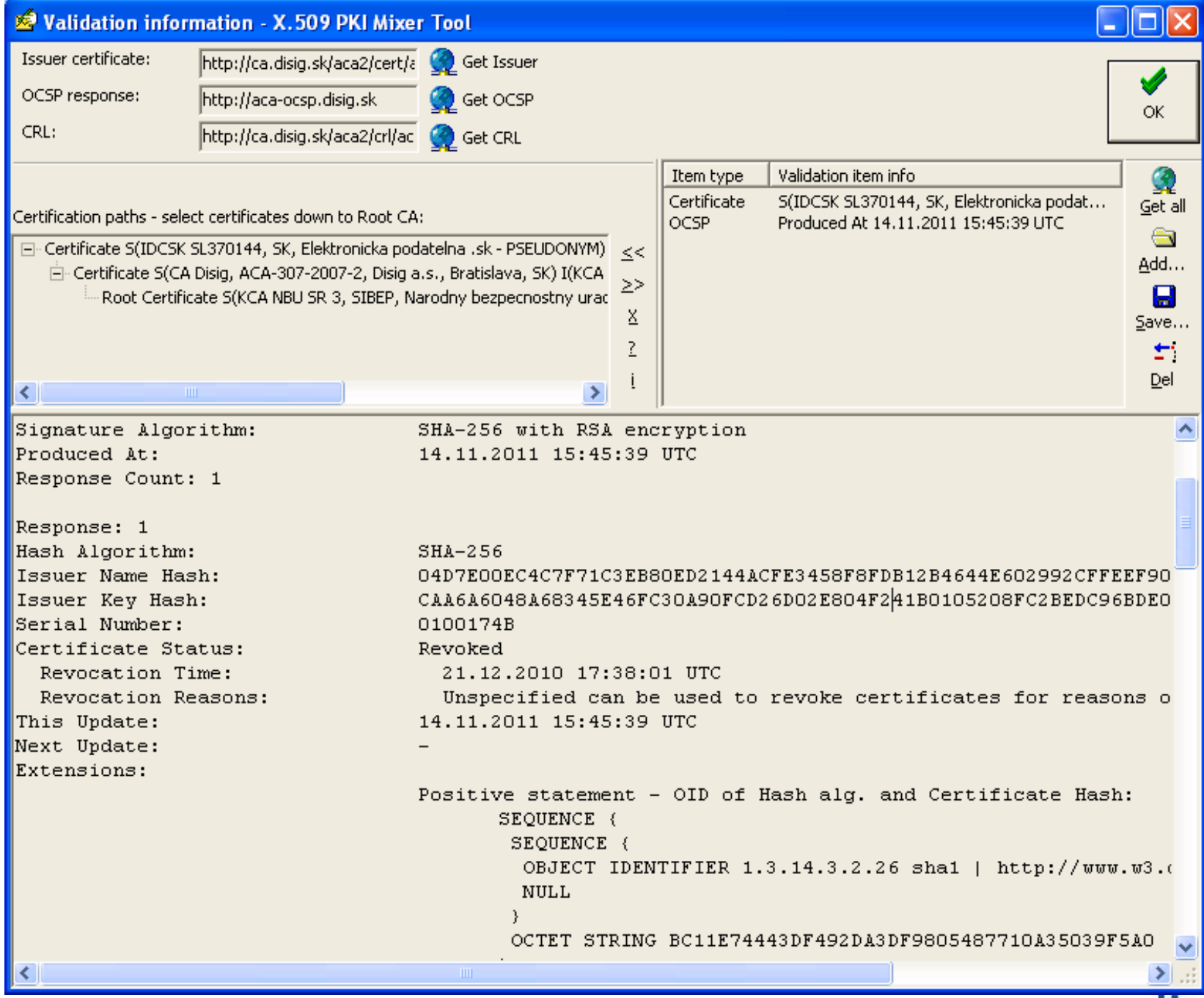

Validation information - X.509 PKI Mixer Tool
Issuer certificate:
http://ep.nbusr.sk/snca/cert:
Get Issuer
OCSP response:
Get OCSP
CRL:
http://ep.nbusr.sk/snca/crls2
Get CRL
Ok
Certification paths - select certificates down to Root CA:
Certificate S(Peter Rybár, SIBEP, Narodny bezpecnostny urad, Bratislava, SK
Root Certificate S(SNCA2, SIBEP, Narodny bezpecnostny urad, Bratislava
Certificate S(SNCA2, SIBEP, Narodny bezpecnostny urad, Bratislava, SK)
Root Certificate S(KCA NBU SR 3, SIBEP, Narodny bezpecnostny urad
Item type
Validation item info
Certificate S(Peter Rybár, SIBEP, Narodny bezpecnos...
Certificate S(SNCA2, SIBEP, Narodny bezpecnostny u...
Certificate S(KCA NBU SR 3, SIBEP, Narodny bezpecn...
Certificate S(SNCA2, SIBEP, Narodny bezpecnostny u...
CRL This Update 17. 3. 2011 3:00:52 UTC I(SN...
CRL This Update 17. 3. 2011 3:05:11 UTC I(KC...
Get all
Add...
Save...
Del
Certificate (X.509)
HASH(SHA256:2 16 840 1 101 3 4 2 1)= 63792C6F85F5D489832F8FFC3A0A0AF19FDD4659FFA85372EEF25469B0566418
Certificate - Subject:
SK - countryName(2.5.4.6)
Bratislava - localityName(2.5.4.7)
Narodny bezpecnostny urad - organizationName(2.5.4.10)
SIBEP - organizationalUnitName(2.5.4.11)
Peter Rybár - commonName(2.5.4.3)
Issuer:
SK - countryName(2.5.4.6)
Bratislava - localityName(2.5.4.7)
Narodny bezpecnostny urad - organizationName(2.5.4.10)
SIBEP - organizationalUnitName(2.5.4.11)
SNCA2 - commonName(2.5.4.3)
Serial Number: 50EB
Valid From: 17. 2. 2011 8:13:36 UTC
Valid To: 17. 2. 2014 8:13:33 UTC
Signature algorithm: SHA-256 with RSA encryption
Public Key Algorithm Identifier: RSA
