



NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

Verzia 1.1

**SIM mobilného zariadenia na elektronické
podpisovanie cez bezpečné WEB/WAP alebo
PKCS#11 rozhranie**

10. apríl 2009

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: info@nbusr.sk

Obsah

1	Úvod	4
2	Predmet dokumentu	4
3	Odkazy	5
4	Skratky.....	5
5	Predpoklady realizácie	6
6	Komponenty a ich použitie.....	6
6.1	Šifrovací súkromný kľúč.....	6
6.2	Podpisový súkromný kľúč	6
6.3	Formát zašifrovaných údajov odosielaných na SIM kartu.....	6
Tabuľka 1.	Typ šifrovaných údajov v SMS TEData v ASN.1	7
6.4	DigiID používateľa	8
Tabuľka 2.	CMS AdES podpis v ASN.1 - DigiID	9
Tabuľka 3.	Úplné SignedData v ASN.1	9
7	Podpisovanie a overovanie podpisov	10
Príloha A (informatívna) Príklady údajov pre podpisovanie v SIM		11
A.1	Textový súbor dôveryhodných certifikátov podpísaný v DigiID.p7m súbore.....	11
A.2	DigiID.p7m súbor zakódovaný v BASE64.....	11
A.3	DigiID.p7m súbor zobrazený v ASN.1 dump.....	12
Príloha B (informatívna) Zoznam použitej literatúry		21
Príloha C História		23

1 Úvod

Komunikácia aplikácií s bezpečnými zariadeniami na vyhotovovanie zaručeného elektronického podpisu SSCD v prostrediach, ktoré nie sú bezpečné, vyžaduje používanie bezpečného kanála, na ktorého vytvorenie je potrebná značná výmena údajov pre počiatočnú výmenu kľúčov a autentifikáciu zariadenia a podpisovej aplikácie. Pri použití mobilného zariadenia, ktorého SIM karta obsahuje súkromné kľúče pre potreby elektronického podpisu, je vytvorenie bezpečného kanála na základe postupov z EN 14890 prakticky nerealizovateľné vzhľadom na malý objem údajov, ktoré je možné prenášať prostredníctvom SMS správy a počtu vymenených SMS správ na zostavenie bezpečného kanála cez Secure Messaging.

2 Predmet dokumentu

Účelom tohto štandardu je vytvorenie profilu pre rozhrania PKCS#11, WEB/WAP a nadefinovanie minimálnych potrebných požiadaviek na typy vymieňaných údajov medzi rozhraním PKCS#11, WEB/WAP a SIM aplikáciou, ktoré je možné použiť pri vyhotovovaní (zaručených) elektronických podpisov. Predpokladaný model pozostáva zo štandardnej klientskej alebo web podpisovej aplikácie komunikujúcej cez rozhranie PKCS#11 a mobilného zariadenia so SIM kartou, ktoré prijíma a odosielá údaje na komunikačné rozhrania prepojené s PKCS#11, hlavne prostredníctvom SMS. Dokument definuje protokol, ktorý nahradza Secure Messaging definovaný v EN 14890, aby sa umožnilo použitie mobilného zariadenia so SIM kartou ako zariadenia umožňujúceho bezpečné podpisovanie po potvrdení požiadavky o podpísanie prístupovým kódom a zadaním podpisového PIN pre zrealizovanie samotného podpisu.

Funkcionalita PKCS#11 rozhrania môže byť zahrnutá v serveroch dostupných cez bezpečné WEB/WAP rozhrania, ktoré zabezpečujú dôveryhodné služby napríklad štátnym alebo komerčným organizáciám. Príkladom môžu byť banky ponúkajúce elektronické platby za rôzne tovary a služby alebo verejné portály pre občanov.

Tento štandard je vydaný na základe § 10 ods. 1 písm. j) zákona č. 215/2002 Z. z. o elektronickom podpise.

3 Odkazy

Odkazy na dokumenty, ktoré definujú použité typy a postupy.

- [1] ETSI TS 101 733: " Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)".
- [2] ETSI TR 102 272: "Electronic Signatures and Infrastructures (ESI); ASN.1 format for signature policies".
- [3] RFC 5280 (2008) "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".
- [4] RFC 3739 (2004): "Qualified Certificates Profile".
- [5] ETSI TS 101 862: "Qualified Certificate Profile".
- [6] RFC 3852 (2004): "Cryptographic Message Syntax (CMS)".
- [7] IETF RFC 3161 (2001): "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)".
- [8] RFC 2560 (1999): "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".
- [9] NSA Qualified Electronic Signature Formats
- [10] EN 14890-1:2008: "Application Interface for smart cards used as Secure Signature Creation Devices - Part 1: Basic services".
- [11] RFC 2044 (1996): UTF-8, a transformation format of Unicode and ISO 10646
- [12] ITU-T RECOMMENDATION X.509 (08/2005) | ISO/IEC 9594-8:2005 "Public-key and attribute certificate frameworks".

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)
OID	Object Identifier
QC	Qualified Certificate
SHA-1	Secure Hash Algorithm 1
SMS	Short Message Service
SMS-C	Short Message Service Centre
SMS gateway	based on SS7 connectivity to route SMS (international termination model)
SS7	Signaling System #7
SSCD	Secure-Signature-Creation Device
URL	Uniform Resource Locator
ZEP	Zaručený elektronický podpis

5 Predpoklady realizácie

Základným predpokladom realizácie podpisovania pomocou SIM aplikácie je vydanie dvoch certifikátov na verejné kľúče, ktorých súkromné kľúče sú generované a uložené iba v SIM karte, z ktorej ich nie je možné vyexportovať. Prvý certifikát je pre podpisový kľúč (RSA/EC-(G)DSA) a druhý certifikát je vydaný pre šifrovací (RSA max 1024bit). Certifikát pre šifrovací kľúč slúži na zašifrovanie požiadavky na podpísanie, odoslanej podpisovou aplikáciou cez SMS na SIM kartu. Zašifrovaná požiadavka obsahuje hash z údajov, ktoré sa majú podpísat' a pomocné dva údaje: hash z certifikátu podpisovateľa a prístupový kód, ktorý pozná len podpisovateľ po tom ako mu ho zobrazí podpisová aplikácia pred zašifrovaním odosielanej SMS požiadavky na podpis. SIM aplikácia prijatú SMS odšifruje, čím získava prístupový kód a následne zobrazí podpisovateľovi žiadosť o zadanie prístupového kódu. Ak podpisovateľ zadá nesprávny prístupový kód, podpisovanie sa odmietne, čím sa zabezpečí ochrana pred podpisom falošnej požiadavky. SIM aplikácia musí tiež na požiadanie pre nedôverčivých užívateľov umožniť zobraziť hash hodnotu z údajov, ktoré sa majú podpísat', aby sa podpisovateľ mohol uistíť, že nedošlo ku podvrhnutiu falošných údajov pre podpísanie. Pre bežných používateľov bude postačovať zadanie prístupového kódu, ktorý pre podpisovateľa vygenerovala a zobrazila podpisová aplikácia.

6 Komponenty a ich použitie

6.1 Šifrovací súkromný kľúč

Šifrovací súkromný kľúč je pod kontrolou SIM aplikácie a SIM aplikácia si pomocou neho odšifruje prijatú SMS požiadavku obsahujúcu hash z údajov na podpísanie, prístupový kód a hash z podpisovateľovho certifikátu. Šifrovací kľúč je plne pod kontrolou podpisovej SIM aplikácie, čo znamená že nik iný okrem podpisovej SIM aplikácie ho nemôže použiť a preto nevyžaduje zadanie PIN. Súkromný šifrovací kľúč nesmie byť exportovateľný a slúži len na odšifrovanie žiadostí na podpis. SIM aplikácia, ktorá používa šifrovací kľúč, nesmie umožniť externé spracovanie odšifrovaných údajov prístupového kódu mimo SIM kartu, aby sa zabránilo útoku s podhodenými falošnými údajmi s rovnakým prístupovým kódom. SIM aplikácia umožní použitie iba takých odšifrovaných údajov, ktoré obsahovali správny prístupový kód, teda ktorý bol zhodný so zadaným prístupovým kódom na mobilnom zariadení po výzve podpisovateľom.

