Crypto-World

Informační sešit GCUCMP

Ročník 5, číslo 1/2003 **15. leden 2003**

1/2003

Připravil : Mgr.Pavel Vondruška

Sešit je rozesílán registrovaným čtenářům.
Starší sešity jsou dostupné na adresách
http://www.mujweb.cz/veda/gcucmp

(395 e-mail výtisků)

Obsah : **Str.**

Příloha : Crypto_p1.pdf
CEN Workshop Agreements (dokumenty vztahující se k elektronickému podpisu)

(články neprocházejí jazykovou korekturou)

A. České technické normy a svět

Pavel Vondruška, ČESKÝ TELECOM, a.s.

V prvním čtvrtletí tohoto roku se na stránkách Crypto-Worldu setkáte s třídílným seriálem „České technické normy a svět“. Je věnován základním informacím o českých technických normách, jejich členění a tvorbě, způsobu vzniku norem, převzetí cizích norem, jejich akceptaci, přehledu mezinárodních a zahraničních normalizačních institucí. V každém čísle bude k dispozici i obsáhlá příloha, ve které budou přehledy norem vztahujících se k elektronickému podpisu. Seriál vznikl na základě zkušenosti z mých přednášek a vystoupení v loňském roce. V diskusi se často objevovala výtka, že Odbor elektronického podpisu nevydává normy k elektronickému podpisu, nebo - že určitý problém není dostatečně (technicky) řešen v prováděcí vyhlášce k elektronickému podpisu. Zjistil jsem tak, že není veřejnosti dostatečně znám statut a proces vytváření a přejímání českých technických norem. Dalším podnětem byla neodůvodněná kritika převzetí originálu normy ISO 17799 do systému ČSN ISO. Kritici pravděpodobně nevěděli, že je to jedna ze čtyř základních možností převzetí evropské a mezinárodní normy do ČSN. Posledním důvodem je potvrzení toho, že má smysl se zabývat normami k elektronickému podpisu, které připravují iniciativy ETSI a CEN, neboť ty normy, které jsou označeny jako EN (European Standard – Norm) jsou určeny v členských státech k povinnému zavedení jako národní normy a vyžadují současné zrušení národních norem, které jsou s ní v rozporu. Jinými slovy: po vstupu do EU budeme muset tyto normy do systému ČSN zavést. Jedná se např. o normu Electronic Signature Formats (TC Security - Electronic Signatures and Infrastructures - ESI). Právě tuto normu, která je z hlediska kompatibility naprosto zásadní, jsem často citoval a reakcí v diskusi bylo, že u nás takováto norma není a že se nelze na ni odvolávat.

Seriál vznikl na základě údajů, které jsou volně dostupné na stránkách ČSNI (Český normalizační institut) a na základě materiálů, které jsem jako člen technické komise č. 20 (Informační technologie) měl k dispozici.

OBSAH :

3. Mezinárodní vztahy
3.1 Mezinárodní organizace pro normalizaci (ISO)
3.2 Mezinárodní elektrotechnická komise (IEC)
3.3 Evropský výbor pro normalizaci (CEN)
3.4 Evropský výbor pro elektrotechnickou normalizaci (CENELEC)

Příloha č.3 (5 stránek)
Mezinárodní a zahraniční normalizační instituce (přehled a spojení)

1. Právní úprava národní technické normalizace

Právní úprava technické normalizace je stanovena zákonem č. 22/1997 Sb. ze dne 24. ledna 1997 o technických požadavcích na výrobky a o změně a doplnění některých zákonů. Tento zákon nabyl účinnosti dne 1.9.1997 a nahrazuje dřívější zákon č. 142/1991 Sb., o československých technických normách, ve znění zákona č. 632/1992 Sb.

Spolu se zákonem č. 22/1997 Sb. vstoupilo v platnost dvanáct nařízení vlády, které tento zákon doplňují ve stanovení technických požadavků na skupiny výrobků. Devět z dvanácti nařízení vlády má přímou předlohu ve směrnicích Evropské unie. Nařízení vlády určují podrobnosti pro posuzování shody s technickými předpisy a harmonizovanými normami, případně také určují konkrétní způsob pro posuzování shody u vyráběných a dovážených výrobků [1].

1.1 Charakteristika české technické normy

Zákon č. 22/1997 Sb. definuje českou technickou normu jako dokument schválený pověřenou právnickou osobou pro opakované nebo stálé použití vytvořený podle tohoto zákona a označený písmenným označením ČSN, jehož vydání bylo oznámeno ve Věstníku Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví.
Česká technická norma není obecně závazná [2].

1.2 Pojem „harmonizovaná česká technická norma“

Zákon zavádí nový pojem “harmonizované české technické normy", jehož obsah je převzat z práva Evropských společenství. Jde o nové vyjádření úlohy “národních technických norem" při regulaci vlastností výrobků. Jeho podstatou je to, že právní regulace týkající se výrobků se omezí na naléhavé potřeby ochrany života a zdraví osob, majetku, životního prostředí apod. Přitom se vychází z toho, že je účelné stanovovat technické požadavky na výrobky relativně obecně tak, aby jednoznačné konkrétní požadavky právních předpisů nevytvářely bariéry technického rozvoje. Uplatnění tohoto přístupu vypadá v praxi tak, že tam, kde je to možné a účelné, je technický požadavek na výrobek v právním předpisu formulován obecně tak, že je ho možno splnit různými způsoby. K technickým právním předpisům jsou pak v rámci Evropské unie vydávány harmonizované evropské normy. Při jejich splnění se má za to, že výrobek odpovídá příslušným obecným ustanovením technického předpisu. Dodržení takových harmonizovaných evropských norem proto nemůže být povinné. Jde vlastně o nabídku technického řešení, která nemusí být využita. Avšak

případnou odpovědnost za škody vzniklé řešením, které je odchylné od harmonizované normy nese ten, kdo nesplnil požadavky obecně formulovaného technického předpisu.

