NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

Verzia 1.0

Správa dôveryhodného zoznamu

7.7.2009

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD
Sekcia informačnej bezpečnosti a elektronického podpisu
Budatínska č. 30, 850 07 Bratislava 57
http://www.nbusr.sk/
e-mail: info@nbusr.sk

Obsah

1 Úvod

Overovanie platnosti zaručených elektronických podpisov (ďalej len „ZEP“) sa realizuje nielen v čase platnosti kvalifikovaných certifikátov, ale môže byť potrebné aj v období, kedy už všetkým certifikátom použitým na overenie ZEP vypršala platnosť (ďalej len „exspirovali“) a väčšina poskytovateľov certifikačných služieb už neposkytuje informácie o zrušení týchto certifikátov v CRL alebo OCSP. Aby bolo možné overenie ZEP aj v období, kedy sú všetky relevantné certifikáty už exspirované, je potrebné zabezpečiť dôveryhodné zverejnenie informácií obsahujúcich históriu o exspirovaných dôveryhodných certifikátoch a rovnako históriu schválených podpisových politík, ktorá je overiteľná aktuálne dôveryhodným certifikátom. Zverejňovanie takýchto informácií sa realizuje pomocou dôveryhodného zoznamu obsahujúceho aktuálne a aj historické údaje.

Pri overovaní ZEP sa musia kontrolovať aj atribúty a vlastnosti, ktoré pri bežných elektronických podpisoch [1, 6] nie sú požadované, ale pri ZEP sú nevyhnutné. Aby sa zabezpečila požadovaná úroveň dôvery v ZEP, je potrebné overiť napríklad, či v čase vyhotovenia podpisu boli použité algoritmy z množiny povolených bezpečných algoritmov a ich parametrov pre vytváranie a overovanie [4, 5, 9, 11] ZEP. Aby sa proces podpísania a overenia platnosti ZEP mohol realizovať automaticky, s čo najmenšími interakciami medzi podpisovateľom a overovateľom , aj v prípade dlhodobého overovania ZEP, je potrebné definovať automatické postupy a údajové štruktúry, ktoré takéto overenie umožnia.

2 Predmet dokumentu

Štandard „Správa dôveryhodného zoznamu“ je vydaný na základe § 4 ods. 6 vyhlášky Národného bezpečnostného úradu (ďalej len úrad) 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).

Štandard definuje pravidlá pre dôveryhodné zverejňovanie zoznamov rozličných typov elektronických dokumentov.

Formou podpísaného dôveryhodného zoznamu (ďalej len DZ) odkazov na schválené PP a dôveryhodné certifikáty sa zverejňuje, na základe § 4 ods. 6 vyhlášky NBÚ č. 135/2009 Z. z., na internetovej stránke úradu *Zoznam schválených PP*, čo umožňuje využitie automatického overenia aktuálnych a historických informácií o platnosti schválených podpisových politík (ďalej len PP) a dôveryhodných certifikátov.

Štandard definuje formát, obsah atribútov a spôsob použitia takéhoto DZ, správu, spôsob zverejňovania, ukončenie platnosti, predĺženie platnosti, predčasné zrušenie a pridávanie nových schválených PP a dôveryhodných certifikátov. Štandard zároveň ruší a nahrádza dokument *Správa podpisových politík*, ktorého posledná verzia pod č. 1891/2006/IBEP-006 bola publikovaná v máji 2006.

Na zverejnenie dôveryhodných zoznamov iných typov elektronických dokumentov než sú podpisové politiky a certifikáty sa použijú požiadavky tohto štandardu primerane.

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 3852	Cryptographic Message Syntax	July 2004
[7] RFC 3161	Time-Stamp Protocol (TSP)	August 2001
[8] RFC 2560	X.509 PKI Online Certificate Status Protocol	June 1999

[9] NBÚ Formáty zaručených elektronických podpisov

[10] EN 14890 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] ETSI TS 102 231 V3.1.1 Provision of harmonized Trust-service status information

[13] Vyhláška NBÚ 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)

[14] Vyhláška NBÚ č. 136/2009 Z. z. o spôsobe a postupe používania elektronického podpisu v obchodnom styku a administratívnom styku