Public Key Size: 2048
Certificate Dump:
SEQUENCE {

CRL



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

OCSP


Validation information - X.509 PKI Mixer Tool
Issuer certificate:
http://ca.disig.sk/aca2/cert/a
Get Issuer
OCSP response:
http://aca-ocsp.disig.sk
Get OCSP
CRL:
http://ca.disig.sk/aca2/crl/ac
Get CRL
OK
Certification paths - select certificates down to Root CA:
Certificate S(IDCSK SL370144, SK, Elektronicka podatelna .sk - PSEUDONYM)
Certificate S(CA Disig, ACA-307-2007-2, Disig a.s., Bratislava, SK) I(KCA
Root Certificate S(KCA NBU SR 3, SIBEP, Narodny bezpecnostny urac
<<
>>
X
?
i
Item type
Validation item info
Certificate
S(IDCSK SL370144, SK, Elektronicka podat...
OCSP
Produced At 14.11.2011 15:45:39 UTC
Get all
Add...
Save...
Del
Signature Algorithm: SHA-256 with RSA encryption
Produced At: 14.11.2011 15:45:39 UTC
Response Count: 1
Response: 1
Hash Algorithm: SHA-256
Issuer Name Hash: 04D7E00EC4C7F71C3EB80ED2144ACFE3458F8FDB12B4644E602992CFFEEF90
Issuer Key Hash: CAA6A6048A68345E46FC30A90FCD26D02E804F241B0105208FC2BEDC96BDE0
Serial Number: 0100174B
Certificate Status: Revoked
Revocation Time: 21.12.2010 17:38:01 UTC
Revocation Reasons: Unspecified can be used to revoke certificates for reasons o
This Update: 14.11.2011 15:45:39 UTC
Next Update: -
Extensions:
Positive statement - OID of Hash alg. and Certificate Hash:
SEQUENCE {
SEQUENCE {
OBJECT IDENTIFIER 1.3.14.3.2.26 sha1 | http://www.w3.
NULL
}
OCTET STRING BC11E74443DF492DA3DF980548771OA35039F5A0

II. KAPITOLA nariadenia - ELEKTRONICKÁ IDENTIFIKÁCIA

Akceptuje sa akýkoľvek prostriedok elektronickej identifikácie vydaný v inom členskom štáte.