Obdobný právní význam mají harmonizované ČSN. Výraz harmonizovaná ČSN vyjadřuje především vztah k technickému předpisu, tj. k nařízení vlády vydanému na základě zákona. I když ve většině případů harmonizované ČSN budou z hlediska obsahového přejímat bez jakýchkoliv změn obsah evropských norem, slovo "harmonizace" se bude vztahovat vždy k technickému předpisu, tj. především k nařízení vlády vydanému podle zákona [3].

Informace o nově vyhlášených harmonizovaných evropských normách lze zjistit v Ústředním věstníku Evropských společenství (OJEC – The Official Journal of the European Communities) ve vazbě na určitou směrnici ES a v měsíčníku The Bulletin of the European Standards Organizations CEN/CENELEC/ETSI, ve kterém jsou uveřejňovány informace o evropských normách a dokumentech vydávaných mezinárodními normalizačními organizacemi CEN/CENELEC a ETSI [4].

1.3 Zabezpečení tvorby norem

Zákon stanovuje, že tvorbu a vydávání norem zaručuje stát. Tímto úkolem je pověřena právnická osoba, kterou pověřuje Ministerstvo průmyslu a obchodu. V současné době je tou právnickou osobou Český normalizační institut. Pověření je nepřevoditelné a po dobu, po kterou je toto pověření platné, nesmí být touto činností pověřena jiná právnická osoba. Ministerstvo může pověření zrušit, jestliže právnická osoba neplní podmínky stanovené zákonem nebo jestliže o to sama požádá. Do doby, než je zvolena jiná právnická osoba, zabezpečuje plnění jejích úkolů Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

Náklady na tvorbu norem hradí ten, kdo požaduje jejich zpracování. Náklady na tvorbu norem, především harmonizovaných norem, zpracovaných na základě požadavku ministerstev nebo jiných ústředních správních úřadů a náklady spojené s členstvím v mezinárodních a evropských normalizačních organizacích, hradí stát.

Zákon upravuje také problematiku autorských práv. Dole na titulním listě jakékoliv české normy je uvedeno: „Podle zákona č. 22/1997 Sb. smějí být české technické normy rozmnožovány je se souhlasem Českého normalizačního institutu."

Jestliže někdo neoprávněně označí dokument značkou ČSN nebo neoprávněně rozmnoží či rozšíří normu, může dostat pokutu do výše 1 milionu Kč [2].

[1] POLÁČEK, Dušan. : „Ohlédnutí za rokem 1997 v normalizaci. *Bulletin ČSNI : informační zpravodaj Českého normalizačního institutu – servis pro masmédia"*, 1998, č. 1, s. 4-6.

[2] Zákon č. 22/1997 Sb. o technických požadavcích na výrobky a o změně a doplnění některých zákonů. Datum platnosti 24. ledna 1997. Datum účinnosti 1. září 1997.

[3] Právní význam ČSN podle zákona č. 22/1997 Sb., Český normalizační institut, http://www.csni.cz/wwwcsni/pravo.htm

[4] NOVÁKOVÁ, Ivana : „Harmonizované české technické normy". *Bulletin ČSNI : informační zpravodaj Českého normalizačního institutu – servis pro masmédia*, 1998, č. 4, s. 6-8.

B. Kryptografie a normy
Digitální certifikáty. IETF-PKIX
Část 8. Protokol pro časové značky (Time-stamp Protocol, TSP)

Jaroslav Pinkava, PVT a.s.

1. Úvod

Tento díl je věnován problematice časových značek, konkrétně protokolu, který je popsán v dokumentu RFC.3161 (lit. [1]). Problematika časových značek je dnes již nezbytným aparátem pro práci s elektronicky podepsanými dokumenty. V řadě praktických situací je třeba dosáhnout dohody na metodě, pomocí které je vytvářen spolehlivý a operabilní nástroj dokazování časového momentu ve kterém byla provedena transakce. Při používání aparátu elektronických (digitálních) podpisů je třeba při jejich verifikaci ověřit, že byly vytvořeny v době, kdy certifikát podepisující strany byl platný. To je nezbytné ze dvou důvodů:

1) během platnosti certifikátu podepisující strany mohl být odpovídající soukromý klíč kompromitován a z tohoto důvodu odvolán .
2) zda podpis nebyl vytvořen po ukončení doby platnosti příslušného digitálního certifikátu.

Toto ověření přitom musí proběhnout důvěryhodnou a bezpečnou cestou. Časové značky u podepisovaných dokumentů zajišťují možnost dodatečného ověření, před kterým okamžikem byl daný dokument podepsán (např. že tak bylo učiněno v době platnosti příslušného digitálního certifikátu).
Časová značka k danému dokumentu neformálně vzato vznikne tak, že autorita časových značek (TSA – Time Stamping Authority) digitálně podepíše hash tohoto dokumentu (což je např. 20 bajtů pro algoritmus SHA-1) spolu s připojeným pořadovým číslem a aktuálním časovým údajem.
Časová značka T může prokázat:

a. **aktuálnost** (T byla vytvořena po časovém okamžiku t_1)
b. **existenci** (T byla vytvořena před časem t_2)
c. **pořadí** (časová značka T byla vytvořena dříve než časová značka S)

Materiál TS 101 861 (lit.[4]) pracovní skupiny ETSI je bezprostředně navazujícím dokumentem k RFC 3161 a přidává určitá doporučení k protokolu pro časové značky.

2. Protokol pro časové značky

Službou časových značek se zabývá tedy speciální třetí důvěryhodná strana – autorita časových značek (TSA). Tato autorita vlastně vytváří důkaz existence dokumentu v určitém časovém momentu. V RFC.3161 jsou stanoveny např. následující požadavky, které musí naplňovat příslušná (TSA):

1. Používat důvěryhodný zdroj času.
2. Zahrnout důvěryhodnou hodnotu času do každé časové značky.
3. Zahrnout jednoznačné celé číslo do každé nově generované časové značky.