4 Skratky

ASCII	American Standard Code for Information Interchange
ASN.1	Abstract Syntax Notation 1
CA	Certification Authority
CAdES	CMS Advanced Electronic Signature
CMS	Cryptographic Message Syntax
CRL	Certificate Revocation List
DER	Distinguished Encoding Rules (for ASN.1)
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PP	Podpisová politika
QC	Qualified Certificate
QES	Qualified Electronic Signature
SHA-1	Secure Hash Algorithm 1
SSCD	Secure-Signature-Creation Device
URL	Uniform Resource Locator
XAdES	XML Advanced Electronic Signature
XML	Extensible Markup Language
ZEP	Zaručený elektronický podpis
DZ	Dôveryhodný zoznam

5 Správa a životný cyklus DZ

Podľa zákona č. 215/2002 Z. z. o elektronickom podpise a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, § 10 ods. 2 písm. d) úrad zverejňuje vlastný verejný kľúč a na základe § 4 vyhlášky NBÚ č. 135/2009 Z. z. úrad zverejňuje schválené PP.

Tieto údaje úrad zverejňuje na svojej internetovej stránke aj vo forme DZ. DZ úrad pravidelne aktualizuje, ak niektorý z použitých komponentov v DZ alebo na overenie DZ zmenil svoj stav [3] (napríklad platnosť), alebo ak boli schválené nové PP, alebo vydané nové dôveryhodné certifikáty.

Certifikát, ktorým bol podpísaný DZ, nebude okamžite zrušený, ostane platný aj po čase zverejnenia nového DZ, aby aplikácie overujúce platnosť podpisu starého DZ mohli pokračovať v overovaní bez hrozby celoplošného znefunkčnenia overovania a potreby manuálneho nastavenia nového DZ. Ak aplikácia pre ZEP zistí, že daný údaj sa nenachádza v aktuálnom DZ aplikácie, upozorní na potrebu nastaviť nový DZ v aplikácii aktualizáciou zo stránky úradu.

Certifikát, ktorým bol podpísaný DZ, môže byť v situácii, ktorá by mohla spôsobiť vážne poškodenie dôveryhodnosti ZEP, zrušený aj bez toho, že by došlo k zmene komponentov použitých v DZ alebo na overenie DZ.

5.1 Pridávanie odkazov na schválené PP a dôveryhodné certifikáty

Úrad po schválení PP na vyhotovenie a overovanie ZEP zverejní schválenú PP na stránke úradu. Rovnako pri vydaní nového dôveryhodného certifikátu podľa § 10 ods. 2 písm. d) zákona č. 215/2002 Z. z. zverejní tento certifikát na stránke úradu. Po zverejnení úrad zaradí tieto údaje do DZ, ktorý bude podpísaný certifikátom určeným na podpisovanie DZ.

Schválená PP je platná v čase uvedenom v podpisovej politike (platnosť od - do), ak uvedená schválená PP nebola predčasne zrušená. Rovnako dôveryhodný certifikát je platný podľa údajov uvedených v dôveryhodnom certifikáte (platnosť od - do), ak uvedený dôveryhodný certifikát nebol predčasne zrušený.

Informácie o tom sú publikované na stránke úradu a zaznamenané aj v DZ, ktorý rovnako zverejňuje a podpisuje úrad.

5.2 Predlžovanie platnosti schválenej PP

Podpisová politika, vzhľadom na starnutie algoritmov, nesmie byť vydaná na neobmedzené obdobie. Platnosť schválenej podpisovej politiky sa automaticky pred ukončením predlžuje vydaním novej podpisovej politiky so zmenenými údajmi dátumu vydania PP, začiatku platnosti, konca platnosti PP a OID identifikátorom PP (a haš hodnoty pri DER PP [2]), ak neboli zistené také nedostatky v schválenej PP, ktoré už nie sú akceptovateľné pre ďalšie obdobie platnosti.

Po predĺžení platnosti schválenej PP úradom, bude schválená PP zverejnená postupom podľa kapitoly 5.1.

5.3 Zrušenie PP a dôveryhodného certifikátu

Schválené PP ruší úrad na návrh žiadateľa, ktorý žiadal o schválenie PP.

Úrad môže zrušiť schválenú PP na návrh inej fyzickej či právnickej osoby alebo aj v prípade, ak sa po jej schválení vyskytnú okolnosti, pre ktoré by uvedená PP nebola schválená.