- Štát pre fyzickú identifikáciu svojich občanov, najmä v zahraničí, vydáva **PAS**. Pas je nevyhnutný najmä na štátnych hraniciach alebo pri poskytovaní služieb: ubytovacie – hotel, či iné služby, kde je potrebná identifikácia zákazníka.
- Elektronický svet (internet) nemá hranice a štát musí zabezpečiť identifikáciu svojich občanov aj v tomto elektronickom priestore. Možné riešenie je pridať do databázy pasov záznamy obsahujúce **verejný kľúč osoby** a **dobu** počas ktorej môže osoba tento kľúč **použiť** na svoju **identifikáciu a autentifikáciu**. Štát potom poskytne elektronickú službu, kde v podpísanej odpovedi potvrdí ÁNO/NIE spojenie zaslanej deklarovanej dvojice údajov. **Dvojica pozostáva** z údaja, ktorý **identifikuje občana** v jeho krajine (rodné číslo, číslo pasu s dátumom, číslo občianskeho preukazu s dátumom, …) a **verejný kľúč s dátumom intervalu kedy bol a poprípade stále je platný pre identifikáciu a autentifikáciu**.

European Citizen Card (ECC)
Identification, Authentication and electronic Signature (IAS)

CEN/TS 15480-1: Identification card systems - European Citizen Card - Part 1: Physical, electrical and transport protocol characteristics
CEN/TS 15480-2: Identification card systems - European Citizen Card - Part 2: Logical data structures and card services
CEN/TS 15480-3: Identification card systems - European Citizen Card - Part 3: European Citizen Card Interoperability using an application interface
CEN/TS 15480-4: Identification card systems - European Citizen Card - Part 4: Recommendations for European Citizen Card issuance, operation and use
prCEN/TS 15480-5: Identification card systems - European Citizen Card - Part 5: General Introduction

EN14890, CEN European Standard: Application Interface for smart cards used as secure signature creation devices
ISO/IEC 7816-15: Identification cards - Integrated circuit(s) cards with contacts — Part 15: Cryptographic information application

ISO/IEC 7816, Identification cards — Integrated circuit(s) cards with contacts
ISO/IEC 14443, Identification cards – Contactless integrated circuit(s) cards - Proximity cards

