Crypto-World

Informační sešit GCUCMP

Ročník 6, číslo 1/2004 **19. leden 2004**

1/2004

Připravil : Mgr.Pavel Vondruška

Sešit je rozesílán registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(490 e-mail výtisků)

Obsah : **Str.**

(články neprocházejí jazykovou korekturou)

A. Tajemství Voynichova rukopisu odhaleno?
Mgr. Pavel Vondruška, ČESKÝ TELECOM, a.s.

Koncem roku 2003 obletěla svět zpráva, že vědecký pracovník G. Rugg (Keele University, UK) jednoduchým způsobem vysvětlil vytvoření záhadného Voynichova rukopisu. K vytvoření šifrového textu, který obsahuje, podle něj stačí opakovaně použít Cardanovu mřížku. Své tvrzení uvádí v článku pro prestižní časopis Cryptologia. Článek bude v nejbližší době publikován (Rugg, G. An elegant hoax? A possible solution to the Voynich manuscript. *Cryptologia*, http://www.dean.usma.edu/math/pubs/cryptologia/).

Voynichův rukopis je natolik známý a je mu věnována taková publicita, že zde pro připomenutí uvedu pouze několik nejzákladnějších údajů. Jedná se o starodávný šifrový text; co je v něm napsáno a co zobrazují bohaté astronomicko / astrologické ilustrace není známo. Tato záhadná kniha se poprvé objevila na dvoře císaře Rudolfa II. (1552-1612), který ji zakoupil do svých sbírek. Její skutečný vznik je však obestřen záhadou – císaři byla prodána s tím, že autorem byl Roger Bacon (1214-1292). Rukopis časem upadl v zapomnění. Znovu byla kniha o více jak 200 stránkách objevena až roku 1912 a podle svého nálezce se stala známá jako Voynichův manuskript.

V současné době je kniha v majetku university Yale. Kvalitní fotokopie celého rukopisu si můžete prohlédnout na jejích stránkách (vstupní heslo Voynich) http://highway49.library.yale.edu/photonegatives/ .

Pokud vás zajímají další podrobnosti o tomto záhadném rukopisu, doporučuji začít na stránkách :
http://www.crystalinks.com/voynich.html
http://math.ucr.edu/home/baez/voynich.html

Řada předních kryptologů i amatérů se téměř sto let snaží rozluštit nebo alespoň objasnit text, který kniha obsahuje. Na Internetu naleznete velice fundované rozbory, statistiky a dokonce i fonty, které připomínají v knize použité písmo.

V úvodu zmíněný článek „World's most mysterious book may be a hoax“ informující o Ruggově tvrzeních byl zveřejněn 17.12.2003 na Nature (http://www.nature.com/nsu/031215/031215-5.html).

Těším se na originální Ruggův článek, který v nejbližší době vyjde v časopise Cryptologia (Volume XXVIII Number 1, January 2004), ale osobně se domnívám, že záhada v něm odhalena zdaleka ještě nebude. Cardanova mřížka (o níž se Nature zmiňuje) je příliš „primitivní“ šifrový systém, než aby text s ní zašifrovaný odolával po sto let systematickému útoku tolika badatelů ….

B. Vztah důvěry mezi můstkovými certifikačními autoritami
Mgr. Pavel Vondruška, ČESKÝ TELECOM, a.s.

V tomto článku se budeme zabývat konkrétními řešeními používanými v rámci jednotlivých můstkových autorit. Představíme si tři nejdůležitější: The Federal Bridge Certificate Authority - FBCA, European Bridge Certificate Authority – EBCA a Interchange of Data between Administrations - IDA. Popíšeme si základní rozdíly v řešeních použitých těmito autoritami, rozdíly v procesu přistoupení nového subjektu k těmto autoritám a oblast, pro kterou má můstková autorita sloužit.