V prípade zrušenia schválenej PP, bude táto PP uvedená na stránke úradu ako zrušená. Keďže bola súčasťou DZ, tak bude jej platnosť v DZ skrátená do času jej zrušenia.

Ak úrad predčasne zruší dôveryhodný certifikát, informáciu o tejto udalosti zverejní na stránke úradu. V prípade zrušenia platnosti dôveryhodného certifikátu bude jeho platnosť v DZ skrátená do času jeho zrušenia.

Po zrušení schválenej PP alebo dôveryhodného certifikátu bude vydaný nový DZ obsahujúci odkaz na zrušenú PP alebo zrušený dôveryhodný certifikát s časom skrátenia platnosti, ktorý bude podpísaný novým certifikátom určeným na podpisovanie DZ. Certifikát, určený na podpisovanie starého DZ, môže byť v situácii, ktorá by mohla spôsobiť vážne poškodenie dôveryhodnosti ZEP, zrušený pred časom zrušenia PP alebo pred časom zrušenia dôveryhodného certifikátu.

5.4 Dôveryhodné zverejňovanie DZ

Súbory schválených PP a dôveryhodných certifikátov sú zverejňované na stránke úradu a slúžia na vytvorenie DZ. DZ musí byť podpísaný integritným podpisom oprávneného a povereného pracovníka úradu, ktorému pre tento účel bude vydaný certifikát overovaný iba aktuálne dôveryhodným certifikátom „Koreňovej CA“ úradu s certifikačnou politikou povinne aj s OID hodnotou 1.3.158.36061701.0.0.1.10.5.0.1. Táto certifikačná politika definuje okrem požiadaviek pre vydávanie a správu kvalifikovaného certifikátu OID 1.3.158.36061701.0.0.0.1.2.2 aj požiadavku pre jeho rušenie v kritických situáciách, v prípade predčasného zrušenia platnosti schválenej PP alebo dôveryhodného certifikátu. Tento OID je jedinečný a nesmie sa uvádzať v iných typoch certifikátov. Úrad na svojej stránke zverejní DZ vo formáte interného integritného podpisu [9], ale bez časovej pečiatky, aby sa podpis overoval k aktuálnemu času a tak sa zabezpečilo správne overenie v prípade zrušenia niektorej schválenej PP alebo dôveryhodného certifikátu.

Poznámka 1:

Vloženie časovej pečiatky by mohlo spôsobiť overovanie k času časovej pečiatky, čo by mohlo viesť k použitiu už neplatnej schválenej PP alebo neplatného dôveryhodného certifikátu.

Poznámka 2:

Pre potreby archivácie obsahu podpísaného textového súboru v DZ sa text iba dopĺňa o nové informácie, alebo sa údaje upresňujú, napríklad sa použije bezpečnejší hash algoritmus, pričom sa staré záznamy nevymažú, čím sa zabezpečí, že aktuálne platným certifikátom na overenie DZ je možné overiť aj platnosť dávno exspirovaných údajov o schválených PP a dôveryhodných certifikátov na stránke úradu v automatickom režime.

6 Formát DZ a postupy pri jeho vytváraní a overovaní

Štruktúra súboru DZ je zhodná so štruktúrou integritného podpisu definovanou v dokumente [9] "http://www.nbusr.sk/sk/elektronicky-podpis/schvalene-formaty/index.html Formáty zaručených elektronických podpisov".

Príklad položiek podpísaného TXT dokumentu v UTF8 kódovaní z DZ:

FILE=http://www.nbusr.sk/archive/**20081231230000ZSignaturePolicy.der**
HASH(SHA1:1 3 14 3 2 26)=47599765A2FB493557750039788E6714AE0BFDC3
NOTICE=**20091231230000Z** NotAfter, OID=1.3.158.36061701.0.0.1.10.4.0.10, FieldOfApplication= Signature policy for QES.
FILE=http://www.nbusr.sk/archive/**20040114163833ZTrustedCertificate.cer**
HASH(SHA1:1 3 14 3 2 26)=A6D7D70982CB73BE7FA69470029E7EF9360EEA68
NOTICE=**20060114155622Z** NotAfter
FILE=http://www.nbusr.sk/archive/**20050222161337ZTrustedCertificate.cer**
HASH(SHA1:1 3 14 3 2 26)=4EA3F1135F43A4D521973DAA1FBEB3CDF2DCF75A
NOTICE=**20150222154357Z** NotAfter, ExplicitPolicy=**1.3.158.36061701.0.0.0.1.2.2**