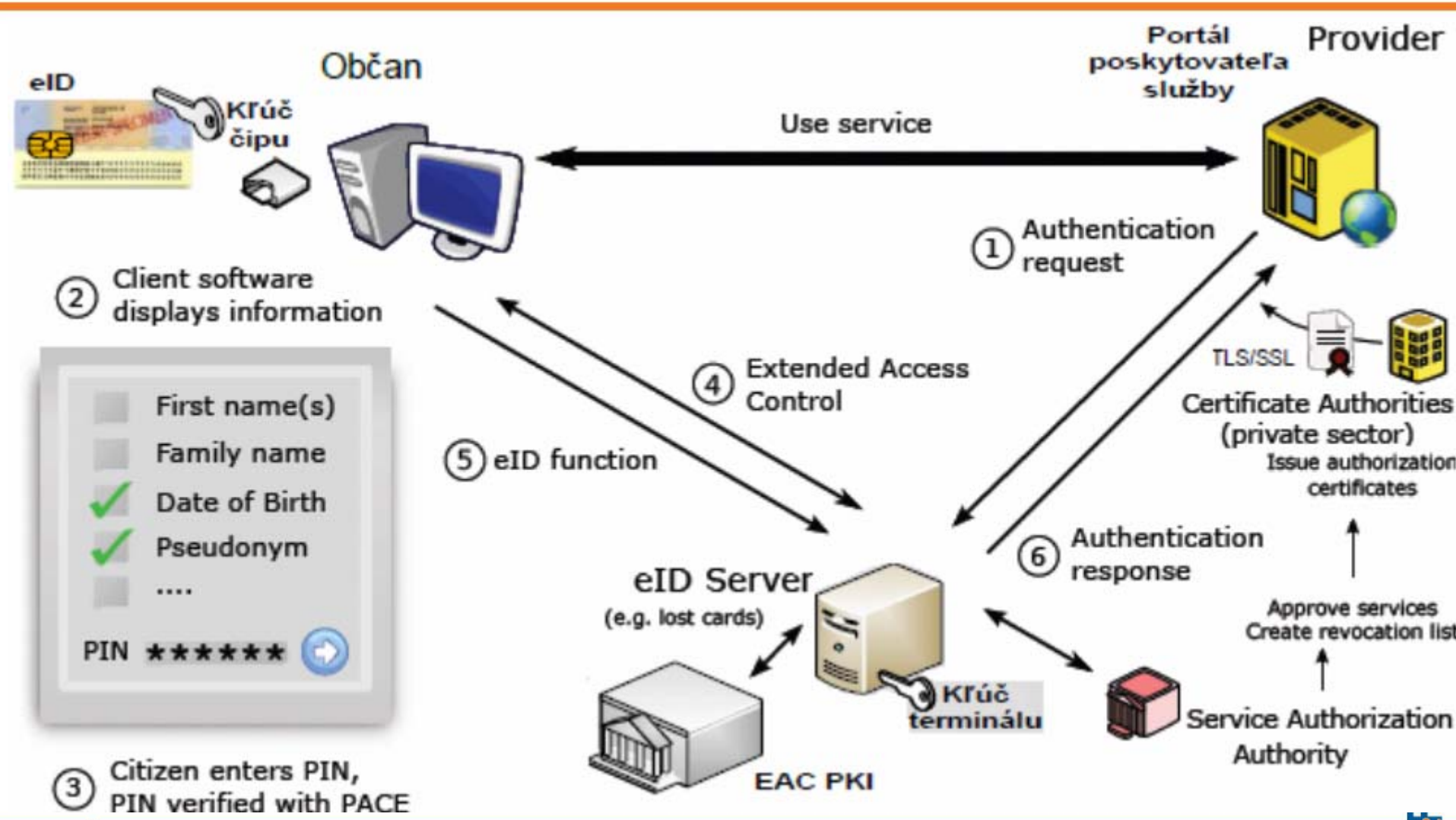
PKCS#11 alebo Crypto API
ISO/IEC 24727-1, Integrated circuit card programming interfaces — Part 1: Architecture
ISO/IEC 24727-2, Identification Cards — Integrated Circuit Cards Programming Interfaces — Part 2: Generic card interface
ISO/IEC 24727-3, Identification Cards — Integrated Circuit Cards Programming Interfaces — Part 3: Application Interface
ISO/IEC 24727-4, Integrated Circuit Cards Programming Interface — Part 4: API Administration