Z hlediska plánu budování e-Evropy (projekt e-Europe 2005, viz např. http://www.micr.cz/) má poslední z jmenovaných můstkových certifikačních autorit (IDA) sehrát důležitou úlohu. Tato autorita má zajistit možnost plnění požadavků přijaté Směrnice 1999/93/ES o zásadách Společenství pro elektronické podpisy a to zejména článku 4. V něm se členským státům Společenství stanoví povinnost, že nesmí v oblastech, na které se vztahuje tato směrnice, omezovat poskytování certifikačních služeb pocházejících z jiného členského státu. Využití certifikátů vydaných v jiných členských státech má zajistit právě IDA.

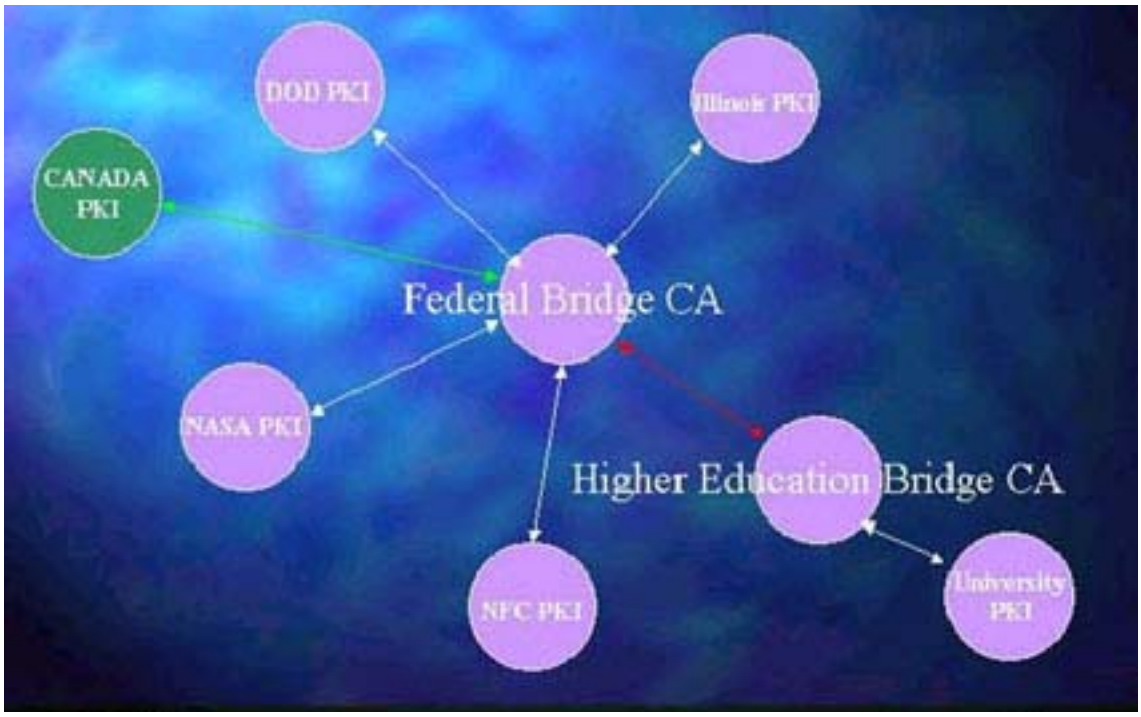
Federální můstková certifikační autorita (The Federal Bridge Certificate Authority)

Náš výklad o můstkových certifikačních autoritách začneme největší a pravděpodobně i nejznámější na světě Federal Bridge Certificate Authority (FBCA). Tato autorita spojuje nejen významná a rozsáhlá PKI velkých vládních subjektů (např. NASA, NIST,…), ale i další můstkové certifikační autority: např. ministerstva obrany (DoD Bridge Certification Authority), univerzitní (Higher Education Bridge CA) a kanadskou můstkovou autoritu (Canada PKI). Schéma FBCA (značně zjednodušené) je uvedené na obrázku č.1.

Výstavba této autority byla plánována od roku 1998. Projekt byl zahájen poté, co byla definitivně v USA opuštěna myšlenka postavit jedinou hierarchickou strukturu, která by měla společnou kořenovou vládní certifikační autoritu. V prosinci 2000 byla vyhlášena první verze Certifikační politiky Federální můstkové certifikační autority. V září roku 2002 ji nahradila verze nová, která je používána dosud.

