



NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

Verzia 1.3

Základné princípy elektronického podpisu a zaručeného elektronického podpisu (ZEP)

10. február 2012

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

Sekcia informačnej bezpečnosti a elektronického podpisu

Budatínska č. 30, P.O.BOX 16, 850 07 Bratislava 57

<http://www.nbusr.sk/>

e-mail: podatelna@nbusr.sk

Obsah

1	Úvod	4
2	Predmet dokumentu	4
3	Odkazy	5
4	Skratky.....	6
5	Využitie elektronického podpisu (EP).....	7
6	Teoretické základy elektronického podpisu	7
7	Kryptografické algoritmy a hash funkcie a ich implementácia v elektronickom podpise..	8
8	Význam používania zaručeného elektronického podpisu v praxi a jeho prínos.....	9
9	Spôsoby overenia ZEP a rola NBÚ pri certifikácii, kontrole a pri overovaní dôvery.....	10
10	Technické prostriedky pre elektronický podpis - SSCD	11
11	PKI infraštruktúra ako prvok dôveryhodnosti v prostredí elektronického podpisu	12
12	Legislatívne prostredie implementácie elektronického podpisu v SR a EÚ	12
13	Platnosť certifikátu a podpisu	13
	Príloha A (informatívna) Príklady	15
	A.1 SSCD pre uloženie kľúčového páru a pre kvalifikovaný certifikát	15
	A.2 Hašovacia funkcia	15
	A.3 Obsah certifikátu X.509	16
	A.4 Vydané CRL.....	17
	A.5 PKI hierarchia overovania.....	17
	A.6 Ideálny model pre overenie ZEP podľa Komisie EÚ	18
	A.7 Podpísanie súboru	19
	A.8 Overenie podpisu	19
	Príloha B (informatívna) Rozhodnutie Komisie (2003/511/ES).....	20
	Príloha C (informatívna) Legislatíva pre elektronický podpis.....	20
	Príloha D (informatívna) Štandardy EÚ a NBÚ	21
	Príloha E (informatívna) Úlohy úradu pre oblasť EP.....	23
	Príloha F (informatívna) Zoznam použitej literatúry	24
	Príloha G História.....	25

1 Úvod

Elektronický podpis a zaručený elektronický podpis sa stáva nevyhnutnou súčasťou pri elektronickej komunikácii medzi orgánmi štátnej správy a v organizáciách, v ktorých je potrebná ochrana integrity elektronických dokumentov proti falšovaniu a nepopierateľné preukázanie, že elektronický dokument v danom čase existoval a jeho obsah bol vytvorený alebo prezentovaný konkrétnou osobou.

2 Predmet dokumentu

Účelom tohto dokumentu je priblížiť využitie a základné komponenty elektronického podpisu a úlohy NBÚ pri akreditácii, certifikácii a vydávaní štandardov pre oblasť zaručeného elektronického podpisu. Tento dokument sa bude snažiť o popis elektronického podpisu s čo najmenšími požiadavkami na zvládnutie odborných vedomostí z oblasti informatiky, ale ak máte záujem o hlbšie informácie, potom podrobné technické a právne informácie z oblasti elektronického podpisu nájdete na stránkach NBÚ na nasledovných adresách [12, 13, 14].

Dokument zahŕňa najmä:

- teoretické základy elektronického podpisu;
- kryptografické algoritmy a hašovacie funkcie a ich implementáciu v elektronickej podpise;
- technické prostriedky pre elektronický podpis – SSCD;
- PKI infraštruktúru ako prvok dôveryhodnosti v prostredí elektronického podpisu;
- legislatívne prostredie implementácie elektronického podpisu v SR a EÚ.

3 Odkazy

Odkazy na dokumenty, ktoré definujú použité typy a postupy.

- [1] ETSI TS 101 733 Electronic Signature Formats
- [2] ETSI TR 102 272 ASN.1 format for signature policies
- [3] RFC 5280 X.509 PKI Certificate and Certificate Revocation List May 2008
- [4] RFC 3739 Qualified Certificates Profile March 2004
- [5] ETSI TS 101 862 Qualified Certificate Profile
- [6] RFC 5652 Cryptographic Message Syntax September 2009
- [7] RFC 3161 Time-Stamp Protocol (TSP) August 2001
- [8] RFC 2560 X.509 PKI Online Certificate Status Protocol June 1999
- [10] EN 14890-1/2:2008 Application Interface for Smart Cards used as Secure Signature Creation Devices - Part 1: Basic Services; Part 2: Additional Services
- [11] RFC 2044 UTF-8, a transformation format of Unicode and ISO 10646 October 1996
- [12] Základné dokumenty legislatívy Slovenskej republiky pre elektronický podpis
<http://www.nbusr.sk/sk/elektronicky-podpis/index.html>
- [13] Formáty zaručených elektronických podpisov
<http://www.nbusr.sk/sk/elektronicky-podpis/schvalene-formaty/index.html>
- [14] Vytvorenie a overenie certifikačnej cesty a profily pre implementáciu Rozhodnutia Komisie 2011/130/EÚ <http://www.nbusr.sk/sk/elektronicky-podpis/overovanie/index.html>
- [15] Smernica Európskeho parlamentu a Rady 1999/93/ES z 13. decembra 1999 o rámci spoločenstva pre elektronické podpisy
- [16] Rozhodnutie Komisie 2009/767/ES zo 16. októbra 2009, ktorým sa ustanovujú opatrenia na uľahčenie postupov elektronickými spôsobmi prostredníctvom „miest jednotného kontaktu“ podľa smernice Európskeho parlamentu a Rady 2006/123/ES o službách na vnútornom trhu (Úradný vestník Európskej únie L 274 z 20. októbra 2009)
- [17] ETSI TS 102 231 – Electronic Signatures and Infrastructures (ESI): Provision of harmonized Trust-service status information.
- [18] ROZHODNUTIE KOMISIE 2011/130/EÚ z 25. februára 2011, ktorým sa ustanovujú minimálne požiadavky na cezhraničné spracovanie dokumentov elektronicky podpísaných príslušnými orgánmi v zmysle smernice Európskeho parlamentu a Rady 2006/123/ES o službách na vnútornom trhu [oznámené pod číslom K(2011) 1081] (Text s významom pre EHP)
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:053:0066:0072:EN:PDF>

Poznámka: Slovenský preklad realizovaný v EÚ Komisii zatiaľ obsahuje závažné chyby prekladu.

4 Skratky

CA	Certification Authority
CMS	Cryptographic Message Syntax
CAeS	CMS Advanced Electronic Signature
CRL	Certificate Revocation List
DER	Distinguished Encoding Rules (for ASN.1)
OID	Object Identifier
QC	Qualified Certificate
SCA	Signature Creation Application
SHA	Secure Hash Algorithm
SSCD	Secure-Signature-Creation Device
URL	Uniform Resource Locator
ZEP	Zaručený elektronický podpis – Slovenská legislatíva
QES	Kvalifikovaný elektronický podpis – Európska legislatíva

5 Využitie elektronického podpisu (EP)

Vzhľadom na potrebu získania všeobecných vedomostí a najmä ich praktického využitia pri činnosti v rámci povinností vyplývajúcich zo zákonov, vyhlášok a nariadení NBÚ, sú nasledujúce kapitoly zamerané hlavne na priblíženie využitia elektronického podpisu v praxi.

6 Teoretické základy elektronického podpisu

Z hľadiska informačnej bezpečnosti by malo byť prvoradým definovanie a kontrolovanie rôznych stupňov zabezpečenia informácií prenášaných a uchovávaných na rôznych médiách. Papierový svet objednávok, faktúr, zmlúv a rôznych potvrdení od štátnych alebo súkromných spoločností si vyžaduje pri potrebe rozmnoženia týchto listín na právne účely nemalé náklady na overovanie kópií. Pritom overenie papierových kópií a ich podpisov len veľmi problematcky vedie k odhaleniu falšovania vo forme pozmenených slov uvedených na kópiách týchto papierových dokumentov.

V elektronickom svete si môžete zadarmo vytvoriť neobmedzený počet identických kópií. Na druhej strane však elektronické dokumenty umožňujú jednoducho a nebadane povkladať rôzne pozmenené slová a číselné hodnoty do elektronických kópií dokumentov, čo pri rozsiahlych dokumentoch môže byť prehliadnuté.

Tieto obavy z používania elektronických dokumentov je ale možné elegantne a takmer zadarmo vyriešiť pomocou uzamknutia dokumentov použitím dvojice kľúčov. **Dvojica kľúčov** má takú vlastnosť, že keď **s jedným kľúčom** dokument **uzamknete**, **odomknúť** ho **môžete len s druhým kľúčom**. **Ten istý kľúč sa na uzamknutie a následné odomknutie použiť nedá.**

Aká z toho plynie výhoda? Ak druhý kľúč verejne poskytnete s informáciou, že je to váš kľúč, tak potom všetko, čo uzamknete s prvým kľúčom z dvojice, ktorý si necháte iba vy, môžu odomknúť ostatní iba s použitím druhého kľúča. Zároveň to znamená, že všetci čo odomkli elektronický dokument s vašim druhým kľúčom, si overili, že elektronický dokument ste mohli zamknúť len vy s vašim prvým kľúčom. Do zamknutého dokumentu už nikto nespraví zmeny (nesfalšuje ho), lebo nemá váš prvý kľúč, ktorým ste ho zamkli; kópiu zamknutého elektronického dokumentu si môže len odomknúť a po odomknutí s ňou pracovať.