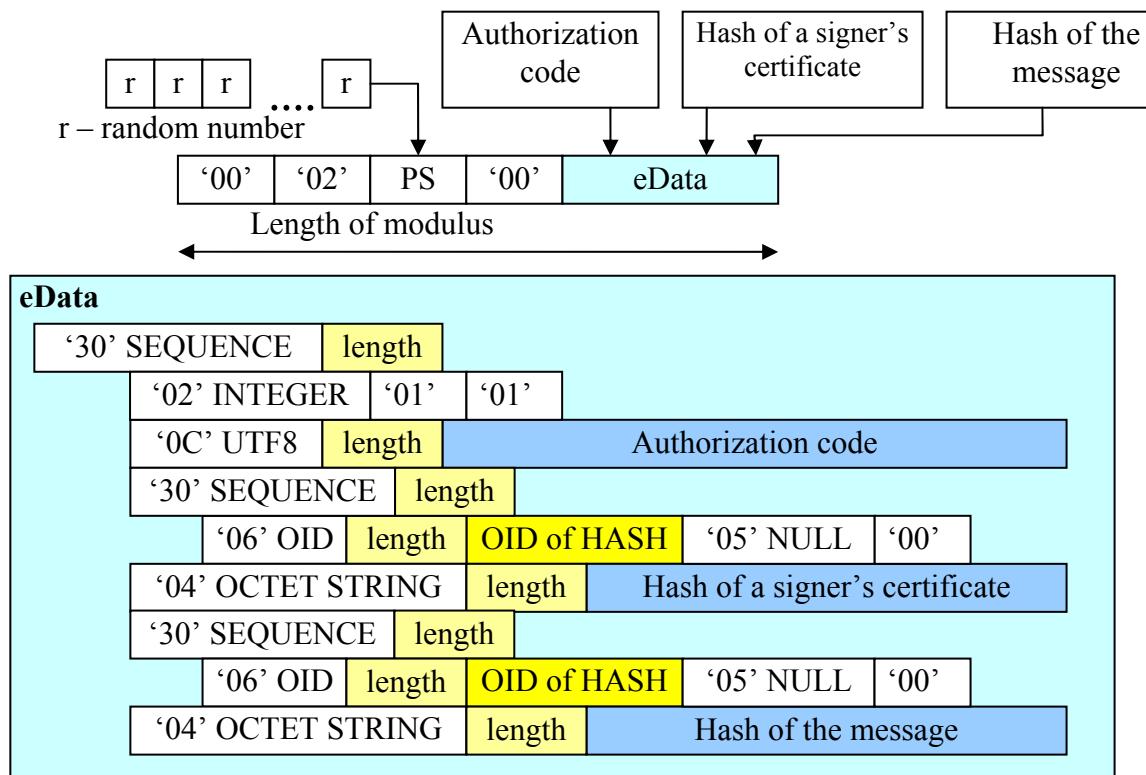
6.2 Podpisový súkromný kľúč

Podpisový kľúč je možné použiť na podpísanie hash hodnoty z údajov na podpis iba po zadaní správneho prístupového kódu a po zadaní podpisového PIN pre kľúč identifikovaný na základe identifikácie cez hash z certifikátu podpisovateľa. Podpisový kľúč musí byť uložený na SIM karte a karta nesmie umožniť jeho exportovanie, aby nedošlo k jeho použitiu mimo SIM kartu. Podpisový PIN sa nesmie použiť na iné účely než je podpisovanie so súkromným podpisovým kľúčom, aby nedošlo k zneužitiu podpisového kľúča inou operáciou pracujúcou s inými údajmi alebo kľúčmi na SIM karte. Kvôli veľkosti odpovede sa odporúča použiť ECDSA (EC-GDSA) namiesto RSA, aby digitálny podpis bolo možné odoslať v jednej SMS.

6.3 Formát zašifrovaných údajov odosielaných na SIM kartu

SMS obsahuje zašifrované najmä 3 položky: prístupový kód pre overenie oprávnenia prístupu k údajom z odšifrovanej SMS, hash certifikátu podpisovateľa, pomocou ktorého SIM aplikácia nájde podpisový súkromný kľúč a hash údajov, ktorý sa má podpísat'. SIM aplikácia po odšifrovaní údajov z SMS požiada o zadanie prístupového kódu a pokračuje v podpisovaní, len ak zadaný prístupový kód podpisovateľom je zhodný s prístupovým kódom z odšifrovanej SMS, ktorý bol vygenerovaný/zadaný a zobrazený podpisovou aplikáciou podpisovateľovi pred odoslaním požiadavky na podpísanie cez SMS. Následne pre zrealizovanie podpisu SIM aplikácia požiada mobilné zariadenie o zobrazenie výzvy na zadanie podpisového PIN a ak zadaný PIN bol správny, zrealizuje podpísanie hash hodnoty z údajov na podpis, ktoré prijala v SMS a odošle podpis v novej

SMS naspäť na zariadenie pripojené k podpisovej aplikácii napríklad cez rozhranie PKCS#11. Formát údajov z prijatej SMS, ktoré sú zašifrované pomocou napríklad RSA s veľkosťou kľúča 1024, je uvedený na nasledujúcom obrázku. Vzhľadom na krátku dobu počas ktorej sú údaje zašifrované, pre potreby šifrovania SMS, postačuje kľúč RSA o veľkosti 1024 bit.



Zašifrované údaje eData typu TEData, ktoré sú definované ako správa M vo formátovaní podľa RFC 3447 PKCS #1, verzia 2.1, kapitola 7.2.1 "EME-PKCS1- v1_5".

Formátovanie podľa RFC 3447 PKCS #1: '00 02' || PS || '00' || M, kde PS je postupnosť oktetov pozostávajúcich z pseudonáhodne generovanej postupnosti oktetov neobsahujúcich nulu. Postupnosť oktetov musí pozostávať z n oktetov, kde n je veľkosť modulu súkromného kľúča určeného na odšifrovanie.

Predpokladom pre bezpečnú komunikáciu je, že len podpisovateľ pred podpisovaním pozná prístupový kód „Authorization code“ a hash správy „Hash of the message“ a útočník nevie podvrhnúť oba údaje.

Tabuľka 1. Typ šifrovaných údajov v SMS TEData v ASN.1

	ASN.1	Info
1.	TEData ::= SEQUENCE {	
2.	version INTEGER,	Aktuálna verzia 1 (1)
3.	authorizationCode UTF8String,	Prístupový kód zobrazený len pre podpisovateľa.
4.	signingCertDigestAlgorithmIdentifier,	OID hash algoritmu pre hash z certifikátu podpisovateľa
5.	signingCertDigest Digest	hash z certifikátu podpisovateľa
6.	messageDigestAlgorithmIdentifier,	OID hash algoritmu pre hash podpisovaných údajov v SIM
7.	messageDigest Digest	hash podpisovaných údajov v SIM
8.	utf8String UTF8String (SIZE (1..MAX))	

9.	AlgorithmIdentifier ::= SEQUENCE { algorithm OBJECT IDENTIFIER, parameters ANY DEFINED BY algorithm OPTIONAL }	Napríklad OID pre SHA-1 (1 3 14 3 2 26) a parameter NULL
10.	Digest ::= OCTET STRING	

6.4 DigiID používateľa

Používateľ SIM aplikácie pre podpisovanie získa dva certifikáty, ktoré mu vydala certifikačná autorita patriaca pod dôveryhodný koreňový certifikát. Z toho vyplýva, že používateľ dôveruje koreňovému certifikátu a samozrejme svojim dvom certifikátom, ktoré umožňujú jeho digitálnu identifikáciu. Aby používateľ SIM podpisovej aplikácie neboli neustále vyrušovaný nastavovaním certifikátov, ktorým dôveruje a konfigurovaním podpisových a overovacích aplikácií, sú pre neho vydané a uložené certifikáty v takom formáte a s takými údajmi, ktoré umožňujú automatickú činnosť aplikácií s minimálnymi požiadavkami na používateľa.