Obsah položiek zoznamu:

- FILE musí obsahovať názov súboru a môže obsahovať aj URL typu HTTP na tento súbor. Meno súboru sa musí skladať z troch častí: prvá časť musí obsahovať dátum a čas začiatku platnosti údajov vo formáte GeneralizedTime 99991231235959Z, druhá časť obsahuje pomenovanie obsahu súboru, kde pri schválenej PP zverejnenej na stránke úradu musí obsahovať „signaturePolicy“ a pri dôveryhodnom certifikáte zverejnenom na stránke úradu musí obsahovať „trustedCertificate“ a tretia časť obsahuje typ súboru „.DER“ pri schválnej PP a „.CER“ pri dôveryhodnom certifikáte, pričom pred tretiu časť je možné pridať rozlišujúce číslo v prípade zhodných názvov súborov,
- HASH musí obsahovať odtlačok súboru uvedeného v položke FILE, teda schválenej PP alebo dôveryhodného certifikátu,
- NOTICE musí obsahovať dátum a čas ukončenia platnosti objektu z predchádzajúcej položky FILE (vo formáte GeneralizedTime), ktorý je medzerou oddelený od reťazca "NotAfter ", za ktorým nasledujú ďalšie nepovinné parametre. Jednotlivé parametre sa oddeľujú čiarkou „,“ a priraďuje sa im hodnota znakom „=“.

Zoznam parametrov:

  - "OID" identifikátor objektu, u PP je to OID schválenej PP.
  - "ExplicitPolicy" zoznam OID identifikátorov explicitných certifikačných politík, ktoré sú požadované pri zostavení certifikačnej cesty po dôveryhodný certifikát uvedený v predchádzajúcej položke FILE. Zoznam OID certifikačných politík je vo formáte „1.2.3.4“ a oddelené sú znakom „|”.
  - "FieldOfApplication" text zo schválenej PP z položky FieldOfApplication alebo popis použitia. Tento parameter je posledný v riadku a preto môže obsahovať ľubovoľné znaky okrem znakov: znak 0x13 a znak 0x10 (CRLF).

Dátum ukončenia platnosti podpisovej politiky alebo dôveryhodného certifikátu, uvedený v položke NOTICE, musí byť pri predčasne nezrušenej schválenej PP alebo dôveryhodného certifikátu zhodný s dátumom *notAfter* uvedeným v súbore z predchádzajúcej položky FILE.

V prípade predčasného zrušenia niektorej schválenej PP alebo dôveryhodného certifikátu musí položka NOTICE obsahovať dátum a čas predčasného zrušenia schválenej PP alebo dôveryhodného certifikátu a nie dátum *notAfter* uvedený v súbore z predchádzajúcej položky FILE.

DZ sa musí overovať k aktuálnemu času a musí vždy obsahovať všetky schválené PP a dôveryhodné certifikáty, teda aj tie, ktoré exspirovali, alebo boli predčasne zrušené a dátum ich zrušenia sa musí nachádzať v položke NOTICE a v položke HASH sa musí nachádzať hodnota vypočítaná aktuálne bezpečným algoritmom v súlade s platnou legislatívou. Tento obsah DZ je veľmi dôležitý z dôvodu možnosti overenia zaručeného elektronického podpisu vytvoreného v minulosti pomocou v tom čase platnej schválenej PP a cesty vytvorenej ku vtedy platnému dôveryhodnému certifikátu (ten je v čase overovania už nahradený novým dôveryhodným certifikátom v aplikáciách pre overenie).

Pri overovaní DZ k aktuálnemu času sa overovacia aplikácia snaží získať aktuálne CRL [3] (OCSP [8]) slúžiace na overenie platnosti certifikátu podpisovateľa DZ. Údaje uvedené v DZ sa môžu prehlásiť za platné len do času thisUpdate z aktuálneho CRL (OCSP) na overenie platnosti certifikátu podpisovateľa DZ, ktorý bol overený ako platný.