4. Vygenerovat časovou značku po obdržení platného požadavku od žadatele, pokud to je možné.
5. Zahrnout do každé časové značky identifikátor, který jednoznačně identifikuje bezpečnostní politiku při využití které byly časová značka generována.
6. Časovou značku vytvářet pouze přes hashovou reprezentaci data, tj. časová známka je asociována s jednocestnou vůči kolizím rezistentní hashovací funkcí definovanou svým OID.
7. Ověřit OID jednocestné vůči kolizím rezistentní hashovací funkce a ověřit, že délka hashe odpovídá příslušnému hashovacímu algoritmu.
8. Žádným způsobem neověřovat otisk, který má být časově označkován (výjimkou je jeho délka dle minulého bodu).
9. Do časové značky nesmí být zahrnuta žádná identifikace žádající entity.
10. Pro podpis každé časové značky použít klíč, který byl vygenerován pouze pro tyto účely a má tuto vlastnost klíče vyznačenu na příslušném certifikátu.
11. Pokud je o toto žádána žadatelem, který využívá rozšíření (extension field) zahrne do časové značky i další informace. Tyto rozšíření musí být podporována autoritou časových značek. Pokud toto nelze, musí autorita odpovědět chybovou hláškou.

Příslušný IETF protokol specifikuje příslušné formáty - požadavku i odpovědi. Přitom pro přenos časových značek lze využívat většinu existujících přenosových protokolů. RFC 3161 obsahuje i příslušná ASN.

První zprávu protokolu zasílá žádající entita jako požadavek na vytvoření časové značky, tento požadavek je zaslán TSA. Druhou zprávou je pak odpověď TSA žádající entitě. Po obdržení této odpovědi zjistí žádající entita chybový statut odpovědi, pokud chyba nevznikla, ověří jednotlivá pole zprávy a platnost digitálního podpisu. Mj. také ověří zda obdržená časová značka se skutečně váže k zaslanému požadavku. Například je také důležité přijmout příslušná opatření, tak aby bylo možné detekovat tzv. replay attack (znovuzaslání dřívější zprávy), zjistit statut certifikátu TSA, ověřit politiku pod kterou byla časová značka vydána – zda je vhodná pro požadované použití dané časové značky.

TSA podepisuje své zprávy speciálním klíčem, který slouží pouze pro tyto účely. Přitom TSA může mít k dispozici několik soukromých klíčů, které odpovídají různým politikám, algoritmům, velikostem klíčů atd.

Požadavek na časovou značku má dle RFC.3161 následující formát:

```
TimeStampReq ::= SEQUENCE {
   version                      INTEGER  { v1(1) },
   messageImprint               MessageImprint,
     --a hash algorithm OID and the hash value of the data to be
     --time-stamped
   reqPolicy             TSAPolicyId              OPTIONAL,
   nonce                 INTEGER                  OPTIONAL,
   certReq               BOOLEAN                  DEFAULT FALSE,
   extensions            [0] IMPLICIT Extensions  OPTIONAL  }
```

Pole MessageImprint by mělo obsahovat hash dat, ke kterým je požadována časová značka

```
   MessageImprint ::= SEQUENCE  {
      hashAlgorithm                AlgorithmIdentifier,
      hashedMessage                OCTET STRING  }
```

Použitý hashovací algoritmus by měl být jednocestnou a vůči kolizím rezistentní funkcí a TSA by měla rozpoznávat pouze dostatečně spolehlivé (známé) hashovací algoritmy.

Číslo nonce (náhodné dostatečně velké číslo opakovatelné pouze ze zanedbatelnou pravděpodobností – např. 64 bitové celé číslo) umožňuje klientovi ověřit časové pořadí odpovědí a tatáž hodnota nonce musí být i součástí odpovědi TSA. Požadavek neobsahuje identifikaci žádající strana, TSA neověřuje tuto informaci – pokud TSA vyžaduje klientovu identifikaci (např. z důvodů finančních poplatků za transakce), pak lze použít jiné identifikační resp. autentizační prostředky (obálka CMS nebo protokol TSL atd.).
Odpověď TSA má následující formát:

```
TimeStampResp ::= SEQUENCE  {
   status                  PKIStatusInfo,
   timeStampToken          TimeStampToken     OPTIONAL  }
```

kde statut (dle RFC2510) je definován následovně:

```
PKIStatusInfo ::= SEQUENCE {
   status        PKIStatus,
   statusString  PKIFreeText     OPTIONAL,
   failInfo      PKIFailureInfo  OPTIONAL  }
```

a

```
TimeStampToken ::= ContentInfo
  -- contentType is id-signedData ([CMS])
  -- content is SignedData ([CMS])
```

Přitom

```
id-ct-TSTInfo  OBJECT IDENTIFIER ::= { iso(1) member-body(2)
us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) ct(1) 4}


TSTInfo ::= SEQUENCE  {
   version                      INTEGER  { v1(1) },
   policy                       TSAPolicyId,
   messageImprint               MessageImprint,
     -- MUST have the same value as the similar field in
     -- TimeStampReq
   serialNumber                 INTEGER,
    -- Time-Stamping users MUST be ready to accommodate integers
    -- up to 160 bits.
   genTime                      GeneralizedTime,
   accuracy                     Accuracy                 OPTIONAL,
   ordering                     BOOLEAN             DEFAULT FALSE,
   nonce                        INTEGER                  OPTIONAL,
     -- MUST be present if the similar field was present
     -- in TimeStampReq.  In that case it MUST have the same value.
   tsa                          [0] GeneralName          OPTIONAL,
   extensions                   [1] IMPLICIT Extensions   OPTIONAL  }
```

Pole `MessageImprint` musí mít touž hodnotu jako odpovídající pole v požadavku. Sériové číslo je číslo, které TSA přiřazuje každé vzniklé časové značce. Musí být unikátním číslem z hlediska časových značek, které daná TSA vydala (a to dokonce v případech, kdy služba TSA pokračuje po nějaké přestávce, zaviněné např. technickou poruchou).