Šifrovací certifikát vlastníka SIM aplikácie obsahuje v položke „subject“ telefónne číslo pre odosielanie SMS na SIM kartu a podpisový certifikát môže obsahovať email adresu, aby bolo možné podpisovať a overovať aj elektronickú poštu. Formát telefónneho čísla definuje ITU-T E.123 a je taktiež uvedený v RFC 3966 a v dokumente „Formáty kvalifikovaných certifikátov“ v tabuľke 5 na riadku 27 <http://www.nbusr.sk/sk/elektronicky-podpis/schvalene-formaty/index.html>

Pred ukončením regisračného procesu, kedy sa vydajú vlastníkovi SIM karty oba certifikáty, je vlastník SIM karty vyzvaný na vyhotovenie prvého elektronického podpisu, ktorý umožní overenie úspešnosti regisračného procesu a zároveň vytvorí používateľovi jeho súbor DigiID dôvery v jeho certifikáty a tak mu umožní vyskúšať si funkčnosť jeho SIM podpisovej aplikácie. Vlastník SIM karty zrealizuje integritný podpis definovaný v dokumente „Formáty zaručených elektronických podpisov“ v prílohe D <http://www.nbusr.sk/sk/elektronicky-podpis/schvalene-formaty/index.html>, kde sa do textového súboru zaznamenajú hash hodnoty z podpisového, šifrovacieho a koreňového certifikátu. Textový súbor sa podpiše interným typom podpisu a uloží do podpisu typu CMS AdES do súboru „DigiID.p7m“, ktorý bude obsahovať minimálne tieto 3 certifikáty v položke podpisu *certificates*.

Pre celkovú funkčnosť rozhrania PKCS#11, prostredníctvom ktorého podpisová aplikácia žiada podpisovanie a overovanie elektronických podpisov a komunikuje so SIM aplikáciou, je nevyhnutné použiť údaje uložené v používateľom podpísanom súbore „DigiID.p7m“.

Podpisová aplikácia vyčíta cez rozhranie PKCS#11, ktoré je nakonfigurované pomocou súboru „DigiID.p7m“, nasledovné údaje:

- Podpisový certifikát (Podpisový certifikát sa použije pri overovaní podpisov a v niektorých aplikáciách aj na prihlásenie sa používateľa, kedy sa dôveruje len údajom, ktoré si sám používateľ podpísal s jeho podpisovým certifikátom, teda zoznamu certifikátov, ktorých odkazy vo forme hash hodnôt sú v podpísanom súbore v „DigiID.p7m“).
- Podpisový algoritmus a veľkosť klíča (Podpisový algoritmus a veľkosť klíča sa použije používateľom pri podpisovaní a tieto údaje sa získajú z certifikátu podpisu „DigiID.p7m“.)
- Hash algoritmus a jeho parametre (Hash algoritmus a jeho parametre, ktoré sa použijú podpisovateľom pri podpisovaní a tieto údaje sa získajú z podpisu „DigiID.p7m“.)
- Zoznam dôveryhodných certifikátov (Zoznam dôveryhodných certifikátov, ktorým podpisovateľ dôveruje a ktoré je možné použiť pri overovaní podpisov automaticky bez neustáleho potvrdzovania dôvery podpisovateľom.)
- Šifrovací certifikát (Šifrovací certifikát obsahujúci telefónne číslo, na ktoré sa odošle SMS s požiadavkou na podpísanie. Pričom požiadavku odošle priamo rozhranie PKCS#11, ak nie je použitá iná komunikácia so SIM aplikáciou napr. USB/serial kábel, infrared...).

Príklad „DigiID.p7m“ je uvedený v prílohe.

Tabuľka 2. CMS AdES podpis v ASN.1 - DigiID

ASN.1
ContentInfo ::= SEQUENCE { contentType ContentType, -- id-signedData content [0] EXPLICIT ANY DEFINED BY contentType }

Tabuľka 3. Úplné SignedData v ASN.1

ASN.1	Info	Must
1. SignedData ::= SEQUENCE {		
2. version CMSVersion,		
3. digestAlgorithms DigestAlgorithmIdentifiers,		
4. encapContentInfo SEQUENCE {		
5. eContentType ContentType,	id-data RFC 3852	
6. eContent [0] EXPLICIT OCTET STRING OPTIONAL },	Textový súbor v UTF8 kódovanie obsahujúci URL na mená súborov a hash hodnoty týchto súborov dôveryhodných certifikátov.	X
7. certificates [0] IMPLICIT CertificateSet OPTIONAL,	Podpisové, šifrovacie a koreňové certifikáty.	X
8. crls [1] IMPLICIT CertificateRevocationLists OPTIONAL,		
9. signerInfos SET OF		
10. SEQUENCE { -- SignerInfo	Podpis vlastníka SIM karty s jeho podpisovým certifikátom.	X
11. version CMSVersion,		
12. sid SignerIdentifier,		
13. digestAlgorithm DigestAlgorithmIdentifier,		
14. signedAttrs [0] IMPLICIT SET SIZE (1..MAX) OF		
15. SEQUENCE { -- Attribute	Minimálne musí obsahovať atribúty: content-type, message-digest, signingCertificate or signingCertificateV2.	X
16. attrType OBJECT IDENTIFIER,		
17. attrValues SET OF AttributeValue } OPTIONAL,		
18. signatureAlgorithm SignatureAlgorithmIdentifier,		
19. signature OCTET STRING, -- SignatureValue		
20. unsignedAttrs [1] IMPLICIT SET SIZE (1..MAX) OF		
21. SEQUENCE {		
22. attrType OBJECT IDENTIFIER,		
23. attrValues SET OF AttributeValue } OPTIONAL }		

Používateľ podpisovej aplikácie komunikujúcej cez rozhranie PKCS#11 musí mať pred prvým použitím nakonfigurovanú knižnicu PKCS#11, napríklad cez grafické rozhranie dostupné cez menu nad ikonu umiestnenú v sysTray, kde si nastaví umiestnenie súboru „DigiID.p7m“, alebo zadá URL na získanie „DigiID.p7m“. Ak podpisovateľ používa WEB/WAP na vyplnenie formulára a podpísanie, v tom prípade zadá URL na „DigiID.p7m“, alebo tento súbor nahrá na WEB/WAP cez WEB rozhranie. Pre zjednodušenie by mohol operátor, poskytujúci SIM karty obsahujúce podpisový a šifrovací súkromný kľúč s aplikáciou pre podpisovanie, ponúknuť štandardný adresár so súborom „DigiID.p7m“ napríklad v tvare <http://www.operator.com/sk/telefonicislo/DigiID.p7m>, čo by zjednodušilo podpisovanie.