Princíp je jednoduchý no z jeho neznalosti častokrát najmä v médiach je možné počuť nezmyselné informácie. Treba si však uvedomiť, že tak ako sa **nedá kúpiť vlastnoručný podpis**, tak na **nedá kúpiť ani elektronický podpis!** Tak ako si kupujete **pero**, kupujete si aj **súkromný kľúč**, ktorým vytvárate elektronický podpis – **zamykáte od tlačok z elektronického dokumentu.**

7 Kryptografické algoritmy a hash funkcie a ich implementácia v elektronickom podpise

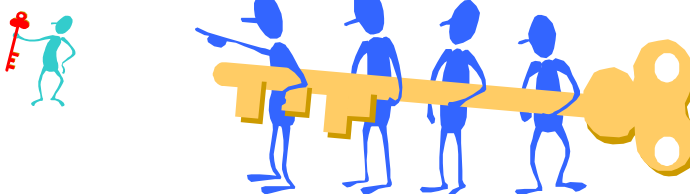
Kľúč z dvojice, ktorý máte len vy, sa volá **súkromný kľúč** alebo podpisový kľúč a kľúč z dvojice, ktorý zverejníte pre ostatných s informáciou, že patrí vám, sa nazýva **verejný kľúč** alebo overovací kľúč.

- **Súkromný kľúč** na uzamknutie odlačku elektronického dokumentu má **len podpisovateľ**



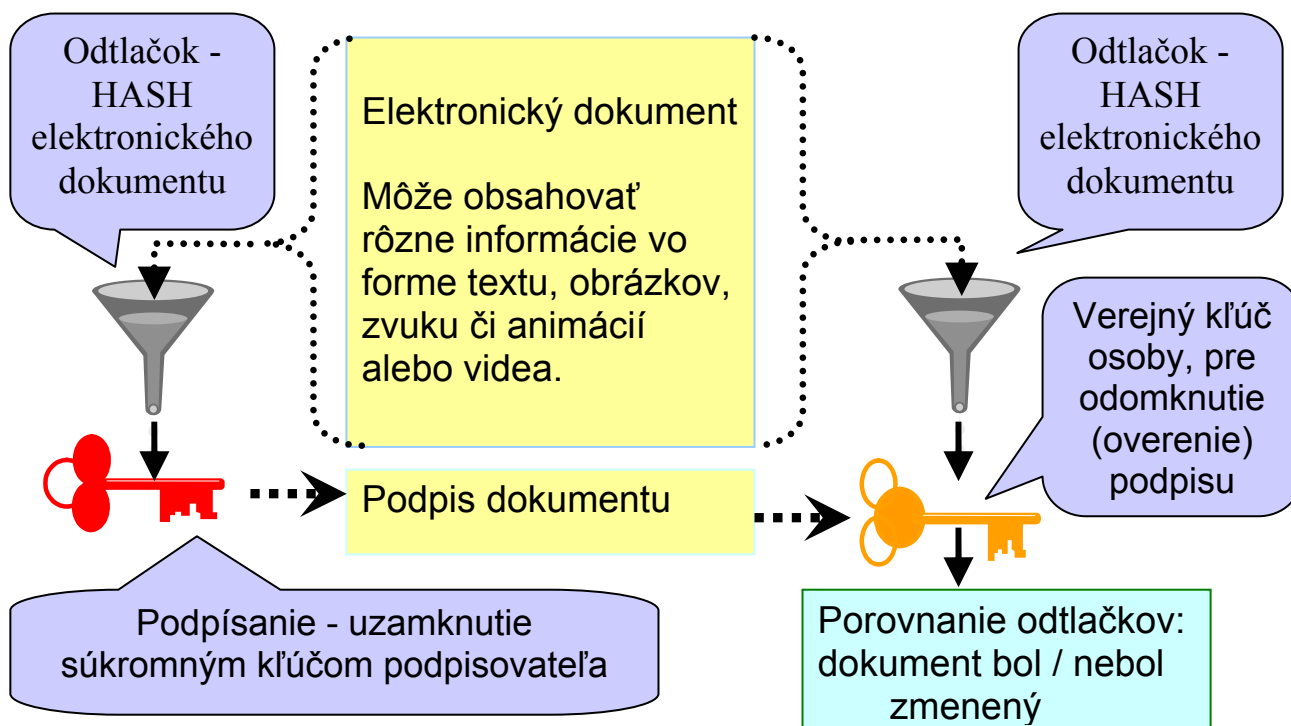
(máte len vy).

- **Verejný kľúč** na odomknutie odlačku a porovnanie s odlačkom kópie elektronického dokumentu je **pre overovateľov** v kópiách **verejne dostupný** (zverejníte ho s informáciou,



že je priradený **len vám**).

- **Overenie** - overovateľ porovnáva oba odlačky elektronického dokumentu:
 - Vypočítaný odlaček elektronického dokumentu.
 - Odomknutý odlaček elektronického dokumentu.



Uzamknutie elektronického dokumentu s vaším súkromným kľúčom sa obrazne označuje ako **elektronický podpis**. Toto pomenovanie uzamknutia elektronického dokumentu „elektronickým podpísaním“ vyvoláva u veľa ľudí úplne iné predstavy, než čo sa v skutočnosti pri elektronickom podpísaní deje. Namiesto **uzamknutia dokumentu** si ľudia často pod slovami „elektronický podpis“ predstavujú **rôzne elektronické kresby**.

Uzamknutie elektronického dokumentu s vaším verejným kľúčom sa označuje ako **zašifrovanie**, lebo odomknúť elektronický dokument môžete len vy s vaším súkromným kľúčom. Odomknutie elektronického dokumentu so súkromným kľúčom sa označuje ako **odšifrovanie**. Ľudia si často neuvedomujú, že ak posielajú nezašifrované elektronické dokumenty napríklad elektronickou poštou, tak tieto dokumenty sú čitateľné ako papierové pohľadnice a ľahko môže dôjsť k zneužitiu údajov z elektronických dokumentov. Preto, ak nechcete posielat' pohľadnice ale zalepené obálky, elektronický dokument pred odoslaním zašifrujte heslom alebo verejným kľúčom príjemcu. Ak šifrujete verejným kľúčom príjemcu, tak nezabudnite zašifrovať aj vaším verejným kľúčom, aby ste si elektronický dokument mohli aj vy odšifrovať. Vyskúšať si to môžete v bezplatnej aplikácii **LockIt** - <http://lockitsk.webnode.sk/> alebo <http://elpi2.szm.com>, ktorá spĺňa najnovšie bezpečnostné požiadavky kladené na takéto aplikácie a požiadavky EÚ Komisie.

8 Význam používania zaručeného elektronického podpisu v praxi a jeho prínos.

Zaručený elektronický podpis (ZEP) je definovaný v slovenskej legislatíve ako prostriedok pre zabezpečenie nepopierateľných vlastností elektronických dokumentov medzi ktoré patria hlavne:

- Obsah elektronického dokumentu nie je možné pozmenením falšovať – podpisovateľ a overovateľ má možnosť zobrazit' údaje z podpísaného elektronického dokumentu v presne tom istom tvare a prípadné zmeny budú pri overovaní ZEP odhalené.
- ZEP je možné overit' len s kópiami z jedného unikátneho verejného kľúča.
- Verejný kľúč na overenie ZEP bol spojený s identitou fyzickej osoby akreditovanou certifikačnou autoritou (ACA) v elektronickom dokumente a tento elektronický dokument sa nazýva kvalifikovaný certifikát. Kvalifikovaný certifikát podpísala ACA a ACA nesie bezvýhradnú zodpovednosť za overenie, že súkromný kľúč v čase podpísania kvalifikovaného certifikátu bol pod výhradnou kontrolou fyzickej osoby ktorej identitu ACA uviedla do kvalifikovaného certifikátu.
- ACA, minimálne po dobu ktorá je uvedená v kvalifikovanom certifikáte, poskytuje verejnú službu nahlásenia a zverejnenia zrušenia platnosti certifikátu vo verejne dostupnom zozname zrušených certifikátov CRL alebo aj v on-line službe OCSP poskytujúcej informácie o stave a platnosti certifikátov o ktorých stav OCSP priamo požiadate. Pri OCSP podľa slovenskej legislatívy musí odpoveď obsahovať aj hodnotu výsledku hašovacej funkcie z certifikátu, ktorého stav OCSP vracia, aby nedošlo k nesprávnej odpovedi pre neexistujúci certifikát a dlhodobo bola chránená integrita certifikátu.

Zákon č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov upravuje v § 40:

- odsek 4, druhá veta: Písomná forma je zachovaná vždy, ak právny úkon urobený elektronickými prostriedkami, je podpísaný zaručeným elektronickým podpisom.
- odsek 5: Pre právne úkony uskutočnené elektronickými prostriedkami, podpísané zaručeným elektronickým podpisom a opatrené časovou pečiatkou, sa osvedčenie pravosti podpisu nevyžaduje.