Pole `genTime` je časový údaj, který indikuje časový moment, ve kterém byla příslušná časová značka vytvořena. Je vyjádřen pomocí UTC (Coordinated Universal Time) – z důvodů nejasností, které by mohly vzniknou používáním času dané lokální časové zóny. Je udáván s přesností minimálně ve vteřinách. Pole `accuracy` charakterizuje přesnost časového údaje (možnou odchylku). pokud je používáno pole `ordering`, pak lze všechny časové značky vytvořené danou časovou autoritou pomocí tohoto pole uspořádat v posloupnosti, která definuje pořadí jejich vzniku. Pole `nonce` musí být použito, pokud bylo použito v požadavku.

Pro přenos zpráv ke a od TSA není definován žádný povinný mechanismus. Lze použít E-mail, přenos souborů, TCP protokol (socket based) resp. použít http – v RFC.3161 je dán popis přibližující použití těchto jednotlivých postupů.

Zbývající část dokumentu se zabývá některými bezpečnostními požadavky na službu TSA. V přílohách je uveden příklad služby časových razítek a příslušná ASN.1 syntaxe.

3. Dokument ETSI 101 861

Dokument TS 101 861 – Time Stamping Profile – vychází z dokumentu RFC.3161 a jeho cílem je definovat

d. co musí podporovat klient časových značek;
e. co musí podporovat server časových značek.

První tři kapitoly obsahují některé všeobecné poznámky (cíle dokumentu, reference, použitou symboliku).

V kapitole 4. stanoví požadavky vzhledem ke klientovi TSP (Time Stamp Protocol). Týkají se mj. následujících bodů:

- nejsou podporována žádná rozšíření;
- jako hashovací funkce lze použít : SHA-1, MD5, RIPEMD-160 (doporučovány jsou SHA-1 a RIPEMD-160);
- podporován musí být jako podpisový algoritmus RSA s SHA-1;
- pole `accuracy` musí být podporováno (a správně chápáno);
- parametr `ordering` není používán či jeho hodnota je FALSE
- parametr `nonce` musí být podporován;
- délka klíče (RSA, DSA) minimálně 1024 bitů.

V kapitole 5. jsou pak stanoveny požadavky vzhledem k TSP serveru:

- podporována musí být „`nonce`“ (jednoznačná neopakovaná hodnota);
- podporován musí být `certReq;`
- musí být podporováno i situace, kdy není definováno žádné rozšíření;
- rozpoznány musí být hashovací algoritmy SHA-1, MD5, RIPEMD-160.
- vzhledem k podporovaným parametrů jsou vysloveny následující požadavky:
  - parametr `genTime` určuje čas s přesností na vteřiny;
  - minimální přesnost (accuracy) je jedna vteřina;
  - parametr `ordering` není používán či jeho hodnota je FALSE;
  - neexistují žádná rozšíření (kritický požadavek)

- podporován musí být jako podpisový algoritmus RSA s SHA-1 (dle RFC.2313);
- délka klíče (RSA, DSA) minimálně 1024 bitů.

V kapitole 6. je řečeno, že ze čtyř přenosových protokolů popsaných v RFC.3161 by každá autorita časových značek měla podporovat protokol opírající se o použití http.

Kapitola 7 obsahuje podrobnější podmínky vzhledem k používaným hashovacím a podpisovým algoritmům (odkazy na příslušné normy, OID).

4. Shrnutí

Problematika časových značek zde byla popsána především z hlediska příslušného protokolu, jehož prostřednictvím jsou zasílány požadavky na vytvoření časové značky a odpovědi (vytvořené časové značky) zasílané TSA. Celá problematika je však trochu širší, je nezbytné dále se např. zabývat i příslušnými požadavky na časovou autoritu (např. příslušná dokumentace, životní cyklus podpisových klíčů atd.) resp. na vzniklé formáty elektronických podpisů, které v sobě již časovou značku obsahují (některé další podrobnosti obsahuje lit. [3], resp. přímo dokumenty na stránkách ETSI). Poslední je důležité zejména pro navazující klientské aplikace.

5. Literatura

[1] PKIX Working Group: http://www.ietf.cnri.reston.va.us/html.charters/pkix-charter.html.

[2] RFC 3161-Time-Stamp Protocol: http://www.ietf.cnri.reston.va.us/rfc/rfc3161.txt
nebo
na domovské stránce Crypto-Worldu http://www.mujweb.cz/veda/gcucmp/pravo/rfc/rfc.htm

[3] Pinkava, J.: Elektronický podpis a PKI – trendy a připravované normy v EU, INVEX 2002

[4] TS 101 861, Time Stamping Profile , http://portal.etsi.org/esi/el-sign.asp

C. Profil kvalifikovaného certifikátu
Část II.
Jan Hobza, ÚOOÚ , Odbor elektronického podpisu
hobza.jan@volny.cz

OBSAH celého příspěvku

2.3 Bod c) Směrnice - jméno podepisující osoby nebo pseudonym, který je jako takový označen

Požadavky obou předpisů se v tomto bodě téměř shodují. Vždy je možné je naplnit pomocí atributů položky Subject. Položka Subject musí obsahovat DN podle X.501. Pro všechny vydané certifikáty u jedné CA musí být všechny DN subjektů unikátní po celou dobu jejího životního cyklu.