7 Podpisovanie a overovanie podpisov

Prvým krokom pred prvým podpisovaním alebo overovaním podpisov je nastavenie cesty na súbor „DigiID.p7m“ vo WEB/WAP rozhraní alebo PKCS#11 knižnici. Potom rozhranie môže načítať všetky potrebné informácie zo súboru „DigiID.p7m“ automaticky (ako je popísané v odseku 6.4), bez potreby požadovania odpovedí na otázky od používateľa, napríklad na výber užívateľského podpisového certifikátu. Ďalej používateľ pracuje s podpisovou aplikáciou rovnako, ako keby bola k počítaču pripojená čipová karta alebo USB token. Pred požiadavkou na podpísanie je používateľovi v rozhraní PKCS#11 vygenerovaný a zobrazený prístupový kód, alebo si ho používateľ zadá ako atribút CKA_LABEL a aplikácia ho vloží do rozhrania PKCS#11 pred zašifrovaním a odoslaním SMS požiadavky o podpísanie. Po prijatí SMS na mobilné zariadenie podpisovateľa je SMS automaticky odšifrovaná a podpisovateľ je vyzvaný na zadanie rovnakého prístupového kódu aký mu bol zobrazený v podpisovej aplikácii. SIM aplikácia prevedie operáciu podpisania len v prípade, ak odšifrovaný z SMS a zadaný prístupový kód na mobilnom zariadení bude rovnaký. Pokročilejší používatelia si môžu nechať zobraziť aj hash hodnotu podpisovaných údajov, no pre bežného používateľa bude táto možnosť dostupná len po jej vyžiadanej tlačidlom v dialógu požadujúcim zadanie prístupového kódu.

Potom podpisovateľ zadá podpisový PIN a mobilné zariadenie podpíše a odošle podpísaný hash naspäť v SMS na rozhranie PKCS#11 alebo WEB. Aplikácie WEB servera alebo PKCS#11 knižnice prekontrolujú podpísaný hash podpisovateľovým certifikátom a poskytne ho podpisovej aplikácii, ktorá vytvorí výsledný elektronický podpis, do ktorého vloží podpisovateľov certifikát a podpísaný dokument.

Pri overovaní podpisov si aplikácia na overovanie podpisov vyčíta cez rozhranie PKCS#11 zoznam certifikátov uložených v „DigiID.p7m“ a požiada o potvrdenie prihlásenia sa výberom podpisového certifikátu, ktorým je podpísaný „DigiID.p7m“. Pritom môžeme očakávať, že podpisovateľ si rozpozná svoj vlastný podpisový certifikát a bude schopný potvrdiť, že certifikát, ktorý bol zobrazený aplikáciou, patrí jemu. Aplikácia po tomto potvrdení môže dôverovať všetkému, čo bolo overené týmto certifikátom. Po potvrdení a overení podpisu súboru „DigiID.p7m“, aplikácia vyčíta zoznam dôveryhodných certifikátov, ktoré už používateľ nepotrebuje ďalej overovať, lebo podpisovateľ im svojim podpisom potvrdil dôveru, čo ušetrí používateľa od náročného a často pre používateľov ťažko pochopiteľného postupu nastavovania dôvery v rôzne certifikáty. Podpisovateľ súboru „DigiID.p7m“ a používateľ overovacej aplikácie je tá istá osoba a teda si sám sebe svojmu podpisu dôveruje.

Po prihlásení sa používateľa, do overovacej aplikácie, podľa postupu popísaného v predchádzajúcim odseku, môžu v aplikácii nasledovať procesy s overovaním rôznych podpisov, ktorých podpisové certifikáty vydali certifikačné autority patriace pod rovnaké dôveryhodné koreňové autority, ktorým dôveruje prihlásený podpisovateľ.

Príloha A (informatívna) Príklady údajov pre podpisovanie v SIM

A.1 Textový súbor dôveryhodných certifikátov podpísaný v DigiID.p7m súbore

Správa pozostáva z jednoduchej postupnosti atribútov FILE, HASH a NOTICE. FILE a HASH sú povinné atribúty, NOTICE je voliteľný atribút. Postupnosť vždy musí začínať s atribútom FILE. Jeden riadok musí obsahovať len jeden atribút. Všetky riadky obsahujú iba ASCII znaky. Jednotlivé riadky sú oddelené s CRLF. Správa je uložená v položke *encapContentInfo* v *SignedData*. Predchádzajúce pravidlá definujú integrálny typ podpisu.

Podpísaná správa pre vytvorenie DigiID, podpísaná v integrálnom podpise (*.p7m), obsahuje informácie o súboroch obsahujúcich dôveryhodné certifikáty.

CRLF character (13) + character (10)

FILE = < [URL] file name >CRLF

HASH (< algorithm >: < OID of algorithm >) = < file hash – capital letters >CRLF

NOTICE = < note, e. g. a name or type of certificate... >CRLF

Príklad:

```
FILE=http://www.operator.com/sk/tel00421123123123/sign.cer
HASH (SHA1:1 3 14 3 2 26)=E0FC2B90315FC4C62E85A76B00B8F5FBAF6CC334
NOTICE=Signature
FILE=http://www.operator.com/sk/tel00421123123123/crypt.cer
HASH (SHA1:1 3 14 3 2 26)=541E1CF31EFBCB2A650E7AED94A1E5C73DBB8D3B6
NOTICE=Encryption
FILE=http://www.operator.com/sk/tel00421123123123/mobileCA.cer
HASH (SHA1:1 3 14 3 2 26)=23DE8E7554544B8841914A9F7DE79FE59FA236A1
NOTICE=Root CA
```

A.2 DigiID.p7m súbor zakódovaný v BASE64

```
MIME-Version: 1.0
Content-Type: application/octet-stream; name="DigiID.p7m"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="DigiID.p7m"
```

```
MII0lgYJKoZIhvCNQcCoII0hzCCDoMCAQExCzAJBgUrDgMCGGUAMIIBTAYJKoZIhvCNQcBoIIB
PQSCAT1GSUxFPUU6XHNpZ24uY2VyDQpIQVNIFNQTE6MSAzIDE0IDMgMiAyNik9RTBGQzJCOTAz
MTVGQzRDNjJFCDVBNzZCMDCOEVY1RkJBRjZDQzMzNA0Ktk9USUNFPVnpZ25hdHVyZQ0KRk1MRT1F
OlxjcnlwdC5jZXINCKhBU0goU0hBMToxIDMgmtQgMyAyIDI2KT01NDFFMUNGmzFFRkNCMkE2NTBF
N0FFRdk0QTFFNUM3M0RCQjhEM0I2DQpOT1RJQ0U9RW5jcnlwdG1vbg0KRk1MRT1F01xtb2JpbGVD
QS5jZXINCKhBU0goU0hBMToxIDMgmtQgMyAyIDI2KT0yM0RFOEU3NTU0NTQ0Qjg4NDE5MTRBOUY3
REU3OUZFNT1GQTIzNkExDQpOT1RJQ0U9Um9vdCBDQQ0KoIIILMTCCA5kwggKBoAMCAQICCGxd5a2
EvhpMA0GCSqGSIb3DQEBBQUAMEwxzAJBgNVBAYTA1NLMRMwEQYDVQQHEwpCcmF0aXNsYXZhMRQw
...
ggHmAeBMFgwTDELMAkGA1UEBhMCU0sxEzARBgNVBAcTCkJyYXRpc2xhdmExFDASBgnVBAoTC0V4
YW1wbGUgT3JnMRIwEAYDVQQDEw1Nb2JpbGUgQ0ECCGxda5a2EvhpMAkGBSsoAwIaBQCggekwGAYJ
KoZIhvCNQkDMQsGCSqGSIb3DQEhATAcBpkqhkIG9w0BCQUxDxcNMdgwNDayMTQ0MDAyWjAjBqkq
hkiG9w0BCQQxFgQUq779FuD6G6BxwTm8z0g5RB3R0aIwgYkGCyqGSiB3DQEJEAIMMXoweDB2MHQE
FDuTPbOAIYg9r74oMcB9ecuvQH4fMFwwUKROMEwxzAJBgNVBAYTA1NLMRMwEQYDVQQHEwpCcmF0
aXNsYXZhMRQwEgYDVQQKEwtFeGFtcGx1IE9yZzESMBAGA1UEAxMjTW9iaWx1IENBAghsXWuWthL4
aTANBgkqhkiG9w0BAQEFAASBhgCnjf36UcgejzW5ugSvXnRDVbJTlsmDr9OS1yy5gPqk5UK5MAH
cPLc/tjuNcIWsvtaZUq0OMaJPcnWa0nq42d18TAnppqKB8m2eLr2Ye7zfJHaeEo11E3ILNcxy1
mtUTEdbVgR/Y72ZTf8jdvpX1EpJ/BdZFu0CfsNMpHjpJ
```