Zákon 215/2002 Z. z. definuje dva typy podpisov:

Elektronický podpis EP (§3) :

- je vyhotovený pomocou súkromného kľúča a elektronického dokumentu;
- pri overovaní na jeho základe a s použitím verejného kľúča možno overiť, že sa dokument nezmenil a možno identifikovať podpisovateľa.

Zaručený elektronický podpis ZEP (§4):

- je vyhotovený pomocou súkromného kľúča, ktorý je určený na vyhotovenie zaručeného EP;
- možno ho vyhotoviť len s použitím bezpečného zariadenia na vyhotovovanie zaručeného EP;
- na verejný kľúč patriaci k súkromnému kľúču použitému na vyhotovenie zaručeného EP je vydaný kvalifikovaný certifikát;
- spôsob jeho vyhotovenia umožňuje spoľahlivo určiť, ktorá fyzická osoba ho vyhotovila.

Spresnené pojmy Smernice 1999/93/ES

Korigendum k Rozhodnutiu Komisie 2009/767/ES zo 16. októbra 2009, ktorým sa ustanovujú opatrenia na uľahčenie postupov elektronickými spôsobmi prostredníctvom „miest jednotného kontaktu“ podľa Smernice Európskeho parlamentu a Rady 2006/123/ES o službách na vnútornom trhu (Úradný vestník Európskej únie L 274 z 20. októbra 2009) definuje:

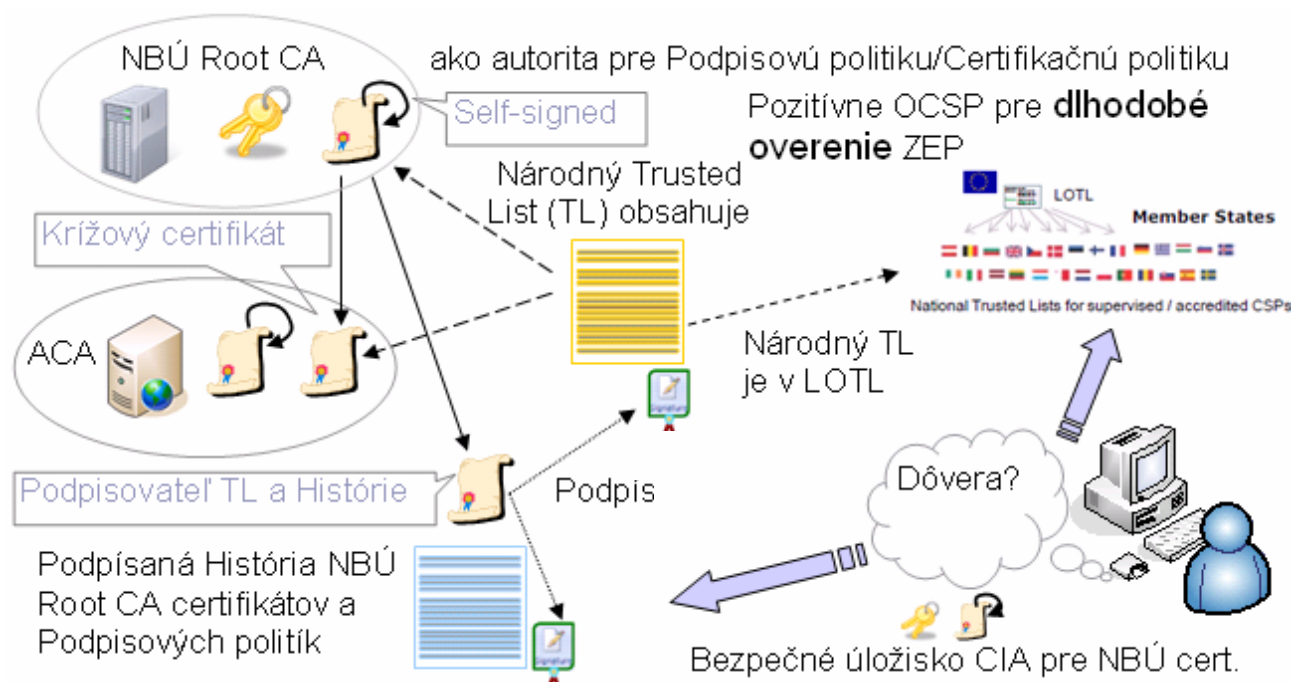
- **Kvalifikovaný elektronický podpis QES:** AdES, ktorý je podporovaný QC a ktorý je vytvorený SSCD, ako je vymedzené v článku 2 Smernice 1999/93/ES (Článok 5 - Právne účinky elektronických podpisov, bod 1.).
- **Zdokonalený elektronický podpis podporovaný kvalifikovaným certifikátom AdES QC:** Ide o elektronický podpis, ktorý spĺňa požiadavky na AdES a je podporovaný QC, ako je vymedzené v článku 2 Smernice 1999/93/ES.
- **Zdokonalený elektronický podpis AdES:** Ako je vymedzené v článku 2 ods. 2 Smernice 1999/93/ES.

QES a ZEP: ich hlavným cieľom je právny predpoklad, že podpisovateľ vytvoril podpis ako prejav svojej vôle – právny akt s časovo neobmedzenou platnosťou, čo je potrebné technicky zabezpečiť, aby nedošlo k popretiu platnosti pri overovaní napr. podpisov zmlúv z technických dôvodov alebo skončenia činnosti ACA. (NBÚ prevádzkuje dlhodobý archív kvalifikovaných certifikátov a certifikátov na správu, ktorých stav je možné zistiť dlhodobo cez Pozitívne OCSP).

EP, AdES a AdES QC: ich hlavným významom je zabezpečiť autentizáciu elektronického dokumentu podpisovateľom (metóda overovania pravosti). Zabezpečenie integrity podpísaného dokumentu a pripojenie identity podpisovateľa (hromadné podpisovanie faktúr organizáciou, potvrdenia z automatických systémov, potvrdenia o procese spracovania elektronických dokumentov bez predpokladu oboznámenia sa s ich obsahom, ako je napríklad prijatie a odoslanie elektronickou podateľňou)

9 Spôsoby overenia ZEP a rola NBÚ pri certifikácii, kontrole a pri overovaní dôvery.

Na celé overenie je potrebné spoľahlivo poznať len jeden kľúč NBÚ koreňovej CA pre dlhodobú dôveru v ZEP. Používateľ môže mať tento kľúč uložený na čipovej karte, ktorá je certifikovaná NBÚ ako SSCD a spĺňa EN 14890-1 obsahujúcu požiadavky z ISO/IEC 7816-15, kde CIA (Cryptographic Information Application) definuje uloženie kľúča koreňovej dôveryhodnej CA, teda NBÚ KCA v prostredí ZEP. Nasledujúci obrázok znázorňuje činnosti, ktoré vykonáva NBÚ a ktoré sú pre používateľa automatizované. Tieto činnosti zahŕňujú aj požiadavky legislatívy EÚ a to najmä Rozhodnutia Komisie 2010/425/EÚ, ktoré novelizovalo Rozhodnutie 2009/767/ES pre vydávanie národných dôveryhodných zoznamov a EÚ centrálného zoznamu odkazov na národné zoznamy.



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
TSA	Time Stamping Authority – vydáva časové pečiatky
TSL	Trust Status List – dôveryhodný zoznam podľa ETSI
TL	Trusted List (ako je definované v Rozhodnutí Komisie 2009/767/ES) – dôveryhodný zoznam podľa EÚ Komisie
SP	Signature Policy – podpisová politika
SSCD	Secure Signature-Creation Device – certifikovaná čipová karta alebo eID s čipom

10 Technické prostriedky pre elektronický podpis - SSCD

Ak štátne orgány pri komunikácii požadujú vlastnoručne podpísané dokumenty a vy chcete tieto dokumenty zaslať elektronicky, potom ich musíte podpísať **zaručeným elektronickým podpisom (ZEP)**, teda uzamknúť vašim súkromným kľúčom. Pritom ale musia byť splnené nasledovné požiadavky:

- **Súkromný kľúč** musí spĺňať technické požiadavky definované NBÚ a váš súkromný kľúč musíte mať uložený na bezpečnom zariadení pre vytváranie zaručeného elektronického podpisu (SSCD - Secure Signature-Creation Device), ktorý taktiež preverilo NBÚ. SSCD je najčastejšie karta s čipom podobná bankomatovej karte. Prakticky za vás tieto požiadavky musí splniť organizácia akreditovaná NBÚ, ktorá vám takéto SSCD predá a podľa technických požiadaviek NBÚ vám v ňom vygeneruje vašu dvojicu súkromného a verejného kľúča. Požiadavky na SSCD vyplývajú z **Rozhodnutia Komisie 2003/511/ES**.
- Aby každý, kto bude overovať váš podpis s vašim verejným kľúčom vedel, že je to váš verejný kľúč, akreditovaná organizácia vytvorí nový elektronický dokument, do ktorého uloží:
 - váš verejný kľúč spolu

- o s vašimi identifikačnými údajmi, ktoré overila na základe vášho občianskeho preukazu alebo pasu (tieto identifikačné údaje pri komunikácii so štátnou správou musia obsahovať aj vaše rodné číslo),
- o ďalej identifikačné údaje akreditovanej organizácie, ktorá zodpovedá za predanie SSCD, vygenerovanie kľúčového páru a overenie vašej identity,
- o a sériové číslo tohto elektronického dokumentu.