RFC 3039 doporučuje použít vhodnou podmnožinu několika základních atributů. Součástí této podmnožiny by měl být alespoň jeden z následujících atributů:

commonName
givenName
pseudonym

Realizace požadavků zákona bude jemně odlišná, neboť v případě druhé varianty by certifikát nemusel obsahovat příjmení, které zákon vyžaduje. Některé současné aplikace vyžadují k prezentaci identity držitele certifikátu atribut commonName bez ohledu na obsah atributů givenName a surename. Zároveň ale atribut commonName nemusí obsahovat přesnou identifikaci držitele [5]. Dále atribut commonName může lépe sloužit jako řetězící položka pro certifikační cestu, než atributy surename a givenName, které není zvykem uvádět

v položce Issuer. Autor proto doporučuje zahrnout do položky Subject všechny tři atributy, přičemž pro koncové uživatele by atribut commonName měl obsahovat kombinaci obsahu atributů surename a givenName a tyto dva atributy by měly obsahovat přesné znění jména a příjmení držitele certifikátu. Pro certifikáty CA autor doporučuje zahrnout firmu od atributu commonName (podle implementace položky Issuer) a atributy surename a givenName vynechat.

Certifikát může obsahovat pseudonym držitele certifikátu. V takovém případě bude obsahovat atribut pseudonym a atributy commonName, surename a givenName budou prázdné. Atribut pseudonym se užívá k utajení osobních údajů držitele certifikátu. Je vhodné jej kombinovat například s emailovou adresou v položce subjectAlternativeName (nebo jejím jiným atributem), podle potřeb spoléhající se strany[1].

Pokud certifikát obsahuje pseudonym, měl by být podle obou předpisů [1,2] jako takový označen. Díky jednoznačnosti OID považuje autor za dostatečné označení uvedení OID atributu pseudonym u daného údaje. Oba předpisy se tímto požadavkem brání tomu, aby v atributech commonName, surename a givenName byly uváděny klamavé údaje o jménu držitele certifikátu. Navrženým postupem a uvedenými doporučeními by se takovému jednání zabránilo.

Dále je vhodné začlenit do položky Subject i atribut countryName, protože řada adresářových aplikací X.500 používá tento atribut pro vstup do adresářových stromů.
Z hlediska zachování unikátnosti položky Subject je potřebné kromě výše doporučených atributů zahrnout i atribut serialNumber, který by jednoznačně identifikoval držitele certifikátu v DIT[2] CA. Způsob nacházení unikátních čísel je mimo rámec tohoto příspěvku.
Položka Subject by tedy měla minimálně obsahovat uvedené atributy (jejich struktura je navržena níže). Praxe může vyžadovat, například za účelem vydávání tzv. profesních či zaměstnaneckých certifikátů, ještě další údaje v položce Subject, pomocí nichž by bylo možné držitele certifikátu zařadit do určité organizace či její části (viz bod d)). Tyto a další možné atributy uvádí RFC 3039 a s výjimkou výše uvedených odlišností je možné v našem prostředí aplikovat i je.

```
Subject  Name

  Name ::= CHOICE { RDNSequence }

    RDNSequence ::=SEQUENCE OF RelativeDistinguishedName

RelativeDistinguishedName ::= SET OF AttributeTypeAndValue

  AttributeTypeAndValue ::= SEQUENCE {

    type   AtributeType,
    value  AttributeValue }

id-at-countryName          AttributeType ::= { id-at 6 }
--odpovídá hodnotě { 2.5.4.6 }
X520countryName ::= PrintableString 'CZ'

RelativeDistinguishedName ::= SET OF AttributeTypeAndValue

  AttributeTypeAndValue ::= SEQUENCE {
```

[1] Spoléhající se strana by měla být vždy schopná identifikovat podepisující osobu, a proto impuls pro specifikaci doplňkových atributů vychází z její strany.
[2] DIT zastupuje pojem Directory Information Tree - X.501.

```
   type   AtributeType,
   value  AttributeValue }

id-at-commonName                AttributeType ::= { id-at 3 }
--odpovídá hodnotě { 2.5.4.3 }
X520CommonName ::= utf8String

RelativeDistinguishedName ::= SET OF AttributeTypeAndValue

  AttributeTypeAndValue ::= SEQUENCE {

   type   AtributeType,
   value  AttributeValue }

id-at-surename              AttributeType ::= { id-at 4 }
--odpovídá hodnotě { 2.5.4.4 }
X520name ::= utf8String

RelativeDistinguishedName ::= SET OF AttributeTypeAndValue

  AttributeTypeAndValue ::= SEQUENCE {

   type   AtributeType,
   value  AttributeValue }

id-at-givenName             AttributeType ::= { id-at 42 }
--odpovídá hodnotě { 2.5.4.42 }
X520name ::= utf8String

RelativeDistinguishedName ::= SET OF AttributeTypeAndValue

  AttributeTypeAndValue ::= SEQUENCE {

   type   AtributeType,
   value  AttributeValue }

id-at-pseudonym             AttributeType ::= { id-at 65 }
--odpovídá hodnotě { 2.5.4.65 }
X520Pseudonym ::= utf8String

RelativeDistinguishedName ::= SET OF AttributeTypeAndValue

  AttributeTypeAndValue ::= SEQUENCE {

   type   AtributeType,
   value  AttributeValue }

id-at-serialNumber          AttributeType ::= { id-at 5 }
--odpovídá hodnotě { 2.5.4.5 }
X520SerialNumber ::= PrintableString
```

1.4 Bod d) Směrnice - zvláštní znaky podepisující osoby, pokud jsou důležité pro účel, pro nějž je certifikát určen

Požadavek obou předpisů je zde shodný. Zvláštní znaky podepisující osoby mohou být takové údaje, které jsou součástí DN držitele certifikátu a mohou být součástí Name v položce Subject a nebo jsou to údaje, které blíže charakterizují držitele certifikátu, ale nejsou součástí

hierarchické struktury DN. Takové údaje mohou být obsaženy v položkách Subject Directory Attributes, Biometric Information nebo v již zmíněné Subject Alternative Name.