A.3 DigID.p7m súbor zobrazený v ASN.1 dump

```
SEQUENCE {
    OBJECT IDENTIFIER signedData (1 2 840 113549 1 7 2)
    [0] {
        SEQUENCE {
            INTEGER 1
            SET {
                SEQUENCE {
                    OBJECT IDENTIFIER sha1 (1 3 14 3 2 26)
                    NULL
                }
            }
        SEQUENCE {
            OBJECT IDENTIFIER data (1 2 840 113549 1 7 1)
            [0] {
                OCTET STRING
                'FILE=http://www.operator.com/sk/tel00421123123123/sign.cer'
                'HASH(SHA1:1 3 14 3 2 26)=E0FC2B90315FC4C62E85A76B00B8F5FBAF6CC334'
                'NOTICE=Signature'
                'FILE=http://www.operator.com/sk/tel00421123123123/crypt.cer'
                'HASH(SHA1:1 3 14 3 2 26)=541E1CF31EFCB2A650E7AED94A1E5C73DBB8D3B6'
                'NOTICE=Encryption'
                'FILE=http://www.operator.com/sk/tel00421123123123/mobileCA.cer'
                'HASH(SHA1:1 3 14 3 2 26)=23DE8E7554544B8841914A9F7DE79FE59FA236A1'
                'NOTICE=Root CA'
            }
        }
    [0] {
        SEQUENCE {
            SEQUENCE {
                [0] {
                    INTEGER 2
                }
                INTEGER 6C 5D 6B 96 B6 12 F8 69
            SEQUENCE {
                OBJECT IDENTIFIER
                . . . sha1withRSAEncryption (1 2 840 113549 1 1 5)
                NULL
            }
            SEQUENCE {
                SET {
                    SEQUENCE {
                        OBJECT IDENTIFIER countryName (2 5 4 6)
                        PrintableString 'SK'
                    }
                }
                SET {
                    SEQUENCE {
                        OBJECT IDENTIFIER localityName (2 5 4 7)
                        PrintableString 'Bratislava'
                    }
                }
                SET {
                    SEQUENCE {
                        OBJECT IDENTIFIER organizationName (2 5 4 10)
                        PrintableString 'Example Org'
                    }
                }
                SET {
                    SEQUENCE {
                        OBJECT IDENTIFIER commonName (2 5 4 3)
                        PrintableString 'Mobile CA'
                    }
                }
                SEQUENCE {
                    UTCTime 31/03/2008 13:08:58 GMT
                    UTCTime 29/03/2018 13:08:58 GMT
                }
                SEQUENCE {
                    SET {
                        SEQUENCE {
                            OBJECT IDENTIFIER countryName (2 5 4 6)
                            PrintableString 'SK'
                        }
                    }
                    SET {

```

```
..... SEQUENCE {
.....   OBJECT IDENTIFIER commonName (2 5 4 3)
.....     PrintableString 'Peter Rybar'
.....   }
..... }
SET {
  SEQUENCE {
    OBJECT IDENTIFIER telephoneNumber (2 5 4 20)
    PrintableString '+421 123 123123'
  }
}
SEQUENCE {
  SEQUENCE {
    OBJECT IDENTIFIER
    . rsaEncryption (1 2 840 113549 1 1 1)
    NULL
  }
  BIT STRING, encapsulates {
    SEQUENCE {
      INTEGER
      . 00 AF 46 BA A8 35 EF C5 F1 05 32 DA BF F6 16 AC
      . 85 A6 14 A1 A1 BB 57 5D B6 5E BF 4F 67 0E 07 88
      . 05 5A 09 CF 3A B3 2F C2 45 5A 5E 7E C5 DC A0 13
      . E6 31 33 7E 9E 0D BE BB 6B 03 C2 E6 36 7D BB 36
      . D4 47 48 9A 11 8C 3C 64 AC 86 AC 53 C3 51 DA 7F
      . 54 EA 2E E7 7E 36 32 6F 13 37 4A 96 A1 9B 13 08
      . 01 2C 77 B4 BB FD 0C 44 6C 7A EC 54 CB D8 56 E6
      . 73 C8 EE 00 78 54 0B 86 34 5B 8D FB 8E B4 7A 05
      ED
      INTEGER 65537
    }
  }
}
[3] {
  SEQUENCE {
    SEQUENCE {
      OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
      OCTET STRING, encapsulates {
        OCTET STRING
        . 92 C5 7A F9 F3 67 DD BF EE 00 98 8B 97 5C C6 DA
        . 36 C8 55 56
      }
    }
    SEQUENCE {
      OBJECT IDENTIFIER keyUsage (2 5 29 15)
      BOOLEAN TRUE
      OCTET STRING, encapsulates {
        BIT STRING 1 unused bit
        . '00000011'B
        Error: Spurious zero bits in bitstring.
      }
    }
    SEQUENCE {
      OBJECT IDENTIFIER subjectAltName (2 5 29 17)
      OCTET STRING, encapsulates {
        SEQUENCE {
          [1] 'pr@mailbox.sk'
        }
      }
    }
    SEQUENCE {
      OBJECT IDENTIFIER basicConstraints (2 5 29 19)
      BOOLEAN TRUE
      OCTET STRING, encapsulates {
        SEQUENCE {}
      }
    }
    SEQUENCE {
      OBJECT IDENTIFIER
      . authorityKeyIdentifier (2 5 29 35)
      OCTET STRING, encapsulates {
        SEQUENCE {
          [0]
          . 01 35 AE 07 FF DE 68 E3 6C F5 8F CB 69 0B 61 61
          . D1 1C B2 70
        }
      }
    }
  }
}
```

```

SEQUENCE {
    OBJECT IDENTIFIER
    . cRLDistributionPoints (2 5 29 31)
    OCTET STRING, encapsulates {
        SEQUENCE {
            SEQUENCE {
                [0] {
                    [0] {
                        [6] 'http://ca.example.sk/crls/ca20080330.crl'
                    }
                }
            }
        }
    }
    SEQUENCE {
        OBJECT IDENTIFIER
        . authorityInfoAuthorization (1 3 6 1 5 5 7 1 1)
        OCTET STRING, encapsulates {
            SEQUENCE {
                SEQUENCE {
                    OBJECT IDENTIFIER
                    . caIssuers (1 3 6 1 5 5 7 48 2)
                    [6] 'http://ca.example.sk/crls/ca20080330.p7c'
                }
            }
        }
        SEQUENCE {
            OBJECT IDENTIFIER certificatePolicies (2 5 29 32)
            OCTET STRING, encapsulates {
                SEQUENCE {
                    SEQUENCE {
                        OBJECT IDENTIFIER anyPolicy (2 5 29 32 0)
                    }
                }
            }
        }
    }
    SEQUENCE {
        OBJECT IDENTIFIER
        . shalwithRSAEncryption (1 2 840 113549 1 1 5)
        NULL
    }
    BIT STRING
        AF 3E 93 E6 A1 83 79 46 3E DE 8D B3 E0 0E 44 37
        45 AA 17 B3 6D 10 83 66 D7 F8 F3 56 C3 30 92 67
        BA 0C 50 4D 54 47 3C 9B D9 79 A0 E7 3F 93 89 71
        37 77 07 ED 1D E1 E5 9B 58 BE FB E4 8A 03 5A 2B
        0A F3 AB 92 B8 17 D6 74 10 FC C2 51 61 D5 EC 71
        ED 06 44 1D A0 92 87 16 76 B5 CE 2A 2D B0 A6 97
        A1 8B 55 1D B1 67 E7 5F CF 6D D0 04 4E 6A 8F 25
        03 5B 13 FA 3F 29 79 E4 4B 46 A8 00 D6 99 80 E3
        AA 98 A9 23 2F 1F 91 6B 1F 82 9C 74 D9 3D 31 9E
        C3 D4 7A E3 26 5B ED F9 F6 03 F1 3E 75 03 6E BB
        90 F2 DC 0F 5C 51 18 90 88 5A AA 8B 17 7B 38 F7
        05 57 29 1B 16 09 19 61 8A 52 1C F9 38 9A 1A 42
        0C 84 B7 69 67 6F 89 0F BE 72 AE 81 DB 35 DF 46
        B8 42 3E E1 5B DD 47 D4 C6 44 83 F2 C9 1A E5 DE
        D2 E9 BF 86 BE CE 01 BA 65 B8 3D 9A 9A 03 23 46
        90 B4 0B C6 A1 DC E0 7A D6 C1 6C 54 5F 2F 83 46
    }
    SEQUENCE {
        SEQUENCE {
            [0] {
                INTEGER 2
            }
            INTEGER 51 AD 7C 91 9B 2F 94 78
            SEQUENCE {
                OBJECT IDENTIFIER
                . shalwithRSAEncryption (1 2 840 113549 1 1 5)
                NULL
            }
            SEQUENCE {
                SET {
                    SEQUENCE {
                        OBJECT IDENTIFIER countryName (2 5 4 6)