Tento elektronický dokument po elektronickom podpísaní nazývame **kvalifikovaný certifikát** a akreditovanú organizáciu, ktorá kvalifikovaný certifikát podpísala, nazývame akreditovanou certifikačnou autoritou.

- Vami podpísaný elektronický dokument, ktorý ste podpísali s vašim súkromným kľúčom, musí byť uložený do takého súboru, ktorého obsah definuje NBÚ vo formátoch pre ZEP, aby overovateľ presne vedel, kde môže nájsť dokument, ktorý ste podpísali a kde je váš podpis a váš kvalifikovaný certifikát obsahujúci váš verejný kľúč, ktorým sa váš podpis overuje. Pritom formát podpísaného elektronického dokumentu môže byť len zo skupiny formátov dokumentov zverejnených NBÚ, ako napríklad RTF, PDF, TXT v UTF8 kódovaní, aby sa podpisovateľovi a overovateľovi podpísaný elektronický dokument zobrazil presne tak isto a bez akýchkoľvek zmien.

11 PKI infraštruktúra ako prvok dôveryhodnosti v prostredí elektronického podpisu

Aby overovateľ vedel, či kvalifikovaný certifikát je skutočne podpísaný akreditovanou certifikačnou autoritou akreditovanou NBÚ, NBÚ po prekontrolovaní splnenia požiadaviek pre akreditáciu, vydá certifikát pre akreditovanú certifikačnú autoritu, ktorý bude obsahovať verejný kľúč akreditovanej certifikačnej autority a identifikačné údaje akreditovanej certifikačnej autority a identifikačné údaje NBÚ. NBÚ si tiež vydá samo sebe takýto certifikát a tento certifikát zverejní ako základný dôveryhodný bod, alebo tiež nazývaný koreňový certifikát. Na základe dôvery v tento koreňový certifikát potom viete postupne overiť elektronické podpisy certifikátov jednotlivých akreditovaných certifikačných autorít až po podpis ZEP, ktorým bol elektronický dokument podpísaný. Aby sa odlišili certifikáty pre overovanie ZEP (certifikáty na správu kvalifikovaných certifikátov) a ostatné certifikáty, napríklad tie, ktoré obsahujú kľúče pre šifrovanie, NBÚ zverejnilo objektový identifikátor (**OID 1.3.158.36061701.0.0.0.1.2.2**), ktorý sa skladá z postupnosti čísel a všetky **certifikáty používané pre overovanie ZEP musia tento OID obsahovať**.

12 Legislatívne prostredie implementácie elektronického podpisu v SR a EÚ

Aby bolo možné overovanie elektronických podpisov aj v rámci EÚ, v súčasnosti Komisia EÚ podpisuje zoznam odkazov na národné dôveryhodné zoznamy na základe implementácie Direktívy o službách a Direktívy 1999/93/ES o elektronickom podpise. Jednotlivé krajiny, na základe týchto direktív, vydávajú dôveryhodné zoznamy, ktoré obsahujú zoznam akreditovaných certifikačných autorít a certifikačných autorít pod dohľadom organizácií definovaných v národných legislatívach. Pri overovaní sa potom certifikáty zahraničnej certifikačnej autority získajú z dôveryhodného zoznamu a tak overovateľ bude vedieť, či elektronický podpis bol vytvorený kľúčom, za ktorý zodpovedala osoba, ktorej nekorektná činnosť je postihnutelná sankciami vyplývajúcimi z legislatívy konkrétneho štátu uvedeného v dôveryhodnom zozname.

Pri komunikácii so zahraničím sa budeme najčastejšie stretávať s anglickými názvami pre ZEP. Ekvivalentom ZEP definovaného slovenskou legislatívou je technický anglický termín Qualified Electronic Signature (QES) ale iba v prípade, ak je aplikácia pre QES certifikovaná podľa pravidiel slovenskej legislatívy. Pri komunikácii so zahraničím si ale treba dávať pozor, lebo v našej legislatíve nepoznáme pojem Advanced Electronic Signature (AdES) based on Qualified Certificate

(QC), teda EP založený na kvalifikovanom certifikáte, ktorého súkromný kľúč nie je uložený na SSCD. A obzvlášť nešťastný je preklad AdES based on QC do českej legislatívy, kde ho nazvali ZEP, čo je niečo úplne iné ako ZEP uvedený v slovenskej legislatíve.

Významný rozmach využitia elektronického podpisu v cezhraničnom prostredí nastal vďaka implementácii požiadaviek smernice o službách, prostredníctvom ktorej sa pri poskytovaní služieb elektronickými prostriedkami prijali nové požiadavky v nasledujúcej európskej legislatíve:

- Smernica Európskeho parlamentu a Rady **2006/123/ES** z 12. decembra 2006 o službách na vnútornom trhu
- Rozhodnutie Komisie **2009/767/ES** zo 16. októbra 2009, ktorým sa ustanovujú opatrenia na uľahčenie postupov elektronickými spôsobmi prostredníctvom „miest jednotného kontaktu“ podľa Smernice Európskeho parlamentu a Rady 2006/123/ES o službách na vnútornom trhu **novelizované** Rozhodnutím Komisie **2010/425/EÚ**, ktoré prikazuje členským štátom vydávať dôveryhodný zoznam TL poskytovateľov certifikačných služieb akreditovaných a pod dohľadom.
 - ETSI TS 102 231 – Electronic Signatures and Infrastructures (ESI): Provision of harmonized Trust-service status information.
- **Rozhodnutie Komisie 2011/130/ES**, ktorým sa ustanovujú minimálne požiadavky na cezhraničné spracovanie dokumentov elektronicky podpísaných príslušnými orgánmi v zmysle Smernice Európskeho parlamentu a Rady 2006/123/ES o službách na vnútornom trhu.

13 Platnosť certifikátu a podpisu

Povinnosťou každého vydavateľa certifikátov je do certifikátu uviesť aj obdobie použiteľnosti vydaného certifikátu (od, do), počas ktorého musí vydavateľ certifikátu poskytovať pre osobu, ktorej bol certifikát vydaný, službu, ktorá umožní nahlásenie straty alebo inej kompromitácie súkromného kľúča. Vydavateľ certifikátu pri nahlásení kompromitácie podpisovateľom musí overiť, či osoba, ktorá nahlásuje kompromitáciu, je na to oprávnená a ak áno, potom musí vydavateľ certifikátu max. do 24 hodín túto informáciu zverejniť vo vydavateľom elektronicky podpísanom zozname zrušených certifikátov (Certificate Revocation List - CRL) ktorý obsahuje sériové číslo zrušeného certifikátu s časom, kedy k zrušeniu certifikátu došlo. Zoznam zrušených certifikátov obsahuje čas, kedy tento zoznam bol vytvorený (nové zrušenie certifikátu môže obsahovať len čas po tomto čase vydania posledného CRL) a identifikačné údaje podpisovateľa tohto zoznamu zrušených certifikátov.

Aby sme vedeli, či ZEP bol vytvorený v čase, kedy bol certifikát platný, teda v časovom intervale uvedenom v certifikáte (od, do) alebo pred časom, kedy zrušenie certifikátu bolo zverejnené v zozname zrušených certifikátov (CRL), do ZEP sa po podpise pridá časová pečiatka informujúca o čase vytvorenia ZEP. Časová pečiatka slúži na zabezpečenie integrity opečiatkovaného elektronického dokumentu a obsahuje čas, kedy bol dokument elektronicky opečiatkovaný. Postup **vytvorenia časovej pečiatky** je definovaný v § 7 ods. 2 vyhlášky č. **135/2009 Z. z.** (o vyhotovení a overovaní elektronického podpisu a časovej pečiatky). **Časová pečiatka** je elektronický dokument podpísaný časovou autoritou, kde podpísaný dokument obsahuje časový údaj a odtlačok zo ZEP podpisu. O časovú pečiatku požiada podpisovateľ po vytvorení elektronického podpisu, kde v žiadosti zašle časovej autorite odtlačok z práve vytvoreného elektronického podpisu a časová autorita vytvorí elektronický dokument, do ktorého pridá práve tento odtlačok a aktuálny časový údaj. Po podpísaní elektronického dokumentu časovou autoritou vznikne časová pečiatka a túto časovú pečiatku časová autorita zašle podpisovateľovi ZEP. Časovú pečiatku môže do ZEP podpisu pridať aj overovateľ, no počas doby, od kedy bol podpis vyhotovený do času, kedy do podpisu vložil časovú pečiatku overovateľ, by mohlo dôjsť k zrušeniu certifikátu a teda ku strate platnosti ZEP, a preto je lepšie, aby o časovú pečiatku ZEP požiadal podpisovateľ ihneď po podpísaní.