Mezi rozšiřující atributy položky Subject může v tomto ohledu být atribut organizationName a organizationalUnitName. Rozšiřující položka Biometric Information obsahuje hash a případně ukazatel URI na příslušnou autentizační informaci. Rozšiřující položka Subject Directory Attributes může obsahovat například státní příslušnost držitele certifikátu (countryOfCitizenship [6]). Způsob použití všech uvedených položek uvádí dokument RFC 3039, resp. RFC 3280 a v našem prostředí je možné je plně implementovat.

```
Subject  Name

 Name ::= CHOICE { RDNSequence }

   RDNSequence ::=SEQUENCE OF RelativeDistinguishedName

RelativeDistinguishedName ::= SET OF AttributeTypeAndValue

 AttributeTypeAndValue ::= SEQUENCE {

   type   AtributeType,
   value  AttributeValue }

id-at-organizationName    AttributeType ::= { id-at 10 }
--odpovídá hodnotě { 2.5.4.10 }
X520OrganizationName ::= utf8String

RelativeDistinguishedName ::= SET OF AttributeTypeAndValue

 AttributeTypeAndValue ::= SEQUENCE {

   type   AtributeType,
   value  AttributeValue }

id-at-organizationUnitName AttributeType ::= { id-at 11 }
--odpovídá hodnotě { 2.5.4.11 }
X520OrganizationUnitName ::= utf8String

biometricInfo  EXTENSION ::= {
            SYNTAX           BiometricSyntax
            IDENTIFIED BY      id-pe-biometricInfo }

              id-pe-biometricInfo OBJECT IDENTIFIER  ::= {id-pe 2}
              --odpovídá hodnotě OID { 1.3.6.1.5.5.7.1.2 }
        BiometricSyntax ::= SEQUENCE OF BiometricData

           BiometricData ::= SEQUENCE {
             typeOfBiometricData  TypeOfBiometricData,
             hashAlgorithm        AlgorithmIdentifier,
             biometricDataHash    OCTET STRING,
             sourceDataUri        IA5String OPTIONAL }

               TypeOfBiometricData ::= CHOICE {
                 predefinedBiometricType    PredefinedBiometricType,
                       biometricDataID           OBJECT IDENTIFIER }

                        PredefinedBiometricType ::= INTEGER { picture(0),
                          handwritten-signature(1)}
--do současné doby byly pro účely certifikátů veřejných klíčů X.509 rozeznány pouze tyto dva typy biometrické
informace.
```

```
subjectDirectoryAttributes  EXTENSION ::= {
        SYTNAX                          SubjectDirectoryAttributesSytax
        IDNETIFIED BY  id-ce-subjectDirectoryAttributes }

          id-ce-subjectDiroctoryAttributes OBJECT IDENTIFIER ::={ id-ce 9 }
          --odpovídá hodnotě { 2.5.29.9 }

                SubjectDirectoryAttributesSyntax   ::= SEQUENCE OF SDAttributes

                 SDAttributes ::= SEQUENCE {
                  type              AttributeType
                  value  AttributeValue }

                        id-pda-countryOfCitizenship AttributeType ::={ id-pda 4 }
                        -- odpovídá hodnotě OID { 1.3.6.1.5.5.7.9.4 }
                        countryOfCitizenship ::= utf8String
```

2.5 Bod e) Směrnice - data pro ověřování podpisu, která odpovídají datům pro vytváření podpisu, která jsou pod kontrolou podepisující osoby

Oba předpisy se v tomto požadavku neliší. Požadavek na uvedení veřejného klíče držitele certifikátu je naplněn v položce subjectPublicKeyInfo, kde je dále uveden i algoritmus pro jeho použití.

```
subjectPublicKeyInfo      SubjectPublicKeyInfo

        SubjectPublicKeyInfo ::= SEQUENCE {
          algorithm AlgorithmIdentifier,
          subjectPublicKey   BIT STRING }

            algorithm AlgorithmIdentifier ::= SEQUENCE {
      algorithm OBJECT IDENTIFIER,
      parameters OPEN TYPE }

        subjectPublicKey BIT STRING
```

2.6 Bod f) Směrnice - označení počátku a konce doby platnosti certifikátu

Požadavek bodu f) Směrnice se shoduje s požadavkem bodu h) Zákona. Je naplněn položkou validity podle ITU X.509. Pravidla pro stanovení času v položce vychází z RFC 3280.

```
        validity  Validity

          Validity ::= SEQUENCE {
            notBefore      Time,
            notAfter       Time }

                  Time ::= CHOICE {
                    utcTime       UTCTime,
generalTime    GeneralizedTime }
```

2.7 Bod g) Směrnice - identifikační kód certifikátu

Požadavek bodu g) je opět stejný, pouze zákon o elektronickém podpisu zdůrazňuje požadavek RFC 3280 na jedinečnost v rámci dané CA. Sériové číslo certifikátu by mělo být pozitivní a ne delší než 20 osmibitových znaků.

```
serialNumber  CertificateSerialNumber

CertificateSerialNumber ::= INTEGER
```

2.8 Bod h) Směrnice - zaručený elektronický podpis poskytovatele certifikačních služeb, který certifikát vydává

Oba předpisy jsou v tomto bodě ve shodě. Zaručený elektronický podpis certifikátu je obsahem položky signatureValue. Jako vstup do funkce definované v signatureAlgoritm je část ASN.1 struktury certifikátů tbsCertificate, kódované metodou DER. Podpis je ve formátu BIT STRING.

```
signatureValue ::= BIT STRING
```