Teda úplné overenie platnosti zaručených elektronických podpisov musí byť iba k času staršiemu alebo rovnakému ako je thisUpdate z aktuálneho CRL (OCSP), ktorým bola overená platnosť podpisovateľovho certifikátu DZ. Podrobnejší popis položiek PP a proces kontroly jednotlivých položiek pri overovaní ZEP, v aplikáciách pre ZEP, je uvedený v dokumente "Podpisové politiky pre ZEP" na stránke http://www.nbusr.sk/sk/elektronicky-podpis/podpisove-politiky/index.html.

Na základe požiadaviek EU komisie bude DZ od roku 2010 vydávaný aj podľa TS 102 231 od V3.1.1.

7 Platnosť zaručeného elektronického podpisu dokumentu

Platnosť zaručeného elektronického podpisu dokumentu sa určuje vždy k času podpisu dokumentu, ktorý určuje časová pečiatka podpisu (ak bola použitá). Platnosť časových pečiatok sa určuje k času, kedy sú tieto pečiatky vydané a teda sa musí nájsť aj PP platná v tomto čase.

Certifikačné cesty pre kontrolu certifikátu podpisovateľa a certifikátov certifikačnej cesty musia končiť na dôveryhodnom certifikáte ,uvedenom v DZ, ktorý bol platný v danom dátume a čase. Certifikačné cesty časových pečiatok musia končiť na dôveryhodnom certifikáte uvedenom v DZ, ktorý bol platný v čase vytvorenia kontrolovanej časovej pečiatky.

Čas kontroly elektronického podpisu dokumentu je buď:

1) Čas z časovej pečiatky elektronického podpisu dokumentu.

2) Pri časovej pečiatke je to čas po čase uvedenom v časovej pečiatke, ktorý je blízky aktuálnemu času overovania a ktorý je pred časom thisUpdate z posledne vydaného CRL (OCSP) na overenie certifikátu časovej pečiatky.

Ak podpis neobsahuje časovú pečiatku podpisu:

3) Čas z bezpečného auditného záznamu obsahujúceho hash elektronického podpisu.

4) Čas blízky aktuálnemu času overovania, ktorý je pred časom thisUpdate z posledne vydaného CRL (OCSP) na overenie certifikátu podpisovateľa dokumentu. Všetky certifikáty celej certifikačnej cesty musia byť platné do tohto času uvedeného v thisUpdate na overenie platnosti certifikátu podpisovateľa, pričom je potrebné získať aj CRL (OCSP) na overenie celej certifikačnej cesty až po dôveryhodný certifikát, kde každé CRL (OCSP) smerom od CRL (OCSP) na overenie certifikátu podpisovateľa dokumentu je vydané v rovnakom alebo neskoršom čase ako predchádzajúce CRL (OCSP).

Ak je k času kontroly platná aj použitá schválená PP a sú splnené aj iné legislatívne požiadavky na platnosť zaručeného elektronického podpisu, tak je možné prehlásiť zaručený elektronický podpis dokumentu za platný. Rovnako pri kontrole časovej pečiatky musí byť k času z kontrolovanej časovej pečiatky použitá v tom čase platná schválená PP.

Príloha A (informatívna) Príklady schválených PP a dôveryhodných certifikátov v DZ

A.1 Príklad podpísaného TXT súboru v DZ

FILE=http://ep.nbusr.sk/kca/certs/kca/20040114163833ZtrustedCertificate.cer
HASH(SHA1:1 3 14 3 2 26)= A6D7D70982CB73BE7FA69470029E7EF9360EEA68
NOTICE= 20060114155622Z NotAfter, ExplicitPolicy=1.3.158.36061701.0.0.0.1.2.2
FILE=http://ep.nbusr.sk/kca/certs/kca/20 050222161337ZtrustedCertificate.cer
HASH(SHA1:1 3 14 3 2 26)= 4EA3F1135F43A4D521973DAA1FBEB3CDF2DCF75A
NOTICE= 20150222154357Z NotAfter, ExplicitPolicy=1.3.158.36061701.0.0.0.1.2.2
FILE=http://www.nbusr.sk/ipublisher/20050221165146ZsignaturePolicy.der
HASH(SHA1:1 3 14 3 2 26)=751B1B1B03A503727E34FC2A6F9779F5EB9B2595
NOTICE= 20150221165146Z NotAfter, OID=1.1.2, FieldOfApplication=(ES-C) Podpisová p.
FILE= http://www.nbusr.sk/ipublisher/20150221165146ZsignaturePolicy.der
HASH(SHA1:1 3 14 3 2 26)=C50A7053039A4BB5D5329C3F47263E7D5F07DDED
NOTICE=20150221165146Z NotAfter, OID=1.1.3, FieldOfApplication=(ES-T) Podpisová p.
FILE=http://www.nbusr.sk/ipublisher/20050102172151ZsignaturePolicy.der
HASH(SHA1:1 3 14 3 2 26)=31CC3582F4423DB1D2023D5379B38F28E1B8753B
NOTICE=20050102172151Z NotAfter, OID=1.1.4, FieldOfApplication=(ES-UTF8) Podpisová p.
FILE=http://www.nbusr.sk/ipublisher/**20050221165146Z**signaturePolicy1.der
HASH(SHA1:1 3 14 3 2 26)=6528E51733D55648F43B4472227498C13995EB8F
NOTICE=**20150221165146Z** NotAfter, OID=1.1.5, FieldOfApplication=(ES) Podpisová politika