Na záver ešte spomeniem niektoré dôležité pojmy. Odtlačok, spomenutý pri časovej pečiatke, je výsledná hodnota z hašovacej funkcie. Hašovacia funkcia zabezpečí transformáciu vstupnej informácie obsiahnutej napr. v podpisovanom dokumente do výstupnej informácie uloženej v konštantne veľkom bloku jednotiek a núl. Obrazne si hašovaciú funkciu môžete predstaviť ako mlynček alebo mixér, do ktorého nahádzate v presne definovanom poradí dokumenty, ktoré sa rozmixujú a z neho vylejete vždy rovnako veľký mix súbor. Inak povedané, ak vhodíte rovnaké dokumenty, tak vyberiete vždy rovnaký mix súbor s rovnakou hodnotou. Najčastejšie sa používajú hašovacie funkcie SHA-256 a SHA-1, ktorých výstupný blok má veľkosť 160 bitov. MD5, ktorej výstupný blok má veľkosť 128 bitov sa už nesmie používať, lebo jej algoritmus už rozbili natoľko, že za pár minút vedia nájsť k jednému MD5 výstupnému 128 bitov veľkému bloku rôzne vstupné dokumenty a teda sfalšovať všetko, kde by MD5 bola použitá. Ak si predstavíme obsah elektronického dokumentu ako jedno veľmi veľké číslo, čiže súbor obsahuje jednu informáciu, potom nám z toho vyplýva, že bežný elektronický dokument o veľkosti 60kBytov ($60 \cdot 1024 \cdot 8$ bitov) môže obsahovať 2^{491520} rôznych informácií, zatiaľ čo hašovacia funkcia SHA-1 "len" 2^{160} rôznych informácií. Z toho nám vyplýva, že ku každej z $(2^{491520} - 2^{160})$ rôznej informácie uloženej v 60kBytovom súbore môžeme nájsť aspoň jednu takú, ktorá bude mať rovnakú hašovaciú hodnotu. Ale 2^{160} je dostatočne veľké číslo na to, aby sme dúfali, že dva rôzne dokumenty nebudú mať rovnakú hašovaciú hodnotu. Z tohto dôvodu NBÚ zverejňuje na svojej stránke zoznamy algoritmov, ktoré sa ešte nepodarilo rozbiť (bez napr. MD5) a minimálne dĺžky kľúčov pre takéto algoritmy a to vo forme **podpisových politik**, ktoré NBÚ schvaľuje a zverejňuje na určité obdobie, počas ktorého sa predpokladá, že nedôjde k prelomeniu zverejnených algoritmov.

Príloha A (informatívna) Príklady

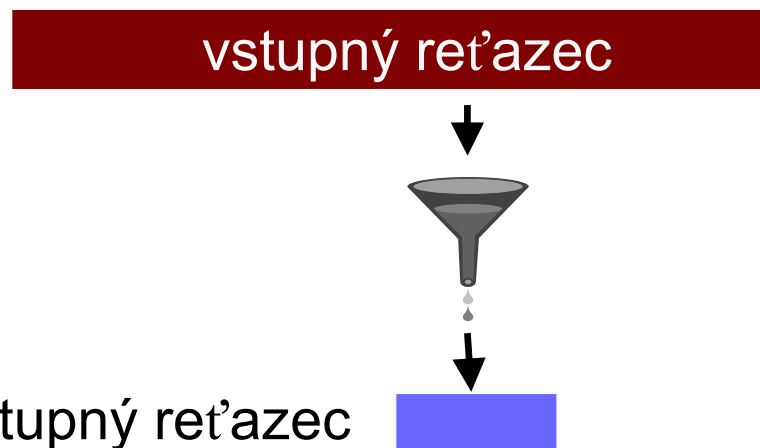
A.1 SSCD pre uloženie kľúčového páru a pre kvalifikovaný certifikát

Uloženie súkromného kľúča:

- čipová smart karta,
- SIM mobilného zariadenia
- USB token



A.2 Hašovacia funkcia



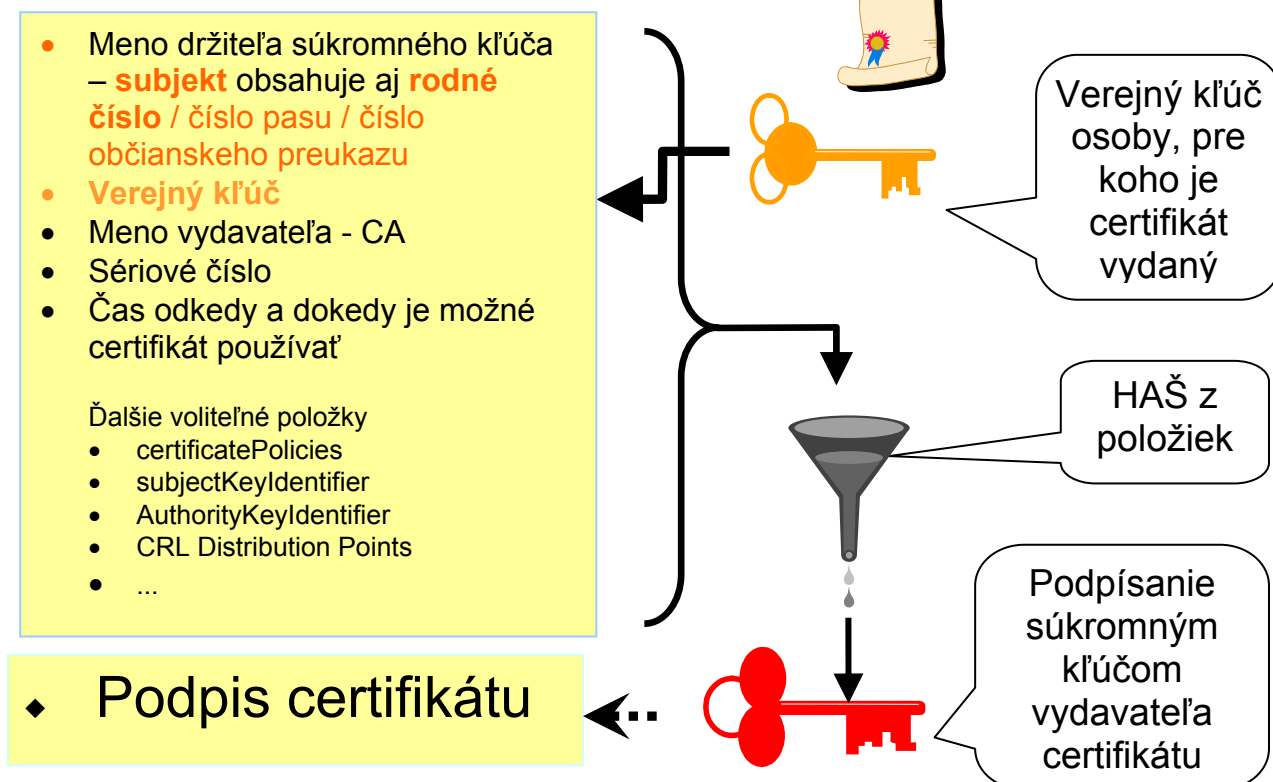
Všeobecne sa pod hašovacou funkciou rozumie zobrazenie h , ktoré vstupnému reťazcu ľubovoľnej dĺžky priraduje výstupný reťazec konštantnej dĺžky.

Hašovacie funkcie pre elektronický podpis musia spĺňať bezpečnostnú vlastnosť, že z výsledného reťazca hašovacej funkcie nie je možné zistiť vstupný reťazec a k jednému výstupnému reťazcu hašovacej funkcie sa nesmie podariť nájsť algoritmus, ako získať dva rôzne vstupné reťazce.

Hašovacia funkcia je kolízna funkcia a preto k jednej hašovacej hodnote musí existovať veľké množstvo rôznych vstupných dokumentov, ak vstupný dokument má viac bitov, ako je veľkosť hašovacej hodnoty (počet bitov hašovacej hodnoty).

.m skúšaním rôznych vstupných hodnôt.

A.3 Obsah certifikátu X.509



Certifikát vydal - Issuer name:

cn = **Info CA1** (Common Name)
ou = **Test** (Organisational Unit Name)
o = **InfoLook** (Organisation Name)
l = **Bratislava** (Locality)
c = **SK** (Country Name)

Certifikát je vydaný pre - Subject name:

cn = **Peter Rybár** (Common Name)
ou = **Vývoj** (Organisational Unit Name)
o = **SAV** (Organisation Name)
l = **Bratislava** (Locality)
c = **SK** (Country Name)
Email = pr@mailbox.sk

Certifikát je platný - Certificate is valid:

Od - from: **25. 9. 2004 11:23:52**
Do - to: **25. 9. 2007 11:23:52**

Sériové číslo certifikátu - serial number:

4DTyp verejného kľúča: **RSA**veľkosť **2048**modulus **00 DB 74 27 F3 4D 86 ...**verejný exponent **65537**

Niektoré štandardné rozšírenia (atribúty):

Základné obmedzenie CA = NIE

Crl Distribution Point is:

URL = <http://infol.sk/ca2001.crl>

Certifikačná politika

OID '1 3 158 36061701 0 0 0 1 2 2'

Použitie kľúča

nonRepudiation

...