Po vyhlášení certifikační politiky následovalo vydání rozsáhlé řady dalších významných dokumentů, které tvoří a doplňují předpisovou základnu FBCA. Všechny dokumenty, určené ke zveřejnění, jsou dostupné na domácí stránce můstkové autority http://www.cio.gov/fpkisc nebo na stránce National Institute of Standards and Technology (NIST, http://csrc.nist.gov/pki), se kterým Federální můstková certifikační autorita v oblasti bezpečnosti a standardů velmi úzce spolupracuje.

Z technologického hlediska jsou PKI jednotlivých entit křížově certifikovány s FBCA. Samotná CA pracuje off-line. Základní metodou šíření důležitých dat pro spoléhající subjekty je využití adresářové služby, která má zaručenou dostupnost on-line 24 x 7 x 365. Z důvodu zajištění nepřetržité dostupnosti jsou adresářové služby budovány duálně (1. dc=gov, 2. o=U.S. Government, c=US).



Obr. č.1– Schéma Federální můstkové certifikační autority

Metodologie, kritéria a samotný proces přistoupení a vyvázání z FBCA byly vydány v samostatném závazném dokumentu v březnu 2003.

Celý proces přistoupení je rozdělen do čtyř následujících fází:

1. Inicializační fáze.
2. Fáze mapování politik .
3. Testovací fáze.
4. Fáze uzavření dohody.

Zastavme se krátce u druhé fáze - mapování politik jednotlivých entit ve FBCA. Tato fáze je z teoretického hlediska velice zajímavá. Při přistoupení nového subjektu s vlastním PKI se díky této proceduře zařadí subjekt do určitého stupně a tím je určen stupeň důvěry v certifikáty, které tento subjekt vydává. Nevyžaduje se tedy splnění nějaké konkrétní základní certifikační politiky, která by byla povinná pro jednotlivé entity, které autorita propojuje. K dispozici je matice převodních vztahů mezi politikami, které odpovídají těmto následujícím přípustným normám - ISO Banking, Can (High, Med, Basic, Rud), Fed PKI (High, Med, Basic, Rud), DoD (2,3,4). Příslušný subjekt je pak označen jako např. uživatel DoD třídy 3 (Subscriber DoD Class 3) apod.

Mimo toto mapování se dále testuje, zda jsou splněny požadavky certifikační politiky (Citizen & Commerce Certificate Policy, Version 1.0, December 3, 2002), která opravňuje k využívání certifikátů koncových uživatelů v oblasti veřejné moci (použijeme-li terminologii našeho zákona o elektronickém podpisu č.227/2000 Sb., paragrafu 11).
Mezi základní požadavky této politiky patří přístup k informacím o stavu certifikátu. Vyžaduje se pomocí CRL (Certificate Revocation List, seznam certifikátů, které byly zneplatněny) nebo OCSP (Online Certificate Status Protocol, protokol typu dotaz – odpověď, který vrací informaci o stavu certifikátu). Změna stavu certifikátu musí být dostupná nejpozději do 72 hodin. Koncoví uživatelé mohou využívat algoritmy RSA a DSA s délkou modulu klíče nejméně 1024 bitů. Klíče musí být generovány a uchovávány

v kryptografických prostředcích, které splňují požadavky normy FIPS 140, Level 2. Pro šifrování mohou být používány pouze algoritmy schválené ve standardech FIPS.

V případě, že mapování bylo ukončeno a byly splněny všechny požadavky této politiky, je příslušná identifikace zapsána pomocí OID (Object Identifier) do certifikátu. OID je unikátní registrovaný alfa-numerický identifikátor, který slouží k jednoznačné identifikaci specifických objektů nebo tříd těchto objektů. V tomto případě je jeho hodnota:

citizen-and-commerce-approved::= 2.16.840.1.101.3.2.1.14.2

Takto označené certifikáty mají, co do použití, stejný význam jako kvalifikované certifikáty vydávané akreditovaným poskytovatelem v ČR.