2.9 Bod i) Směrnice - případně omezení použitelnosti certifikátu

Požadavky obou předpisů se v tomto bodě opět poněkud odlišují. Požadavek Směrnice na případné omezení použitelnosti certifikátu se vztahuje na případné omezení v certifikační politice (identifikované v položce certificatePolicies), nebo na omezení použitelnosti veřejného klíče v položce keyUsage, případně extendedKeyUsage. Český překlad bodu i) v zákonu je spíše opisný než doslovný a spojení „případné omezení podle povahy a rozsahu“ je velmi neurčité. Z textu není jasné, o povahu a rozsah čeho se jedná. Zda se jedná o hodnotu transakcí, prostředí použití klíčů, skupinu spoléhajících osob, nebo možnosti použití veřejného klíče. Pro řešení výkladové nejistoty je možné využít analogie a pokusit se vyložit bod i) podobně, jako je vykládán bod i) Směrnice; tedy řešení spočívá v použití výše uvedených rozšiřujících položek certifikátu. Omezení pomocí certifikační politiky je věcí vzájemného vztahu mezi poskytovatelem a držitelem certifikátu a je mimo rámec tohoto příspěvku. Jeho následná implementace do ASN.1 struktury by byla obdobná jako v bodě a) 1., a proto ji dále nebudeme uvádět. Zásadní je omezení pomocí položky keyUsage [5]. Ta se vztahuje na možnosti použití veřejného klíče držitele. Položka má následně definovanou škálu omezení použití:

```
digitalSignature        (0),
nonRepudiation          (1),
keyEncipherment         (2),
dataEncipherment        (3),
keyAgreement            (4),
keyCertSign             (5),
cRLSign                 (6),
encipherOnly            (7),
decipherOnly            (8).
```

Omezení použití by měly být schopny rozeznat všechny aplikace odpovídající RFC 3280. Zároveň by si tohoto omezení měly být vědomy všechny strany, které s certifikátem a příslušným soukromým klíčem zacházejí. Nemělo by se například stát (a to jak z vůle podepisující osoby, tak vinou chybně fungující aplikace), aby při omezení na digitalSignature a nonRepuditation, byl veřejný klíč použitelný k ověření podpisu CRL.

Vzhledem k požadavkům směrnice, která jasně definuje účel elektronických podpisů založených na kvalifikovaných certifikátech, a vzhledem k dikci RFC 3039 autor doporučuje omezit použití veřejných klíčů kvalifikovaných certifikátů za účelem nonRepudiation podle RFC 3039, nebo v kombinaci s digitalSignature podle RFC 3280. ExtendedKeyUsage by se v takovém případě omezila na emailProtection a byla by nadbytečná.

```
keyUsage EXTENSION ::= {
    SYNTAX        KeyUsage
    IDENTIFIED BY id-ce-keyUsage }

 id-ce-keyUsage OBJECT IDENTIFIER ::= {id-ce 15 }
 --odpovídá hodnotě { 2.5.29.15 }

            critical ::= BOOLEAN TRUE

            KeyUsage ::= BIT STRING {
              digitalSignature  (0),
        nonRepudiation    (1) }
```

2.10 Bod j) Směrnice - případně omezení hodnot transakcí, pro něž lze certifikát použít

Požadavek obou předpisů je v tomto bodě téměř totožný. Lze jej naplnit prohlášením definovaným v položce qualifiedCertificateStatement. Na rozdíl od bodu a) není vhodné definovat toto prohlášení pouze pomocí jeho OID, ale zároveň v certifikátu uvést hodnotu transakce (vyjádřenou číslem a označením měny [9]). Důvody k tomu jsou zřejmé. Nicméně i toto řešení si vyžaduje definování a zveřejnění prohlášení o omezení hodnoty transakcí dozorovým/akreditačním orgánem, obdobně jako v bodě a). Dokument TS 101 862 zachází s požadavkem bodu j) obdobně.

```
qcStatements EXTENSION ::= {
  SYNTAX                  QCStatements,
  IDENTIFIED BY           id-pe-qcStatements }

    id-pe-qcStatements OBJECT IDENTIFIER ::= { id-pe 3 }
   --odpovídá hodnotě OID „1.3.6.1.5.5.7.1.3“

  QCStatements ::= SEQUENCE OF QCStatement

    QCStatement-2 ::= SEQUENCE {
          SYNTAX            QcLimitValue,
IDENTIFIED BY id-etsi-qcs-QcLimitValue }

                    id-etsi-qcs-QcLimitValue OBJECT IDENTIFIER ::= {
                    id-etsi-qcs 2 }
```

--odpovídá hodnotě OID { 0.4.0.1862.1.2 }. Pro účely kvalifikovaných certifikátů vydávaných podle zákona o elektronickém podpisu autor navrhuje vytvořit vlastní prohlášení.

```
QcLimitValue ::= MonetaryValue

        MonetaryValue ::= SEQUENCE {
                currency Iso4217CurrencyCode,
                amount   INTEGER,
                exponent INTEGER }

                    Iso4217CurrencyCode ::= PrintableString `CZK`
```

3 Závěr

Formáty některých atributů jsou v příspěvku uvedeny bez dalších možných variant.

Kódování UTF8 autor upřednostňuje, ale nevylučuje použití jiných formátů podle RFC 3280. Důvodem je časové omezení platnosti ostatních formátů.

Příspěvek obsahuje upřesnění několika položek kvalifikovaného certifikátu podle zákona o elektronickém podpisu. Nezabývá se všemi položkami certifikátu, které by měly být jeho součástí. K vytvoření úplného profilu certifikátu autor doporučuje zároveň použít RFC 3039.

4 References

[1] Směrnice Evropského parlamentu a Rady 1999/93/ES o zásadách společenství pro elektronické podpisy

[2] Zákon č. 227/2000 Sb., o elektronickém podpisu

[3] ITU-T Recommendation X.509 (1997): ISO/IEC 9594-8: Information Technology - Open Systems Interconnection – The directory: Public-key and attribute certificate frameworks.

[4] ETSI TS 101 862 v1.2.1 (2001): Qualified certificate profile.

[5] RFC 3280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile.

[6] RFC 3039: Internet X.509 Public Key Infrastructure Qualified Certificate Profile.

[7] RFC 2247: Using Domains in LDAP/X.500 Distinguished Names.

[8] ISO/IEC 8824-1 (1998): ITU-T Recommendation X.680 (1997): Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation.

[9] ISO 4217 (1995): Codes for the representation of currencies and funds.

D. Letem šifrovým světem

Pozvánka 1

2. MEZINÁRODNÍ KONFERENCE NATO PfP/PWP "Bezpečnost a ochrana utajovaných skutečností"

Přednášky expertů a diskuse ke koncepci a metodám zajištění bezpečnosti a ochrany informací ve státní administrativě a aktuálním poznatkům z oblasti bezpečnosti počítačových sítí.