Hašovacia hodnota certifikátu - fingerprint:

SHA1 = **DB 65 39 7D 1E F8 71 F2 32 74
1D D7 86 48 11 C9 ED 26 2C 15**

A.4 Vydané CRL

CRL vydal - Issuer name:
 cn = **Info CA1** (Common Name)
 ou = **Test** (Organisational Unit Name)
 o = **InfoLook** (Organisation Name)
 l = **Bratislava** (Locality)
 c = **SK** (Country Name)

Čas vydania CRL **25. 9. 2005 11:29:57**,

Čas ďalšieho vydania **26. 9. 2005 11:29:57**

Zoznamu zrušených certifikátov:

Sériové číslo certifikátu: **01**
 Čas zrušenia **3. 5. 2000 13:27:24**

Sériové číslo certifikátu: **02**
 Čas zrušenia **3. 5. 2000 13:27:36**

Sériové číslo certifikátu: **03**
 Čas zrušenia **3. 5. 2000 13:27:51**

Sériové číslo certifikátu: **04**
 Čas zrušenia **2. 5. 2001 10:57:35**

Sériové číslo certifikátu: **3B**

Čas zrušenia **7. 5. 2001 12:51:34**

Sériové číslo certifikátu: **4D**

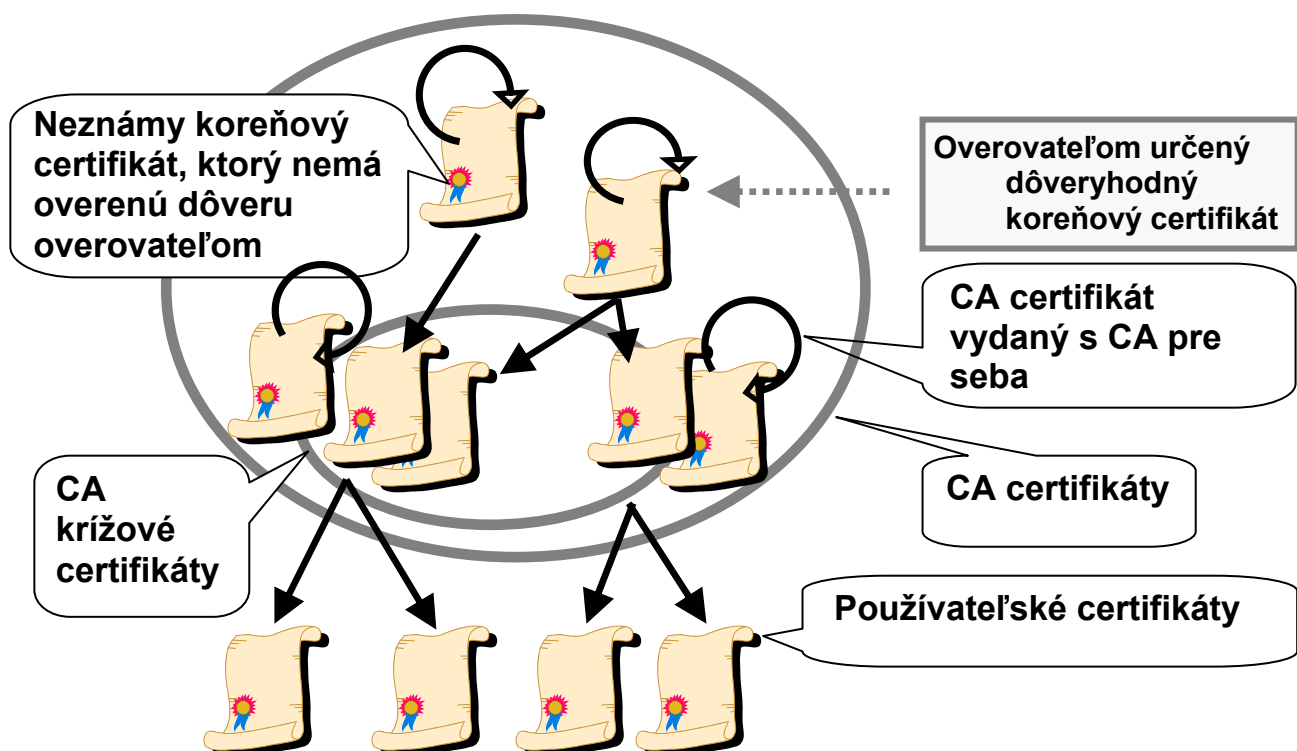
Čas zrušenia **25. 7. 2005 11:29:43**

Čas Invalidity Date **23. 7. 2005 11:29:57**

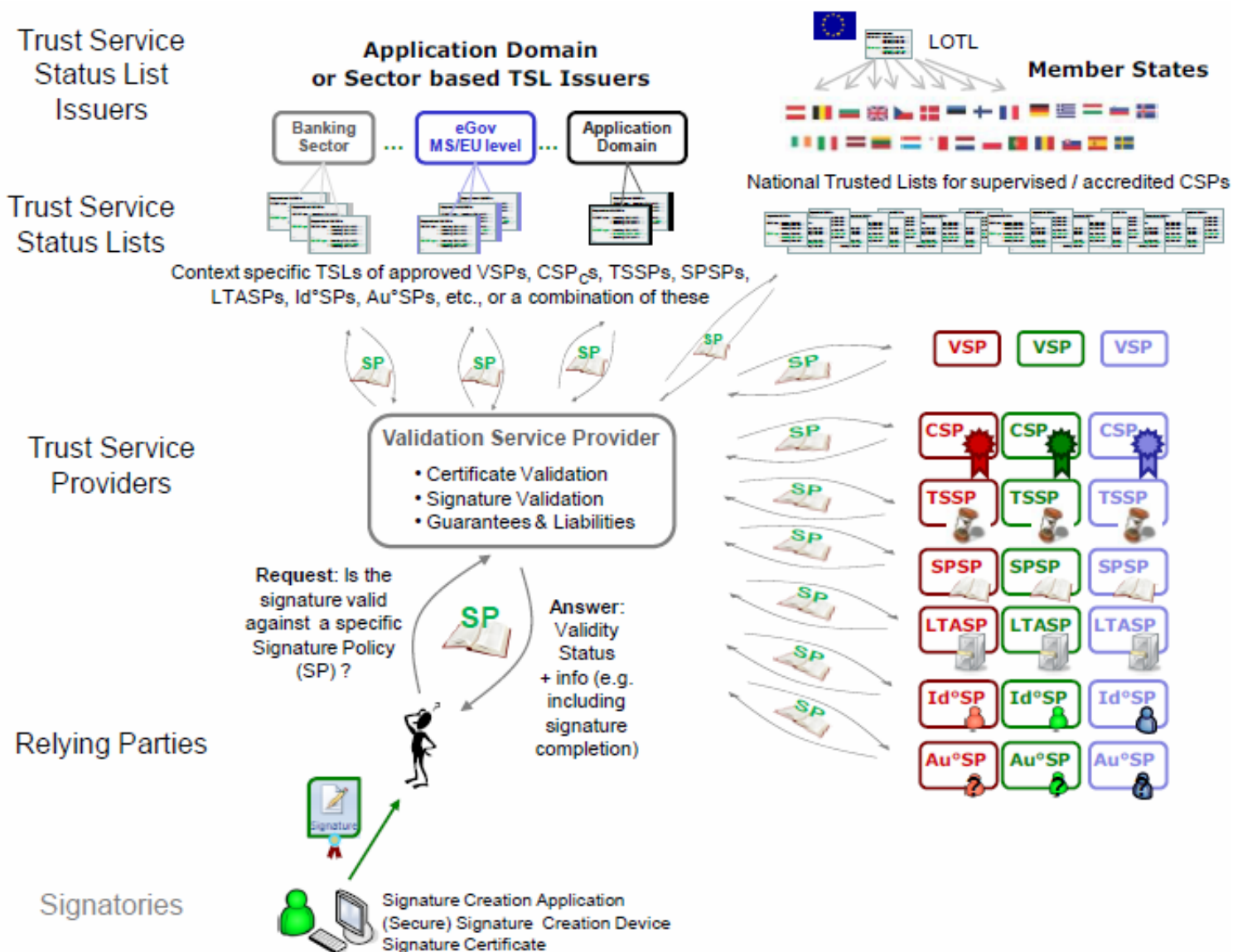
V zákone o elektronickom podpise (EP) sa v § 8 ods. 3 píše, že telo zoznamu zrušených certifikátov (CRL) je elektronický dokument, ktorý obsahuje najmä

1. identifikačné údaje vydavateľa certifikátov, ktorý spravuje tieto certifikáty,
2. dátum a čas vydania zoznamu zrušených certifikátov,
3. dátum a čas najneskoršieho vydania ďalšieho zoznamu zrušených certifikátov,
4. zoznam identifikačných čísiel certifikátov, ktoré boli zrušené spolu s dátumom a časom ich zrušenia.