Lze tedy konstatovat, že ve FBCA jsou sdruženy entity, které vydávají certifikáty různých „kvalit“. Kvalita certifikátu je vyznačena takovým způsobem, aby spoléhající se subjekt byl informován o zařazení do příslušné kategorie. Certifikáty (bez ohledu na předchozí zařazení), které lze použít pro vládní komunikaci, jsou označeny speciálním OID.

Nyní tuto můstkovou autoritu a její specifické řešení opustíme a přesuneme se do Evropy, přesněji do Evropské unie.

Evropská můstková autorita (European Bridge Certification Autority)

Nejrozsáhlejší a nejznámější můstkovou autoritou v Evropě je Evropská můstková autorita (European Bridge Certification Autority, EBCA). Vznikla v květnu roku 2000 z podnětu Deutsche Telekom a Deutsche Bank. EBCA je řízena výborem (Board) s mezinárodním zastoupením z hospodářské sféry, veřejné správy a oblasti vědy. Ve výboru zasedá Deutsche Telekom, Deutsche Bank, DaimlerChrysler, TeleTrusT, SIZ (Sparkassenorganisation) a BSI (Spolkový úřad pro bezpečnost v IT). BSI ve výboru zastupuje Spolková ministerstva a úřady. Je to otevřené sdružení a tedy rozšiřování o další subjekty je možné a je podporováno (např. v březnu 2003 se připojil SAP a v květnu 2003 Německá bankovní spořitelna).

Evropská můstková autorita je neziskovou iniciativou řady podnikatelských subjektů a veřejných institucí. Koncepce můstkové autority je založena na využití stávajících PKI a již vydaných certifikátů a tím chrání původní vynaložené investice účastníků. Sdružují se v ní organizace využívající certifikáty rozličných interních PKI. V úloze přemostění mezi jednotlivými organizacemi ověřuje EBCA kořenové certifikáty jednotlivých účastníků. Nový uchazeč může bezprostředně po přijetí začít komunikovat důvěryhodným způsobem se všemi ostatními přihlášenými účastníky. Bez využití EBCA by musel vést samostatná zdlouhavá dvoustranná jednání či uzavírat smlouvy o vzájemném uznávání certifikátů se subjekty, které jsou v můstkové autoritě sdruženy. Díky EBCA odpadá předávání jednotlivých uživatelských certifikátů nebo zřizování křížové certifikace s velkým počtem organizací. Účast v Evropské můstkové autoritě dále umožňuje výměnu zkušeností mezi účastníky a odbornou pomoc zájemcům, jež dosud vlastní PKI nevybudovali, nebo mají problémy s kompatibilitou svého řešení.

Základní podmínkou, která musí být v certifikačních politikách interních certifikačních autorit jednotlivých subjektů splněna, je osobní registrace žadatelů o certifikát se současným ověřením totožnosti žadatele. Původním cílem projektu bylo zajištění bezpečné poštovní komunikace mezi subjekty sdružené v můstkové autoritě, z tohoto důvodu se dále vyžaduje, aby Mail systém všech subjektů využíval protokol S/MIME.

V „milnících“ výstavby, která je k dispozici na www stránce Evropské můstkové autority (http://www.bridge-ca.org/), je uvedeno, že v květnu a červnu 2003 proběhlo úspěšné otestování využití vztahu důvěry pro různé PKI služby všech členů EBCA a původní vzájemné využití pouze poštovních služeb bylo rozšířeno. Zabezpečení poštovních služeb mezi účastníky můstkové autority fungovalo úspěšně od srpna 2000 a to bez ohledu na to, že jednotliví účastníci využívají nejrůznější mailové systémy. Např. Deutsche Bank využívá Lotus Notes s plug-in „MailProtect“, naproti tomu Deutsche Telekom Outlook 98 a SECUDE plug-in Authentmail.

.