http://www.cen.eu/

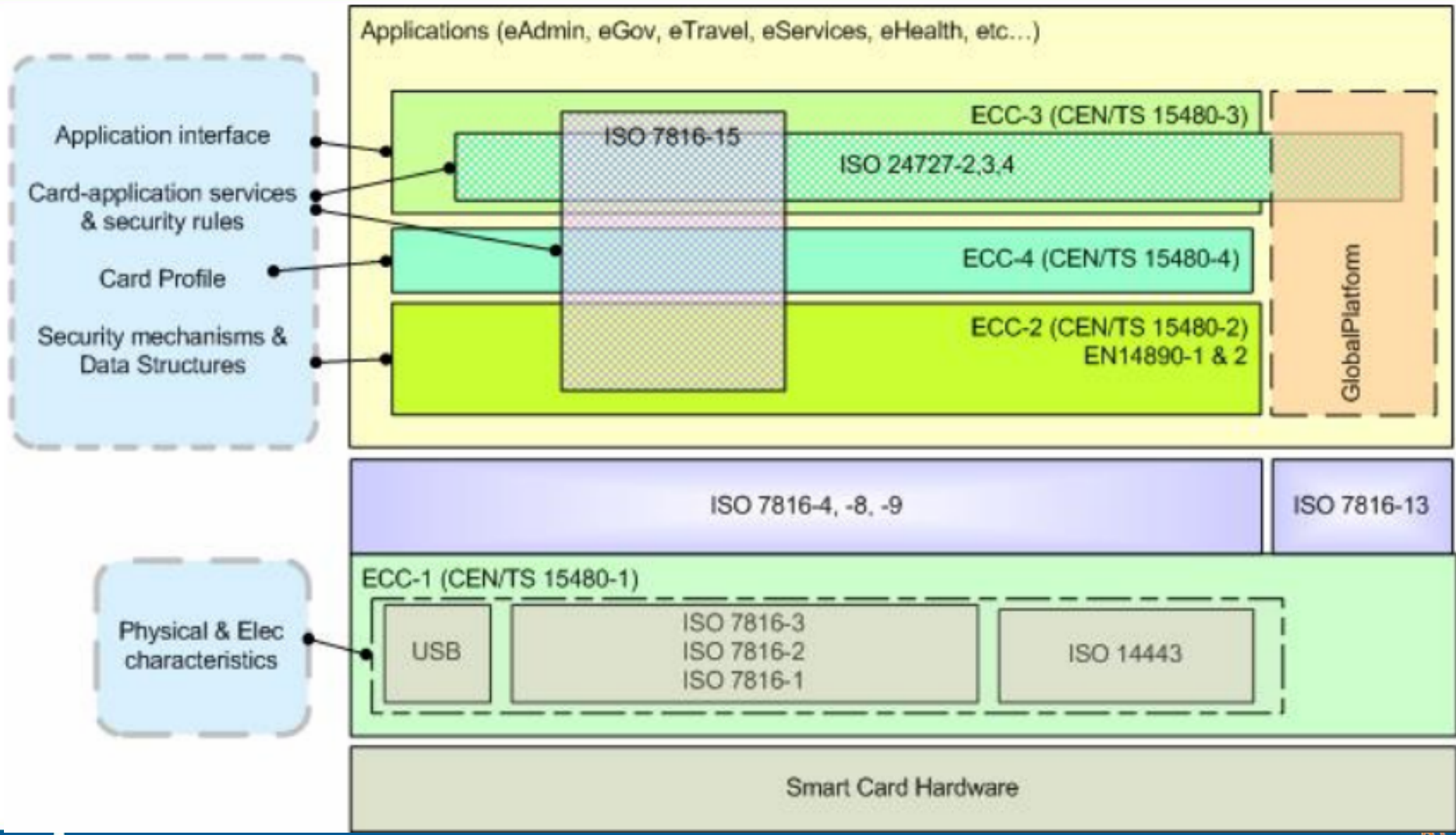
CEN/TS 15480: Identification card systems - European Citizen Card

Aktuálne riešenia eID cez identifikačný server (ktorý overí identitu občana napr. cez eID) poskytujú možnosť získať osobné údaje z eID alebo databázy len obmedzenej množine organizácií, ktorí sú priamo zaregistrovaní pre daný identifikačný server. Takto vznikne bariéra pre iné ako štátne subjekty alebo veľké organizácie pri využití eID na identifikáciu klientov pri poskytovaní služieb cez elektronickú komunikáciu, ale na druhej strane sa vymieňajú len potrebné údaje, ktoré povolí držiteľ eID cez zabezpečené spojenia.