A.5 PKI hierarchia overovania

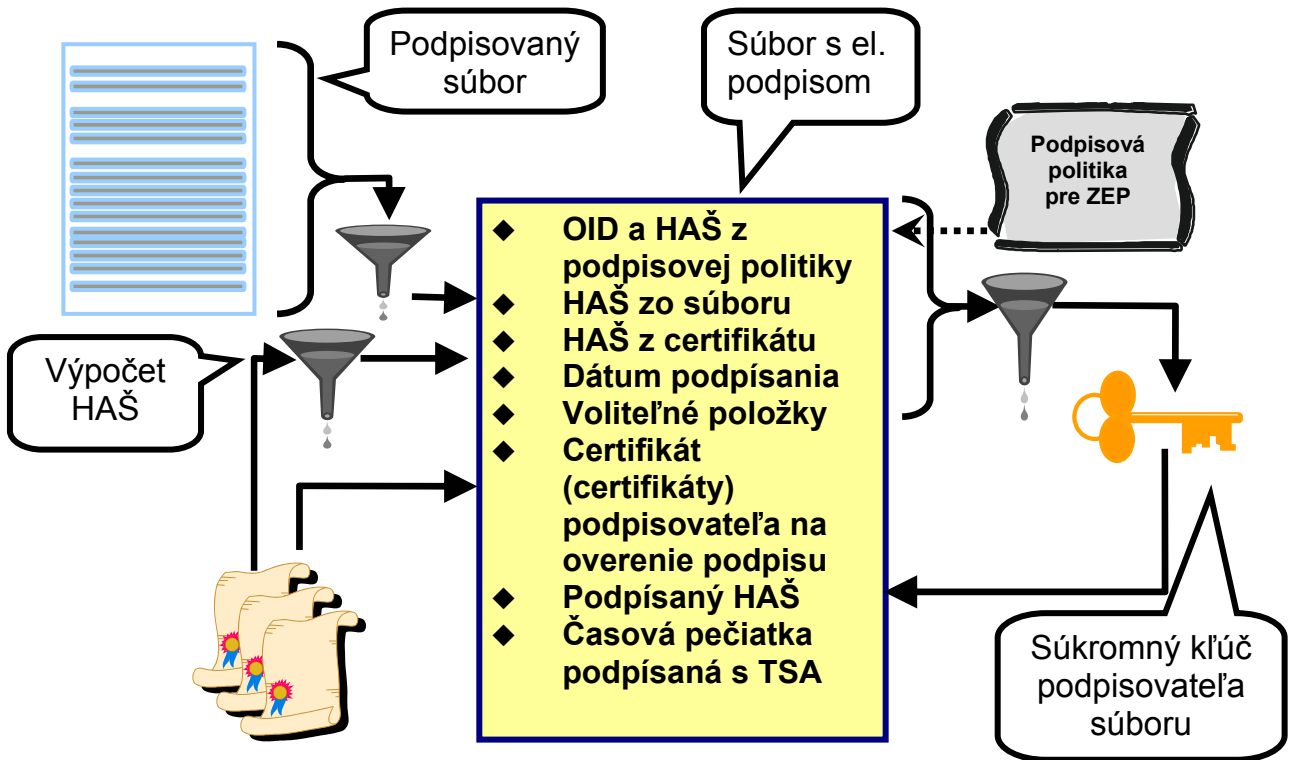


A.6 Ideálny model pre overenie ZEP podľa Komisie EÚ

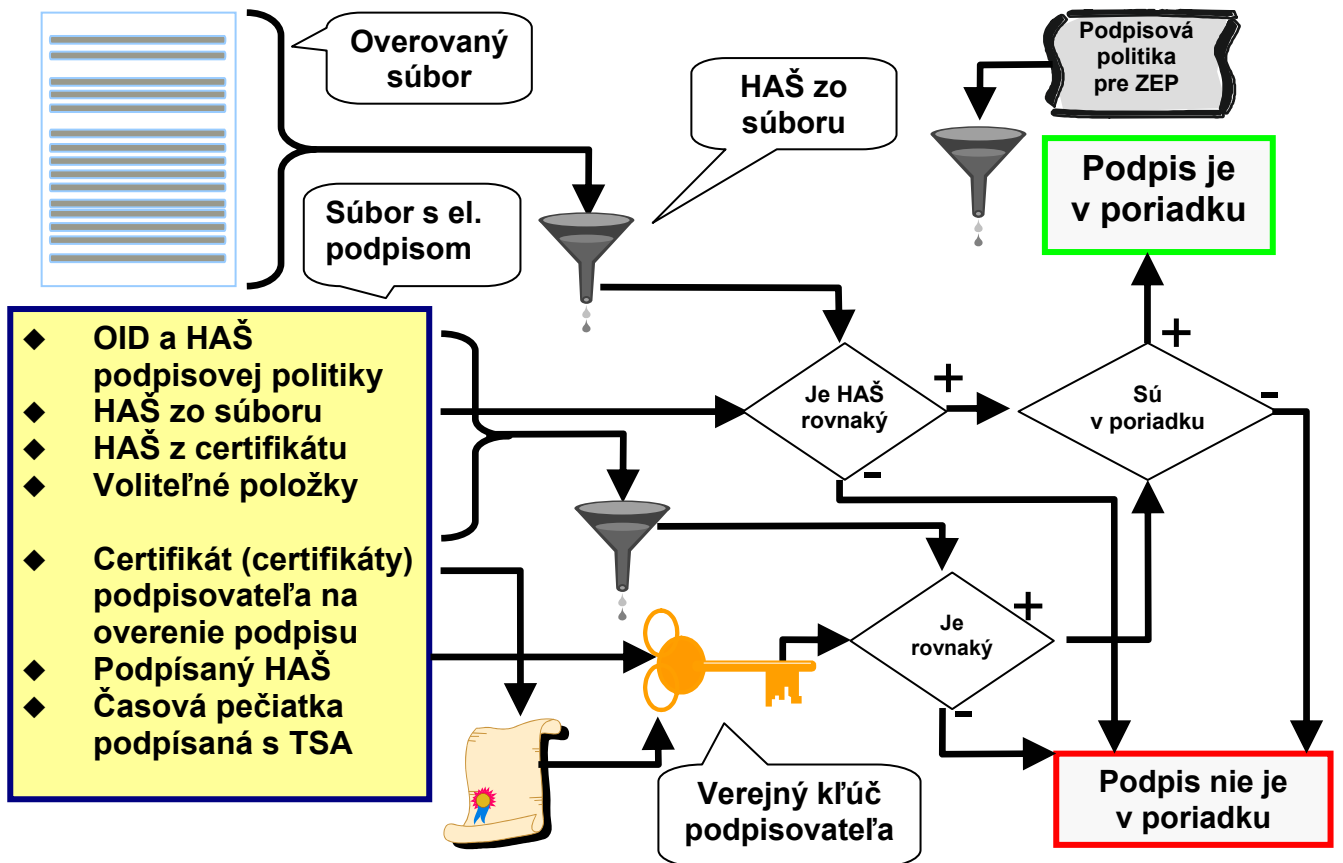


- CSP Certification Service Provider
- VSP Validation Service Provider
- CA Certification Authority
- TSSP Time Stamping Service Provider
- LTASP Long Term Archiving Service Provider
- SPSP Signature Policy Service Provider (Signature Policy Issuer)
- Id°SP Identification Service Provider
- Au°SP Authentication Service Provider
- SP Signature Policy
- TSL Trust Status List
- TL Trusted List (as defined in Commission Decision 2009/767/EC)
- LOTL List Of The Lists

A.7 Podpísanie súboru



A.8 Overenie podpisu



Príloha B (informatívna) Rozhodnutie Komisie (2003/511/ES)

A. Zoznam všeobecne uznávaných štandardov pre produkty elektronického podpisu, ktoré členské štáty musia akceptovať, sú v súlade s požiadavkami uvedenými v Prílohe II (f) Smernice 1999/93/ES.

- CWA 14167-1 (marec 2003) Bezpečnostné požiadavky pre dôveryhodné systémy spravujúce certifikáty pre elektronické podpisy, Časť 1: Požiadavky bezpečnosti systému
- CWA 14167-2 (marec 2002) Bezpečnostné požiadavky pre dôveryhodné systémy spravujúce certifikáty pre elektronické podpisy, Časť 2: Kryptografický modul pre podpisové operácie CSP–Profil ochrany (MCSO – PP)

B. Zoznam všeobecne uznávaných štandardov pre produkty elektronického podpisu, ktoré členské štáty musia akceptovať, sú v súlade s požiadavkami uvedenými v Prílohe III Smernice 1999/93/ES.

- CWA 14169 (marec 2002) Bezpečné zariadenia na vyhotovenie podpisu "EAL 4+"

Príloha C (informatívna) Legislatíva pre elektronický podpis

Dňa 15. marca 2002 bol Národnou radou Slovenskej republiky prijatý zákon č. [215/2002 Z. z.](#) o elektronickom podpise a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon“). Zákon upravuje vzťahy vznikajúce v súvislosti s vyhotovovaním a používaním elektronického podpisu, práva a povinnosti fyzických osôb a právnických osôb pri používaní elektronického podpisu, hodnovernosť a ochranu elektronických dokumentov podpísaných elektronickým podpisom. Zákon nadobudol účinnosť v plnom rozsahu dňa 1. septembra 2002. Zákon vychádza zo Smernice Európskej únie č. 1999/93/ES z decembra 1999.

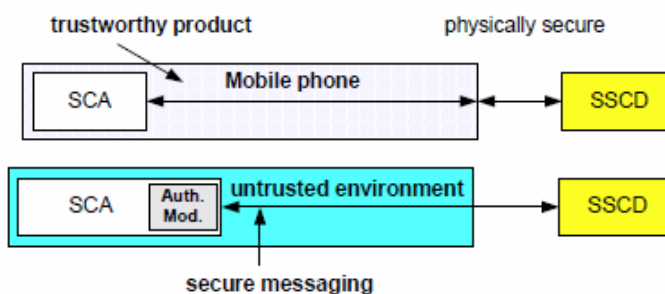
Národný bezpečnostný úrad je ústredným orgánom štátnej správy pre elektronický podpis.