Pět kroků k bezpečnému partnerství v EBCA

1. **Certifikační politika** – Tato etapa je prováděna uvnitř organizace a jde v ní o to, aby použitá Certifikační politika splňovala minimální požadavky na členy EBCA. Jedná se zejména o proces registrace žadatelů (o vyžadované osobní registraci a ověření totožnosti jsme se již zmínili), zajištění bezpečnosti vydávání a následné správy certifikátů, dostupnost CRL. Dále je potřeba provést vlastní ohodnocení kompatibility řešení, zejména se soustředit na přípravu implementace údajů dodávaných Evropskou můstkovou autoritou a ověření, zda uživatelé interního PKI používají poštovní klienty schopné vhodné konfigurace (silná kryptografie, algoritmy pro šifrování a vytváření elektronických podpisů, S/MIME).
2. **Kontakt** – Následuje kontakt zájemce s Evropskou můstkovou autoritou. Může být uskutečněn telefonicky, e-mailem, faxem nebo listovní zásilkou. Možné je též využít formulář o přistoupení umístěný na webové stránce http://www..bridge-ca.org. Fáze kontaktu je ukončena vyplněním žádosti o ověření důvěryhodnosti přistupující organizace.
3. **Test interoperability** – Ve třetí etapě obdrží žadatel o vstup do můstkové autority pokyny týkající se technického testu interoperability jeho řešení. Pro vlastní provedení testu je dále přidělen k dispozici pracovník EBCA. Ve většině případů dochází pouze k drobným úpravám v nastavení interního PKI, např. nutné konfiguraci maileru a může být aplikován i dodatečný plugin.
4. **Uzavření smlouvy** – Po úspěšných předchozích etapách je předána účastnická smlouva k podpisu a navzájem jsou důvěryhodným způsobem předány kořenový certifikát přistupující CA a certifikát EBCA.
5. **Využití** – Následuje registrace kořenového certifikátu nově přijatého subjektu v rámci EBCA a jeho distribuce všem ostatním účastnickým organizacím, jejichž důvěryhodnost byla dříve stejným způsobem ověřena. Nový člen obdrží od EBCA seznam důvěryhodných certifikátů účastnických organizací. Provedením importu doručených kořenových certifikátů jednotlivými členy se nový subjekt stává plnohodnotným účastníkem EBCA a může bezprostředně zahájit bezpečnou komunikaci s ostatními účastníky.

K bezpečné komunikaci mezi Evropskou můstkovou autoritou a jejími členy se používá velice prosté metody. Distribuovaná data se nejprve zazipují a elektronicky se podepíšou příslušnou autoritou. Data se potom rozesílají vložená do e-mailu jako příloha. Tento e-mail je zašifrován pro příslušného příjemce a podepsán konkrétním odesílatelem. V nejbližší době se předpokládá nahrazení této metody důsledným využíváním protokolu CTL (Certificate Trust List) který slouží pro přenos důvěryhodných zpráv. Je to proprietární standard firmy Microsoft, který je založen na de-facto standardu PKCS #7 (Cryptographic Message Syntax Standard) firmy RSA Security. CTL standard je dostupný téměř ve všech

aplikacích firmy Microsoft, které jsou připraveny k využití PKI. Na obrázku č.2 je uvedena definice (na nejvyšší úrovni) tohoto standardu pomocí jazyku pro popis dat ASN (Abstract Syntax Notation).

```
CertificateTrustList ::=SEQUENCE
Version              Version DEFAULT v1,
subjectUsage         Subject Usage,
listIdentifier       ListIdentifier          OPTIONAL
sequenceNumber       INTEGER                 OPTIONAL
thisUpdate           ChoiceOfTime,
nextUpdate           ChoiceOfTime,
subjectAlgorithm     AlgorithmIdentifier,
trustedSubjects      TrustedSubjects,
extensions           extensions              OPTIONAL
```