```

```

. . . . . PrintableString 'SK'
. . . .
. . . }
. . . SET {
. . . . SEQUENCE {
. . . . . OBJECT IDENTIFIER localityName (2 5 4 7)
. . . . . PrintableString 'Bratislava'
. . . . }
. . . . }
. . . SET {
. . . . SEQUENCE {
. . . . . OBJECT IDENTIFIER organizationName (2 5 4 10)
. . . . . PrintableString 'Example Org'
. . . . }
. . . . }
. . . SET {
. . . . SEQUENCE {
. . . . . OBJECT IDENTIFIER commonName (2 5 4 3)
. . . . . PrintableString 'Mobile CA'
. . . . }
. . . . }
. . . . }
. . . . SEQUENCE {
. . . . . UTCTime 31/03/2008 13:21:22 GMT
. . . . . UTCTime 31/03/2017 13:21:07 GMT
. . . . }
. . . . SEQUENCE {
. . . . . SET {
. . . . . . SEQUENCE {
. . . . . . . OBJECT IDENTIFIER countryName (2 5 4 6)
. . . . . . . PrintableString 'SK'
. . . . . . }
. . . . . }
. . . . . SET {
. . . . . . SEQUENCE {
. . . . . . . OBJECT IDENTIFIER localityName (2 5 4 7)
. . . . . . . PrintableString 'Bratislava'
. . . . . . }
. . . . . }
. . . . . SET {
. . . . . . SEQUENCE {
. . . . . . . OBJECT IDENTIFIER organizationName (2 5 4 10)
. . . . . . . PrintableString 'Example Org'
. . . . . . }
. . . . . }
. . . . . SET {
. . . . . . SEQUENCE {
. . . . . . . OBJECT IDENTIFIER commonName (2 5 4 3)
. . . . . . . PrintableString 'Mobile CA'
. . . . . . }
. . . . . }
. . . . . }
. . . . . SEQUENCE {
. . . . . . SEQUENCE {
. . . . . . . OBJECT IDENTIFIER
. . . . . . . rsaEncryption (1 2 840 113549 1 1 1)
. . . . . . . NULL
. . . . . . }
. . . . . . BIT STRING, encapsulates {
. . . . . . . SEQUENCE {
. . . . . . . . INTEGER
. . . . . . . . 00 C4 09 27 7B F0 E3 DD FB F7 C0 2B B3 B0 AF 43
. . . . . . . . 9F 6E B6 7D 37 7F C5 99 51 E4 E9 AF FF 16 6A F9
. . . . . . . . 11 EF 0D 3C 94 6A AF 3E 17 C3 A5 32 95 A3 7E F4
. . . . . . . . 1C BA A7 2F AE AD 3D 18 92 02 8A 42 A3 9C C4 8A
. . . . . . . . 24 79 16 29 EB 7D BC AF D2 44 EE A5 19 AD 23 98
. . . . . . . . 07 8A D5 31 D7 1A 48 15 68 C2 ED 00 37 DA 5C E2
. . . . . . . . C4 17 24 28 1C E8 14 0B C7 AF BA 57 1C 11 49 77
. . . . . . . . A6 72 66 78 97 AC C3 3B 43 60 45 95 6D 04 74 AA
. . . . . . . . A3 2A 01 3E 2B 4E FA 42 C2 B1 68 83 F4 F0 7F 30
. . . . . . . . 6E 4E 48 C4 92 9A B4 1C 45 98 FE 20 35 3E C0 BD
. . . . . . . . 8D 12 02 1A 82 D5 85 9D FC 5F 6A 0D 6F 20 8D 75
. . . . . . . . DD 44 E0 85 22 69 B8 12 CA E1 C2 BD F5 31 88 98
. . . . . . . . 84 48 3B B1 9B 00 F7 11 A7 19 89 02 C5 14 D4 BF
. . . . . . . . FD 97 20 54 B8 E2 A7 29 DE 12 18 4E 1D 74 30 77
. . . . . . . . 53 C9 DB 8C 58 8E F9 34 8E 43 50 B8 02 5C 0C CA
. . . . . . . . 48 A3 D6 AC E0 94 C1 53 72 37 40 E4 52 96 F3 2C
. . . . . . . . 71
. . . . . . . . INTEGER 65537