[Vykonávacie právne predpisy](#) k zákonu č. 215/2002 Z. z. o elektronickom podpise a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, účinné od 8. apríla 2009:

- Vyhláška Národného bezpečnostného úradu č. 131/2009 Z. z., o formáte, obsahu a správe certifikátov a kvalifikovaných certifikátov a formáte, periodicite a spôsobe vydávania zoznamu zrušených kvalifikovaných certifikátov (**o certifikátoch a kvalifikovaných certifikátoch**)
- Vyhláška Národného bezpečnostného úradu č. 132/2009 Z. z., o podmienkach na poskytovanie akreditovaných certifikačných služieb a o požiadavkách na audit, rozsah auditu a kvalifikáciu auditorov (**o službách ACA a audite**)
- Vyhláška Národného bezpečnostného úradu č. 133/2009 Z. z., o obsahu a rozsahu prevádzkovej dokumentácie vedenej certifikačnou autoritou a o bezpečnostných pravidlách a pravidlách na výkon certifikačných činností (**o bezpečnosti služieb CA**)
- Vyhláška Národného bezpečnostného úradu č. 134/2009 Z. z., ktorou sa ustanovujú podrobnosti o požiadavkách na bezpečné zariadenia na vyhotovovanie časovej pečiatky a požiadavky na produkty pre elektronický podpis (**o produktoch elektronického podpisu**)
- Vyhláška Národného bezpečnostného úradu č. 135/2009 Z. z., o formáte a spôsobe vyhotovenia zaručeného elektronického podpisu, spôsobe zverejňovania verejného kľúča úradu, podmienkach platnosti pre zaručený elektronický podpis, postupe pri overovaní a podmienkach overovania zaručeného elektronického podpisu, formáte časovej pečiatky a spôsobe jej vyhotovenia, požiadavkách na zdroj časových údajov a požiadavkách na vedenie dokumentácie časových pečiatok (**o vyhotovení a overovaní elektronického podpisu a časovej pečiatky**)
- Vyhláška Národného bezpečnostného úradu č. 136/2009 Z. z., o spôsobe a postupe používania elektronického podpisu v obchodnom styku a administratívnom styku

Štandardy EÚ a NBÚ pre SSCD

Štandard EÚ - EN 14890-1:2008



Štandard NBÚ - SIM karta mobilu ako bezpečné zariadenie pre vytváranie zaručeného elektronického podpisu (ZEP).

Definuje DiGiID súbor pre automatickú konfiguráciu podpisovej a overovacej aplikácie (podpísaný podpisovateľom). Obsahuje verejný podpisový a šifrovací kľúč podpisovateľa uložený v certifikátoch a koreňové certifikáty dôvery.

Súkromný podpisový a (od)šifrovací kľúč je uložený na SIM



Na mobile sa zadá správny **prístupový kód**, ktorý bol zobrazený podpisovateľovi pred podpísaním (WEB, PC).



Až potom je možné zadať podpisový PIN pre podpis.



Príloha E (informatívna) Úlohy úradu pre oblasť EP

Podľa § 10 zákona 215/2002 Z. z. z 15. marca 2002 - NBÚ (ďalej len úrad):

(1) Ústredným orgánom štátnej správy pre elektronický podpis je úrad.

(2) Úrad plní tieto úlohy:

a) vykonáva kontrolu dodržiavania tohto zákona (§ 11),

b) posudzuje žiadosti certifikačných autorít pôsobiacich na území Slovenskej republiky o akreditáciu, udeľuje a odníma certifikačným autoritám akreditáciu a vydáva osvedčenia o akreditácii,

c) vydáva certifikáty verejných kľúčov podľa § 6 ods. 7 ním akreditovaným certifikačným autoritám,

d) zverejňuje vlastný verejný kľúč podľa § 4 ods. 5 a vydáva certifikát svojho vlastného verejného kľúča podľa § 6 ods. 9,

e) vydáva certifikáty verejných kľúčov zahraničným certifikačným autoritám podľa § 17 ods. 1 písm. a) a c),

f) eviduje certifikačné authority pôsobiace v Slovenskej republike,

g) vedie zoznam akreditovaných certifikačných autorít pôsobiacich na území Slovenskej republiky a zoznam certifikačných autorít, ktorým odňal akreditáciu; tento zoznam úrad zverejňuje na voľne prístupnej internetovej stránke,

h) zrušuje certifikát, ktorý vydal akreditovanej certifikačnej autorite, ak akreditovanej certifikačnej autorite odníme akreditáciu alebo ak táto ukončí svoju činnosť,

i) vedie register zahraničných certifikačných autorít, ktorých certifikáty boli úradom uznané na použitie v Slovenskej republike,

j) certifikuje produkty pre elektronický podpis, najmä bezpečné zariadenia na vyhotovovanie elektronického podpisu a bezpečné zariadenia na vyhotovovanie časových pečiatok, vydáva odporúčania, štandardy a smernice z oblasti elektronického podpisu,

k) plní ďalšie úlohy, ktoré mu vyplývajú z tohto zákona; na plnenie svojich úloh môže požiadať o spoluprácu aj iné štátne orgány a ďalšie fyzické osoby a právnické osoby,

l) poskytuje akreditované certifikačné služby príslušníkom a zamestnancom úradu a na požiadanie príslušníkom Policajného zboru a zamestnancom Ministerstva vnútra Slovenskej republiky pre plnenie úloh ustanovených osobitným predpisom, 2e) príslušníkom ozbrojených síl a zamestnancom Ministerstva obrany Slovenskej republiky pre plnenie úloh ustanovených osobitným predpisom, 2f) príslušníkom a zamestnancom Slovenskej informačnej služby, zamestnancom Ministerstva spravodlivosti Slovenskej republiky, súdom Slovenskej republiky a prokuratúre pre plnenie úloh ustanovených osobitnými predpismi, 2g)

m) vedie zoznam všetkých vydaných kvalifikovaných certifikátov spolu s informáciami o ich platnosti zaslaných podľa § 14 ods. 3 písm. e) a poskytuje z neho informácie,

n) vydáva certifikáty ním akreditovaným certifikačným autoritám pre službu časovej pečiatky podľa § 2 písm. l) tretieho bodu,

o) poskytuje Európskej komisii a členským štátom Európskej únie zoznamy akreditovaných certifikačných autorít pôsobiacich na území Slovenskej republiky, zoznamy certifikačných autorít, ktorým odňal akreditáciu, údaje z registra zahraničných certifikačných autorít, ktorých certifikáty boli úradom uznané na použitie v Slovenskej republike a bezodkladne im oznamuje každú zmenu a doplnenie poskytovaných informácií.

(3) Požiadavky na správu kvalifikovaných certifikátov akreditovanou certifikačnou autoritou sa vzťahujú aj na úrad.

Príloha F (informatívna) Zoznam použitej literatúry

<http://www.nbusr.sk/sk/elektronicky-podpis/index.html>

ETSI TS 102 176-1: "Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms".

Electronic Signatures

<http://www.cen.eu/CENORM/BusinessDomains/businessdomains/iss/cwa/electronic+signatures.asp>

CEN/TC+224- Standards under development

<http://www.cen.eu/CENORM/BusinessDomains/TechnicalCommitteesWorkshops/CENTechnicalCommittees/WP.asp?param=6205&title=CEN/TC%2B224>

EN 14890-1 Application Interface for smart cards used as secure signature creation devices - Part 1: Basic services

EN 14890-2 Application Interface for smart cards used as secure signature creation devices - Part 2: Additional services

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:299:0018:0054:EN:PDF>
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:299:0018:0054:SK:PDF>

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=DD:13:24:31999L0093:SK:PDF>
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:175:0045:0046:EN:PDF>

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:274:SOM:SK:HTML>

Certifikát EU trust TSL

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:057:0015:0015:SK:PDF>
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:057:0015:0015:EN:PDF>

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:199:0030:0035:EN:PDF>
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:199:0030:0035:SK:PDF>

List of Trusted List information as notified by Member States, compliant with Commission Decision 2009/767/EC as amended by Commission Decision 2010/425/EU has been published at the location(s) that are announced on

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

Minimálne požiadavky na cezhraničné spracovanie dokumentov elektronicky podpísaných príslušnými orgánmi. ROZHODNUTIE KOMISIE z 25. februára 2011, (2011/130/EÚ)

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:053:0066:0072:EN:PDF>
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:053:0066:0072:SK:PDF>

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

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:053:0066:0072:EN:PDF>
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:053:0066:0072:SK:PDF>

Príloha G História

Verzia:	Dátum vydania:	Poznámka:	Vypracoval:
Verzia 1.0 Č.: 2335/2009/IBEP-001	24.2.2009	Prvé vydanie	Ing. Peter Rybár, NBÚ
Verzia 1.1 Č.: 2968/2010/IBEP/OEP-001	9.4.2010	Doplnené o Rozhodnutie Komisie EÚ	Ing. Peter Rybár, NBÚ
Verzia 1.2 Č.: 2863/2011/IBEP/OEP-001	11.4.2011	Doplnené o Rozhodnutie Komisie 2011/130/EÚ	Ing. Peter Rybár, NBÚ
Verzia 1.3 Č.: 1039/2012/IBEP/OEP-003	10.2.2012	Doplnené o NBÚ dlhodobý archív a pozitívne OCSP	Ing. Peter Rybár, NBÚ