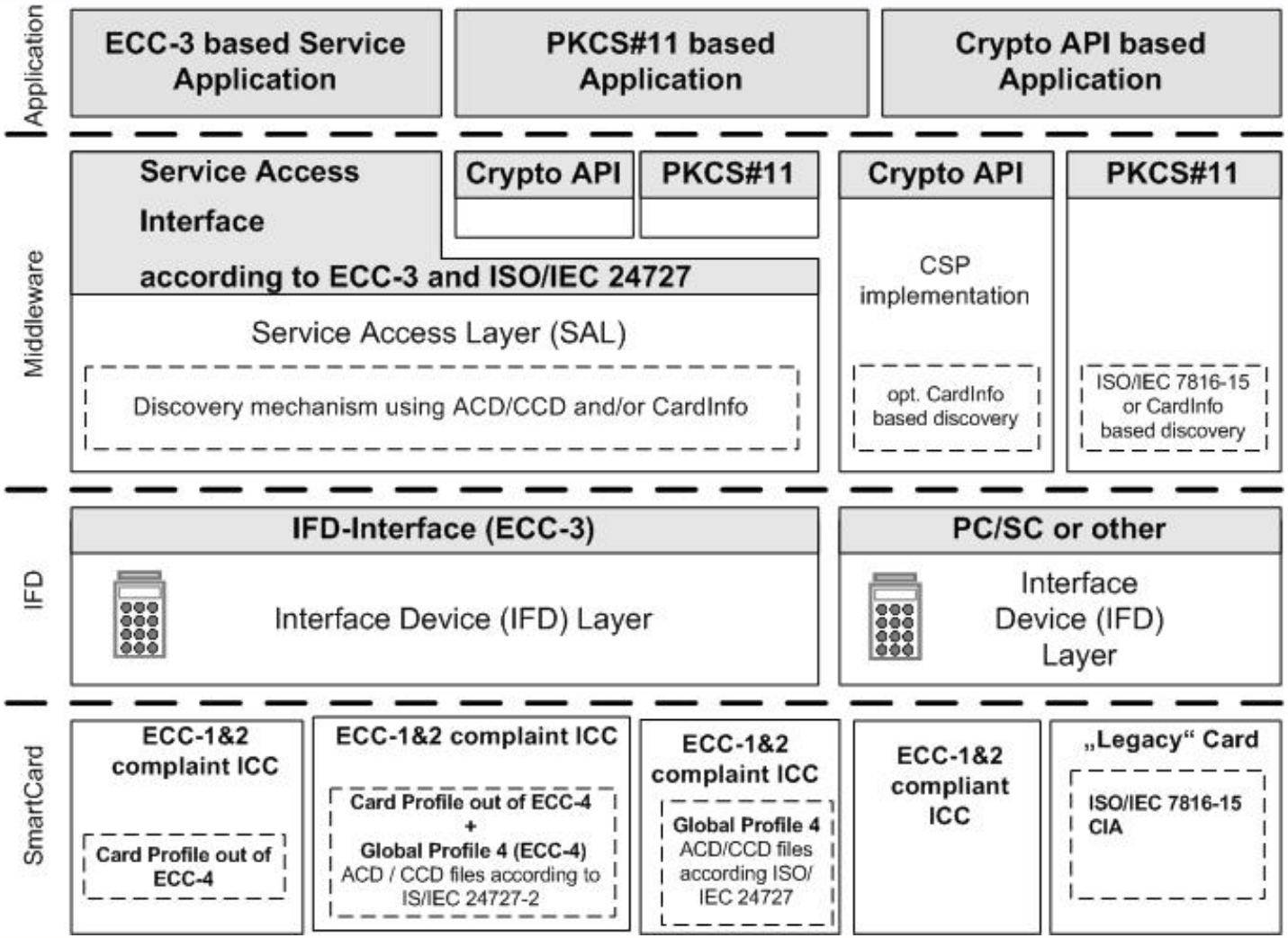
Príklad implementácie - CEN/TS 15480 - European Citizen Card



Prepojenie CEN s ISO v ECC
(TS 15480-5)

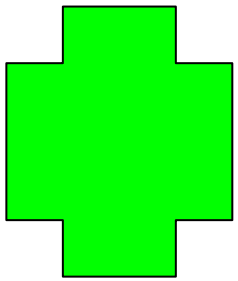


ECC ako uvádza CEN/TS15480-3 Identification card systems - European Citizen Card - Part 3: European Citizen Card Interoperability using an application interface