```

```
        . . . . .
        . . . . }
        . . . .
        . [3] {
        . . . . SEQUENCE {
        . . . . . SEQUENCE {
        . . . . . . OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
        . . . . . . OCTET STRING, encapsulates {
        . . . . . . . OCTET STRING
        . . . . . . . 01 35 AE 07 FF DE 68 E3 6C F5 8F CB 69 0B 61 61
        . . . . . . . D1 1C B2 70
        . . . . . . }
        . . . . . }
        . . . . . SEQUENCE {
        . . . . . . OBJECT IDENTIFIER certificatePolicies (2 5 29 32)
        . . . . . . OCTET STRING, encapsulates {
        . . . . . . . SEQUENCE {
        . . . . . . . . SEQUENCE {
        . . . . . . . . . OBJECT IDENTIFIER anyPolicy (2 5 29 32 0)
        . . . . . . . . }
        . . . . . . . }
        . . . . . . . }
        . . . . . . }
        . . . . . . SEQUENCE {
        . . . . . . . OBJECT IDENTIFIER keyUsage (2 5 29 15)
        . . . . . . . BOOLEAN TRUE
        . . . . . . OCTET STRING, encapsulates {
        . . . . . . . BIT STRING 1 unused bit
        . . . . . . . '1100000'B
        . . . . . . }
        . . . . . . SEQUENCE {
        . . . . . . . OBJECT IDENTIFIER basicConstraints (2 5 29 19)
        . . . . . . . BOOLEAN TRUE
        . . . . . . OCTET STRING, encapsulates {
        . . . . . . . . SEQUENCE {
        . . . . . . . . . BOOLEAN TRUE
        . . . . . . . . }
        . . . . . . . }
        . . . . . . }
        . . . . . . SEQUENCE {
        . . . . . . . OBJECT IDENTIFIER
        . . . . . . . sha1withRSAEncryption (1 2 840 113549 1 1 5)
        . . . . . . . NULL
        . . . . . . }
        . . . . . . BIT STRING
        . . . . . . . 25 6C 5A BF FB B9 0F BF A6 23 B0 AA 73 AD 47 19
        . . . . . . . D9 4D 19 30 41 05 1C 6B 03 D1 E0 C7 D3 A7 8D F4
        . . . . . . . 30 6B 49 8D D6 09 D0 7D 86 4E 9E 56 40 28 D8 B8
        . . . . . . . A2 1B 88 E5 A7 04 D9 10 30 94 96 16 11 98 11 C1
        . . . . . . . BE DC 9B E0 97 E0 E8 98 DF 77 A1 EA D7 FC BA B2
        . . . . . . . D6 8A 7A FD CB CC A0 A1 AD CE B3 72 98 17 73 3E
        . . . . . . . 45 A9 3B 4C A1 4C 29 76 E7 39 C0 71 5C ED 71 50
        . . . . . . . 9A 38 D1 7A 94 4A 0E FF 16 45 53 69 9B 7E C6 74
        . . . . . . . E9 D3 86 4F 1D B5 69 58 A2 A9 7B 77 30 74 99 44
        . . . . . . . 31 7C F9 1E 6F EC A0 A1 34 5E C9 A3 C5 6D D2 BD
        . . . . . . . 76 F5 57 EE DF 72 71 60 38 F7 DB 8D C9 47 5F 2D
        . . . . . . . 11 58 68 15 B9 97 50 C5 EA 50 89 3D 4C C4 6D A1
        . . . . . . . BF CF A2 02 0F 74 86 E5 CD 6B 8F 27 C5 7B B8 E1
        . . . . . . . F6 08 EE 1A 2D 8E 8A 89 9E B4 25 5E 0B FB 8B 09
        . . . . . . . 2D 0D 8F F3 FE 68 DE 45 FF 1F BF DA D0 AA 45 DD
        . . . . . . . 97 C6 17 E5 26 63 C9 CB 57 F7 6F 84 5F 21 52 F7
        . . . . }
        . . . . SEQUENCE {
        . . . . . SEQUENCE {
        . . . . . . [0] {
        . . . . . . . INTEGER 2
        . . . . . . }
        . . . . . . . INTEGER 6C 5D 6B 96 B6 12 F8 69
        . . . . . . SEQUENCE {
        . . . . . . . . OBJECT IDENTIFIER
        . . . . . . . . sha1withRSAEncryption (1 2 840 113549 1 1 5)
        . . . . . . . . NULL
        . . . . . . }
        . . . . . . SEQUENCE {
        . . . . . . . SET {
```

```

. . . . . SEQUENCE {
. . . . .   OBJECT IDENTIFIER countryName (2 5 4 6)
. . . . .     PrintableString 'SK'
. . . . .
. . . . }
. . . . SET {
. . . .   SEQUENCE {
. . . .     OBJECT IDENTIFIER localityName (2 5 4 7)
. . . .     PrintableString 'Bratislava'
. . . .   }
. . . . }
. . . . SET {
. . . .   SEQUENCE {
. . . .     OBJECT IDENTIFIER organizationName (2 5 4 10)
. . . .     PrintableString 'Example Org'
. . . .   }
. . . . }
. . . . SET {
. . . .   SEQUENCE {
. . . .     OBJECT IDENTIFIER commonName (2 5 4 3)
. . . .     PrintableString 'Mobile CA'
. . . .   }
. . . . }
. . . . SET {
. . . .   SEQUENCE {
. . . .     UTCTime 31/03/2008 13:08:58 GMT
. . . .     UTCTime 29/03/2018 13:08:58 GMT
. . . .   }
. . . . SEQUENCE {
. . . .   SET {
. . . .     SEQUENCE {
. . . .       OBJECT IDENTIFIER countryName (2 5 4 6)
. . . .       PrintableString 'SK'
. . . .     }
. . . .   }
. . . .   SET {
. . . .     SEQUENCE {
. . . .       OBJECT IDENTIFIER commonName (2 5 4 3)
. . . .       PrintableString 'Peter Rybar'
. . . .     }
. . . .   }
. . . .   SET {
. . . .     SEQUENCE {
. . . .       OBJECT IDENTIFIER telephoneNumber (2 5 4 20)
. . . .       PrintableString '+421 123 123123'
. . . .     }
. . . .   }
. . . .   }
. . . . SEQUENCE {
. . . .   SEQUENCE {
. . . .     OBJECT IDENTIFIER
. . . .     rsaEncryption (1 2 840 113549 1 1 1)
. . . .     NULL
. . . .   }
. . . .   BIT STRING, encapsulates {
. . . .     SEQUENCE {
. . . .       INTEGER
. . . .       00 C8 0E BD 53 AD 87 84 B4 40 2F A6 19 F4 09 24
. . . .       8C A0 FE 9E 9B 7A C1 C3 B8 CE 72 86 60 6D 74 5F
. . . .       5D 5B C6 90 F5 C4 EA 77 10 B5 68 7B 9D 8B 93 53
. . . .       86 74 CC 96 B1 1E 0E B8 DA 53 AF 32 09 74 7D FF
. . . .       B7 41 41 E7 97 79 24 2C 95 7F 98 40 5D 63 2A 86
. . . .       E6 B3 EC 76 57 8E D7 1C 51 E8 66 52 9C 0B D9 73
. . . .       55 79 4F 96 C6 14 BC 5C 4E 7A A7 93 5B F4 6A 5A
. . . .       A4 55 C1 DD FB 99 00 22 48 7B 3B 65 2E 21 E9 D5
. . . .       1F 24 FD C7 92 D8 01 33 44 DA 52 49 8A D3 A8 F4
. . . .       F5 6B 7F 90 51 9D 53 58 00 0A 47 1A 54 5B CD 2A
. . . .       B0 73 9E 16 0C 0B E1 2F 8C EE 98 65 D2 3F 70 BF
. . . .       B8 A8 B7 EB FB C7 1A 7B 0C 25 E0 13 8A D1 07 2C
. . . .       9B A1 BC BF 80 EA 09 DE 8B BA BF 3D AD 2C A4 85
. . . .       6E 4D 67 D6 3C 75 59 39 C0 2F 4E EC 80 A6 CA D2
. . . .       BC CA F1 AF C7 A4 84 F9 D7 40 E8 EF 7E EB D0 76
. . . .       49 30 B7 E2 3E F7 DD 13 17 5A 60 5C 54 32 AA 44
. . . .       C3
. . . .       INTEGER 65537
. . . .     }
. . . .   }
. . . . [3] {