A.2 Príklady zrušenia schválenej PP s OID 1.1.5 v DZ

FILE=http://ep.nbusr.sk/kca/certs/kca/20040114163833ZtrustedCertificate.cer
HASH(SHA1:1 3 14 3 2 26)= A6D7D70982CB73BE7FA69470029E7EF9360EEA68
NOTICE= 20060114155622Z NotAfter, ExplicitPolicy=1.3.158.36061701.0.0.0.1.2.2
FILE=http://ep.nbusr.sk/kca/certs/kca/20050222161337ZtrustedCertificate.cer
HASH(SHA1:1 3 14 3 2 26)= 4EA3F1135F43A4D521973DAA1FBEB3CDF2DCF75A
NOTICE= 20150222154357Z NotAfter, ExplicitPolicy=1.3.158.36061701.0.0.0.1.2.2
FILE=http://www.nbusr.sk/ipublisher/20050221165146ZsignaturePolicy.der
HASH(SHA1:1 3 14 3 2 26)=751B1B1B03A503727E34FC2A6F9779F5EB9B2595
NOTICE= 20150221165146Z NotAfter, OID=1.1.2, FieldOfApplication=(ES-C) Podpisová p.
FILE= http://www.nbusr.sk/ipublisher/20050221165146ZsignaturePolicy.der
HASH(SHA1:1 3 14 3 2 26)=C50A7053039A4BB5D5329C3F47263E7D5F07DDED
NOTICE=20150221165146Z NotAfter, OID=1.1.3, FieldOfApplication=(ES-T) Podpisová p.
FILE=http://www.nbusr.sk/ipublisher/20040102172151ZsignaturePolicy.der
HASH(SHA1:1 3 14 3 2 26)=31CC3582F4423DB1D2023D5379B38F28E1B8753B
NOTICE=20050102172151Z NotAfter, OID=1.1.4, FieldOfApplication=(ES-UTF8) Podpisová p.
FILE=http://www.nbusr.sk/ipublisher/**20050221165146Z**signaturePolicy1.der
HASH(SHA1:1 3 14 3 2 26)=6528E51733D55648F43B4472227498C13995EB8F
NOTICE=**20080221165146Z** NotAfter, OID=1.1.5, FieldOfApplication=(ES) Podpisová politika

Príloha B (informatívna) Revízie vykonané od predošlého vydania

B.1 Pridané požiadavky

Pridané položky, ktoré významne zmenili význam predchádzajúcich požiadaviek:

Neboli.

B.2 Upravené požiadavky

Položky, ktoré upravujú predchádzajúce požiadavky:

Neboli.

B.3 Vysvetlenia

Položky, ktoré boli zmenené pre vysvetlenie predchádzajúcich požiadaviek:

Neboli.

B.4 Publikačné zmeny

Zmeny, ktoré neovplyvňujú technický význam dokumentu:

Neboli.