Kontaktní osoba: Jaroslav Dočkal (jdockal@vabo.cz)

Informaci najdete zde : http://www.vabo.cz/spi/

Témata odborné části konference:

Pondělí 28. duben 2003 odpoledne : ***Bezpečnost počítačové sítě***

Úterý 29. duben 2003 dopoledne : ***Ochrana utajovaných skutečností***

Úterý 29. duben 2003 odpoledne : **Bezpečnost informací ve vojenském prostředí**

Středa 30. duben 2003 : ***Počítačová kryptografie***

Počítačová kryptografie
Je specializovaný workshop Velikonoční kryptologie 2003 a navazuje na tradici vánočních a velikonočních setkání českých a slovenských kryptologů .

Vypsaná témata :
- aplikovaná kryptografie
- bezpečnostní aplikace kryptografie
- kryptoanalýza
- kryptografické algoritmy, jejich návrh a implementace
- modularita a opakované použití ověřených kritických komponent
- stanovení míry kryptografické bezpečnosti
- přijatelná rizika kryptografické bezpečnosti
  standardizace a kryptografie
- legislativa související s kryptografií
- technologie posilující soukromí
- další oblasti kryptografie

Termín odevzdání referátů do sborníku je do 28.2.2003 na e-mailovou adresu jaroslav.dockal@vabo.cz . Rozsah příspěvku je omezen 10 stranami. Předpokládaná délka je 15 minut.

Pozvánka 2

The 3rd Central European Conference on Cryptology TATRACRYPT '03

Datum : June 26-28, 2003
Místo: Bratislava, Slovakia

Pořadatel: Institute of Mathematics, Slovak Academy of Sciences, Bratislava
Department of Mathematics, Faculty of Electrical Engineering and Information Technology in Bratislava

Detaily na stránce : http://www.elf.stuba.sk/Katedry/KM/TATRACRYPT/index.htm

Kontaktní adresy: grosek@kmat.elf.stuba.sk , nemoga@mat.savba.sk

Tato konference je pokračováním úspěšných konferencí:

TATRACRYPT '01 - Liptovský Ján, Slovakia
http://www.elf.stuba.sk/Katedry/KM/crypto/slovak/konf/index.htm
a
HAJDUCRYPT '02 - Debrecen, Hungary
http://neumann.math.klte.hu/~hcrypt/

Předběžný seznam zvaných řečníků :
- Professor Spyros S. Magliveras, Florida Atlantic University, USA
- RNDr. Vlastimil Klima, CSc., ICZ a.s, Praha 10, Czech Republic
- Professor Pino Caballero Gil, Universidad de la Laguna, Tenerife, Spain

Důležitá data :
February 28, 2003: to submit a plenary talk
March 31, 2003: 2nd announcement
May 31, 2003: to submit abstracts of short talks
May 31, 2003: to be registered, at the latest
June 9, 2003: preliminary program
June 26-28, 2003: the Conference

Pozvánka 3

5.ročník konference Internet a konkurenceschopnost podniku

Pořadatel : Univerzita Tomáše Bati
Kontakt : Renata Sysalová, FaME UTB ve Zlíně
Ústav informatiky a statistiky
Mostní 5139, 760 01 Zlín
tel.: 57 603 2584 nebo 57 603 7416
e-mail: sysalova@fame.utb.cz

Koncepce konference:
Hlavní téma je definování současného stavu a možnosti využívání Internetu pro zvyšování konkurenceschopnosti podniku.
V rámci konference budou předneseny a prezentovány produkty a služby internetu v následujících tématických blocích:
Blok A – Elektronické podnikání
Blok B – Internet a bezpečnost podniku
Blok C – Intranet v podnikové komunikaci
Blok D – E-learning v podnikovém vzdělávání

O čem jsme psali v lednu 2000 - 2002

Crypto-World 1/2000

Crypto-World Vánoce/2000

Crypto-World 1/2001

Příloha:
trustcert.pdf (upoutávka na služby Certifikační Autority TrustCert)

Crypto-World 1/2002

E. Závěrečné informace

1. Sešit

Crypto-World je oficiální informační sešit "Kryptologické sekce Jednoty českých matematiků a fyziků" (GCUCMP). Všechny uvedené informace jsou převzaty z volně dostupných prověřených zdrojů (Internet, noviny) nebo se jedná o původní články podepsané autory. Případné chyby a nepřesnosti jsou dílem P.Vondrušky a autorů jednotlivých podepsaných článků, GCUCMP za ně nemá odbornou ani jinou zodpovědnost.

Články neprocházejí jazykovou kontrolou!

Adresa URL, na níž můžete najít tento sešit (nejdříve 15 dní po jeho rozeslání) a předchozí sešity GCUCMP (zkonvertovány do PDF formátu), informace o přednáškách z kryptologie na MFF UK, některé články a další související témata :
http://www.mujweb.cz/veda/gcucmp

2. Registrace / zrušení registrace

Zájemci **o zasílání** tohoto sešitu se mohou zaregistrovat pomocí e-mailu na adrese pavel.vondruska@post.cz (předmět: Crypto-World) nebo použít k odeslání žádosti o registraci formulář na http://www.mujweb.cz/veda/gcucmp/ . Při registraci vyžadujeme pouze jméno a příjmení, titul, pracoviště (není podmínkou) a e-mail adresu určenou k zasílání sešitu.

Ke **zrušení registrace** stačí zaslat krátkou zprávu na e-mail pavel.vondruska@post.cz (předmět: ruším odběr Crypto-Worldu !). Ve zprávě prosím uveďte jméno a příjmení a e-mail adresu, na kterou byl sešit zasílán.

3. Spojení

běžná komunikace, zasílání příspěvků k otištění , informace
pavel.vondruska@ct.cz
vondruska.p@seznam.cz
pavel.vondruska@post.cz