```

```
..... SEQUENCE {
.....   SEQUENCE {
.....     OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
.....     OCTET STRING, encapsulates {
.....       OCTET STRING
.....       A9 5C AB 95 BB 82 AA C2 E6 37 59 0B 11 22 02 40
.....       63 A3 6F 92
.....     }
.....   }
.....   SEQUENCE {
.....     OBJECT IDENTIFIER keyUsage (2 5 29 15)
.....     BOOLEAN TRUE
.....     OCTET STRING, encapsulates {
.....       BIT STRING 4 unused bits
.....       '1100'B
.....     }
.....   }
.....   SEQUENCE {
.....     OBJECT IDENTIFIER subjectAltName (2 5 29 17)
.....     OCTET STRING, encapsulates {
.....       SEQUENCE {
.....         [1] 'pr@mailbox.sk'
.....       }
.....     }
.....   }
.....   SEQUENCE {
.....     OBJECT IDENTIFIER basicConstraints (2 5 29 19)
.....     BOOLEAN TRUE
.....     OCTET STRING, encapsulates {
.....       SEQUENCE {}
.....     }
.....   }
.....   SEQUENCE {
.....     OBJECT IDENTIFIER
.....     authorityKeyIdentifier (2 5 29 35)
.....     OCTET STRING, encapsulates {
.....       SEQUENCE {
.....         [0]
.....         01 35 AE 07 FF DE 68 E3 6C F5 8F CB 69 0B 61 61
.....         D1 1C B2 70
.....       }
.....     }
.....   }
.....   SEQUENCE {
.....     OBJECT IDENTIFIER
.....     cRLDistributionPoints (2 5 29 31)
.....     OCTET STRING, encapsulates {
.....       SEQUENCE {
.....         SEQUENCE {
.....           [0] {
.....             [0] {
.....               [6] 'http://ca.example.sk/crls/ca20080330.crl'
.....             }
.....           }
.....         }
.....       }
.....     }
.....   }
.....   SEQUENCE {
.....     OBJECT IDENTIFIER
.....     authorityInfoAuthorization (1 3 6 1 5 5 7 1 1)
.....     OCTET STRING, encapsulates {
.....       SEQUENCE {
.....         SEQUENCE {
.....           OBJECT IDENTIFIER
.....           caIssuers (1 3 6 1 5 5 7 48 2)
.....           [6] 'http://ca.example.sk/crls/ca20080330.p7c'
.....         }
.....       }
.....     }
.....   }
.....   SEQUENCE {
.....     OBJECT IDENTIFIER certificatePolicies (2 5 29 32)
.....     OCTET STRING, encapsulates {
.....       SEQUENCE {
.....         SEQUENCE {
.....           OBJECT IDENTIFIER anyPolicy (2 5 29 32 0)
.....         }
.....       }
.....     }
..... }
```

```

        . . .
        . . .
        . . }
        . . .
        . . . } }
        . . . SEQUENCE {
        . . .   OBJECT IDENTIFIER
        . . .     sha1withRSAEncryption (1 2 840 113549 1 1 5)
        . . .   NULL
        . . . }
        . . . BIT STRING
        . . .   63 51 F3 24 54 2C B9 AD BD 34 2C 37 0E B0 D8 84
        . . .   BD A7 CA 51 61 F8 A9 76 AB 0C 4D 6E 65 FD 77 02
        . . .   BB 79 04 C8 0C 48 48 62 C6 5D 51 0F 5A EE 82 F0
        . . .   1B F4 D2 A6 04 E1 5E 1A DB 11 0E DB CB 90 E4 43
        . . .   98 6E 7E 24 73 05 0B 7A EE D3 3A 51 EF 9E 6A F8
        . . .   F3 90 2C BE BE C1 EB A0 2E 32 7D 83 F6 B6 F4 BD
        . . .   C4 3F 0D F4 F3 DF BF 40 BC 0D 68 71 4A A3 D7 AC
        . . .   5D A8 7C 96 16 4E 8C 74 17 EA 10 8B 77 55 F8 4B
        . . .   A5 73 0A CC B2 AC 39 1F B9 EE 08 DC 1B 66 E3 8E
        . . .   BC 55 8A 32 B8 FE 99 36 83 FF 83 E5 4D FC 2F 8F
        . . .   80 BB 32 58 67 0A 3E 3A C0 0F 26 0D 74 59 82 49
        . . .   32 2F 1E B8 7F 34 A1 E7 A8 12 26 08 40 48 D8 DA
        . . .   7A AE 7A A2 8B 6B CE CE 37 34 D0 20 BD 2A 40 1A
        . . .   0D F7 ED 54 E2 B4 8B A0 AF D6 A2 49 B0 D9 20 0F
        . . .   70 3F 31 C4 85 85 59 A1 CF 5B 6D B5 48 F2 C6 7D
        . . .   8B 7E CA 4B 85 21 15 44 7F 46 55 F2 88 30 AF AC
        . . . }
        . . . }
        . . . SET {
        . . .   SEQUENCE {
        . . .     INTEGER 1
        . . .     SEQUENCE {
        . . .       SEQUENCE {
        . . .         SET {
        . . .           SEQUENCE {
        . . .             OBJECT IDENTIFIER countryName (2 5 4 6)
        . . .             PrintableString 'SK'
        . . .           }
        . . .         }
        . . .       SET {
        . . .         SEQUENCE {
        . . .           OBJECT IDENTIFIER localityName (2 5 4 7)
        . . .           PrintableString 'Bratislava'
        . . .         }
        . . .       }
        . . .     SET {
        . . .       SEQUENCE {
        . . .         OBJECT IDENTIFIER organizationName (2 5 4 10)
        . . .         PrintableString 'Example Org'
        . . .       }
        . . .     }
        . . .   SET {
        . . .     SEQUENCE {
        . . .       OBJECT IDENTIFIER commonName (2 5 4 3)
        . . .       PrintableString 'Mobile CA'
        . . .     }
        . . .   }
        . . .   INTEGER 6C 5D 6B 96 B6 12 F8 69
        . . . }
        . . . SEQUENCE {
        . . .   OBJECT IDENTIFIER sha1 (1 3 14 3 2 26)
        . . .   NULL
        . . . }
        [0] {
        . . .   SEQUENCE {
        . . .     OBJECT IDENTIFIER contentType (1 2 840 113549 1 9 3)
        . . .     SET {
        . . .       OBJECT IDENTIFIER data (1 2 840 113549 1 7 1)
        . . .     }
        . . .   }
        . . .   SEQUENCE {
        . . .     OBJECT IDENTIFIER signingTime (1 2 840 113549 1 9 5)
        . . .     SET {
        . . .       UTCTime 02/04/2008 14:40:02 GMT
        . . .     }
        . . .   }
        . . .   SEQUENCE {

```


Príloha B (informatívna) Zoznam použitej literatúry

Základné dokumenty legislatívy Slovenskej republiky pre elektronický podpis

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

Formáty zaručených elektronických podpisov

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

Vytvorenie a overenie certifikačnej cesty

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

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

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

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

NOTE: 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)"

NOTE: Available at <http://www.w3.org/TR/xmldsig-core/>

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

NOTE: 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

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

- NIST X.509 path validation test suite

NOTE: 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)

NOTE: Available at <http://www.oid-info.com/>

- FESA – Forum of European Supervisory Authorities,

NOTE: Available at <http://www.fesa.rtr.at>

- OID tree structure,

NOTE: 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"

NOTE: 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) "

NOTE: Available at <http://tools.ietf.org/html/draft-ietf-pkix-rfc3161bis-01>

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

NOTE: 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

NOTE: 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

NOTE: Available at <http://ec.europa.eu/idabc/en/document/7312>

- European Network and Information Security Agency (ENISA)

NOTE: Available at <http://www.enisa.europa.eu/>

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

Príloha C História

Verzia:	Dátum vydania:	Poznámka:	Vypracoval:
Verzia 0.1 Č.: -	16.12.2007	Prvé vydanie (draft)	Ing. Peter Rybár, NBÚ
Version 1.0. Č.: 2739/2008/IBEP-003	31.3.2008	Prvé vydanie	Ing. Peter Rybár, NBÚ
Version 1.1. Č.: 584/2009/IBEP-007	10.4.2009	Spresnenie použitia prístupového kódu	Ing. Peter Rybár, NBÚ