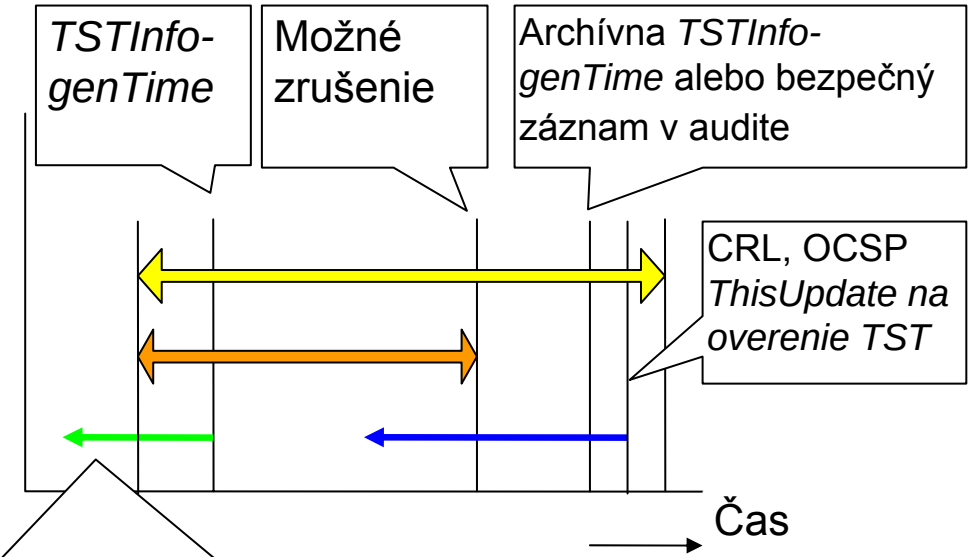


http://www.cen.eu/

5. oddiel nariadenia - Časová pečiatka ako evidencia, že opečiatkovaný objekt existoval pred časom z časovej pečiatky - time-stamp



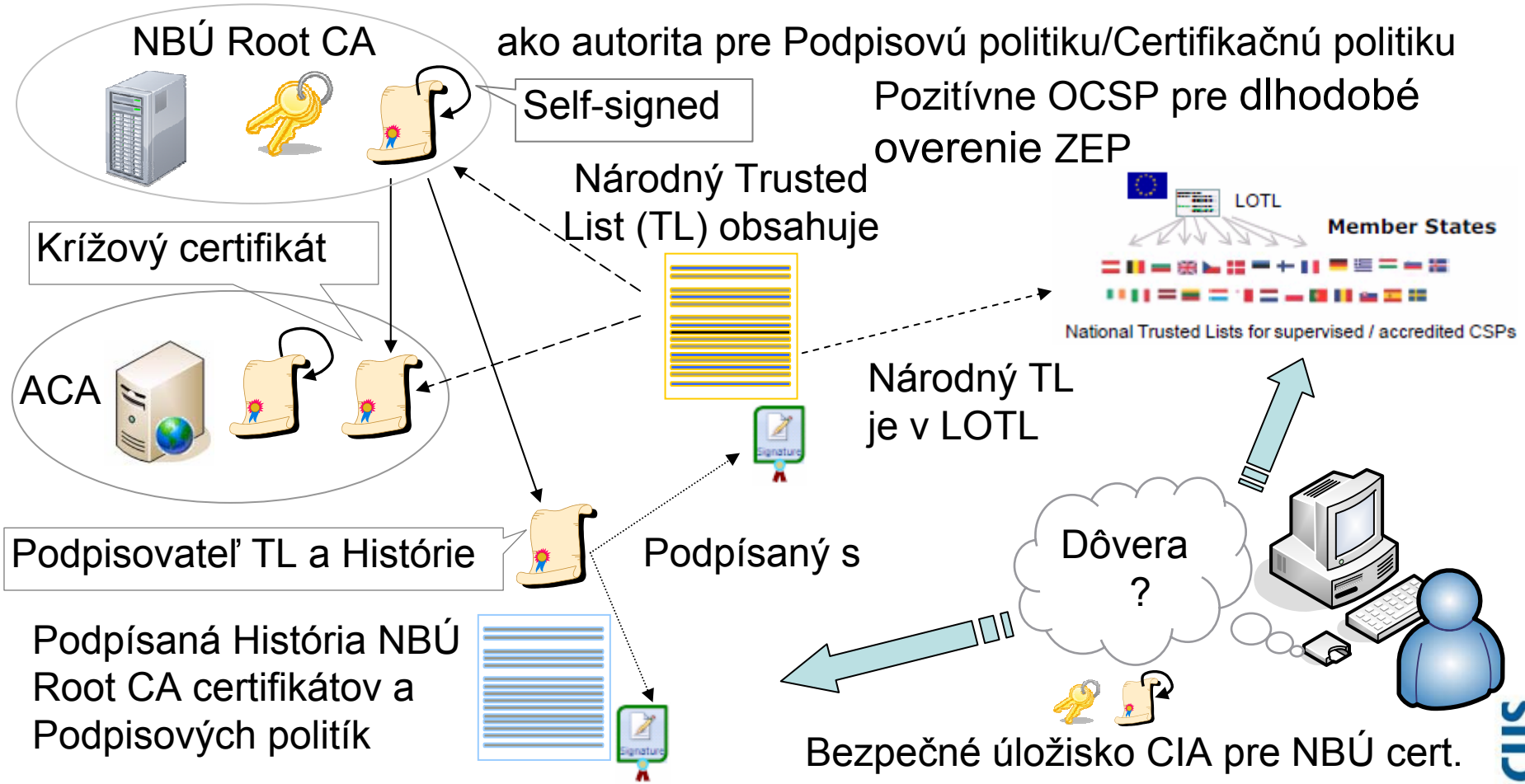
Timestamp: potrebné overiť platnosť TST podpisovateľa!
Možné zrušenie.
TSTInfo-genTime (čas z pečiatky pre overenie certifikátov, CRL, OCSP a integrity údajov)