Príloha C (informatívna) Zoznam použitej literatúry

Základné dokumenty legislatívy Slovenskej republiky pre elektronický podpis
http://www.nbusr.sk/sk/elektronicky-podpis/legislativa/index.html
Formáty zaručených elektronických podpisov
http://www.nbusr.sk/sk/elektronicky-podpis/schvalene-formaty/index.html
Zostavenie certifikačnej cesty a overenie platnosti certifikátov
http://www.nbusr.sk/sk/elektronicky-podpis/overovanie/index.html

- IETF RFC 4158 "Internet X.509 Public Key Infrastructure: Certification Path Building"

Poznámka: Available at http://www.rfc-archive.org/getrfc.php?rfc=4158

- IETF RFC 5217 "Multi-Domain PKI Interoperability" July 2008

Poznámka: Available at http://www.rfc-archive.org/getrfc.php?rfc=5217

- IETF RFC 4853 (2007): "Cryptographic Message Syntax (CMS) Multiple Signer Clarification"
- IETF RFC 3447 (2003): "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1"
- ISO/IEC 8825-1:1998, Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)
- ISO/IEC 19794-2:2005, Biometrics — Biometric Data Interchange Formats — Part 2: Finger Minutiae
- IETF RFC 3279 (2002): "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile"
- IETF RFC 4055 (2005): "Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile"
- IETF RFC 3281 (2002): "An Internet Attribute Certificate profile for Authorization"
- IETF RFC 3370 (2002): "Cryptographic Message Syntax (CMS) Algorithms"
- ETSI TR 102 038: "TC Security - Electronic Signatures and Infrastructures (ESI); XML format for signature policies"
- ETSI TS 101 861: "Time stamping profile"
- EN 14890-2:2008: "Application Interface for smart cards used as Secure Signature Creation Devices - Part 2: Additional Services"
- ETSI TS 101 456: "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates"
- ETSI TS 102 042: "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates"
- CWA 14167-1: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements"
- CWA 14167-2: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2: Cryptographic module for CSP Signing Operations with Backup - Protection Profile"
- CWA 14167-3: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 3: Cryptographic module for CSP key generation services - Protection profile (CMCKG-PP)"
- CWA 14167-4: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 4: Cryptographic module for CSP signing operations - Protection profile - CMCSO PP"
- W3C Recommendation (10 June 2008): "XML Signature Syntax and Processing (Second Edition)"

Poznámka: Available at http://www.w3.org/TR/xmldsig-core/

- W3C Recommendation (10 December 2002): "XML Encryption Syntax and Processing"

Poznámka: Available at http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/

- CWA 14169: "Secure Signature-Creation Devices "EAL 4+"
- IETF RFC 4949 "Internet Security Glossary, Version 2" August 2007

Poznámka: Available at http://www.rfc-archive.org/getrfc.php?rfc=4949

- NIST X.509 path validation test suite

Poznámka: Available at http://csrc.nist.gov/pki/testing/x509paths.html
http://csrc.nist.gov/pki/testing/pathdiscovery.html

- Object Identifier (OID) Repository: ITU-T X.660 & X.670 Recommendation series (or ISO/IEC 9834 series of International Standards)

Poznámka: Available at http://www.oid-info.com/

- FESA – Forum of European Supervisory Authorities,

Poznámka: Available at http://www.fesa.rtr.at

- OID tree structure,

Poznámka: Available at http://www.darmstadt.gmd.de/secude/Doc/htm/oidgraph.htm

- Common ISIS-MTT Specification for interoperable PKI applications. Version 1.1. 16 March 2004
- Internet Draft "X.509 Public Key Infrastructure: Additional Algorithms and Identifiers for DSA and ECDSA"

Poznámka: Available at http://tools.ietf.org/html/draft-ietf-pkix-sha2-dsa-ecdsa-05

- Internet Draft "X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) "

Poznámka: Available at http://tools.ietf.org/html/draft-ietf-pkix-rfc3161bis-01

- TeleTrusT Deutschland e. V., "OID-Liste",

Poznámka: Available at http://www.teletrust.de/index.php?id=171

European Commission http://ec.europa.eu/

- Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures

Poznámka: Available at
http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31999L0093&model=guichett

- IDABC stands for Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens. - eSignature Agenda & Presentations

Poznámka: Available at http://ec.europa.eu/idabc/en/document/7312

- European Network and Information Security Agency (ENISA)

Poznámka: Available at http://www.enisa.europa.eu/

- PKIX Status Pages http://tools.ietf.org/wg/pkix/

Príloha D História

Verzia:	Dátum vydania:	Poznámka:	Vypracoval:
Verzia 1.0 Č.: 6644/2008/IBEP-001	7.7.2009	Prvé vydanie	Ing. Peter Rybár, NBÚ