Interval použitia časovej pečiatky z objektov (certifikáty, CRL, OCSP odpovede, predchádzajúce časové pečiatky alebo údaje ako elektronické dokumenty...)

http://tools.ietf.org/html/rfc3161

III. KAPITOLA nariadenia - dôveryhodné služby 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 Trusted Lists Format - 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

Štandardy NBÚ vydávané ako profily medzinárodných štandardov pre EP

Podľa vyhlášok NBÚ č. 131/2009 Z.z. a č. 135/2009 Z.z. úrad zverejňuje platné formáty zaručených elektronických podpisov a ich formálne špecifikácie, obsah a štruktúru podpisovej politiky, schválené formáty kvalifikovaných certifikátov a schválené formáty zoznamu zrušených kvalifikovaných certifikátov.

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

- Formáty certifikátov a kvalifikovaných certifikátov 3.0
- Formats of certificates and qualified certificates 3.0
- Formáty zaručených elektronických podpisov 3.0
- Qualified Electronic Signature Formats 3.0
- Formáty zoznamu zrušených certifikátov a potvrdzovania stavu a platnosti certifikátov 3.0
- Formats of certificate revocation list and confirming the status and validity of certificates 3.0
- Upresnenia obsahu a formálne špecifikácie formátov dokumentov pre ZEP 1.0
- SIM mobilného zariadenia na elektronické podpisovanie cez bezpečné WEB/WAP alebo PKCS#11 rozhranie 1.1

Základné štandardy, ktoré predstavujú minimum pre EP

- **ITU-T Rec. X.509 (11/08)** Public-key and attribute certificate frameworks http://www.itu.int/rec/T-REC-X.509
- IETF, RFC 5652, Cryptographic Message Syntax (CMS), http://tools.ietf.org/html/rfc5652.
- IETF, RFC 3161, Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP), http://tools.ietf.org/html/rfc3161.
- ETSI TS 101 733: CMS Advanced Electronic Signatures (CAdES).
- ETSI TS 101 903: XML Advanced Electronic Signatures (XAdES).
- W3C, XML Signature Syntax and Processing, (Second Edition), http://www.w3.org/TR/xmldsig-core/
- ETSI TS 102 176: Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms; Part 2: "Secure channel protocols and algorithms for signature creation devices".

- ISO 14533-1:2012 Processes, data elements and documents in commerce, industry and administration -- Long term signature profiles -- Part 1: Long term signature profiles for CMS Advanced Electronic Signatures (CAdES)

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, XML dokumentov). http://lockitin.webnode.sk/products/produkt-1/

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