Obr. č.2 – Definice CTL pomocí ASN

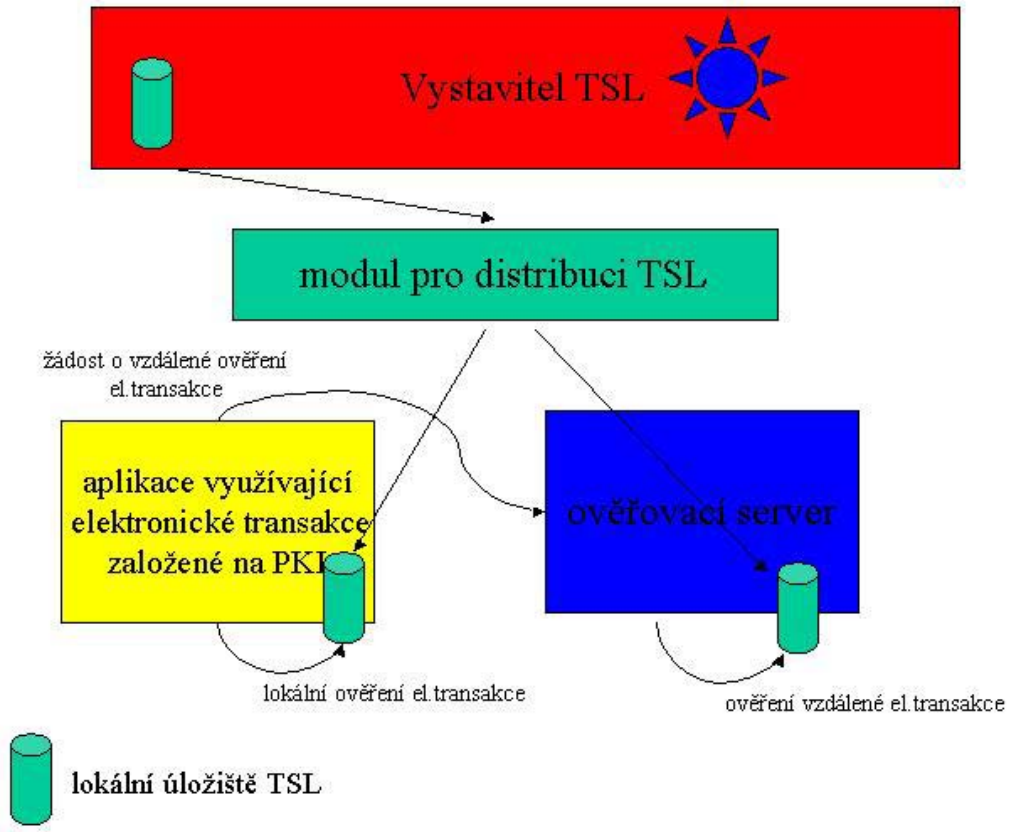
EBCA je rozsáhlá můstková autorita, která zajišťuje bezpečnou komunikaci a využití dalších PKI služeb mezi komerčními subjekty v Evropě. Na rozdíl od FBCA nejsou využívány společné adresářové služby. Výměna důležitých informací se zde děje jednoduchým, efektivním a bezpečným způsobem. Vzhledem k výše popsanému systému však důvěryhodnost komunikace v rámci EBCA závisí do jisté míry výrazně nejen na chování samotné můstkové certifikační autority, ale i správců jednotlivých interních PKI tohoto sdružení. Z tohoto důvodu se klade velký význam na audit celého systému. Audit zahrnuje i chování administrativních správců jednotlivých interních PKI. Velikou výhodou je dokonalá kompatibilita všech používaných systémů, technická podpora členů EBCA a nízké náklady na provoz EBCA, které vyplývají z jednoduchého a účelně fungujícího systému.

Můstková certifikační autorita IDA (Interchange of Data between Administrations)

Evropská můstková autorita je především sdružením komerčních subjektů a je využívána ke komerčním účelům. Při vstupu nových členů se neklade důraz na to, zda jejich interní PKI byla budována v souladu s požadavky Směrnice 1999/93/ES o zásadách Společenství pro elektronické podpisy nebo ne. Pro zajištění komunikace v rámci plánovaného projektu e-Europe 2005 tedy není tato autorita vhodná. Úlohu můstkové autority, která by zajistila nastavení vztahů důvěry mezi subjekty jednotlivých členských států Společenství a zajistila tak komunikaci státní správy v EU, má zajistit jiná můstková certifikační autorita - IDA (Interchange of Data between Administrations). Výstavba této autority byla zahájena v roce 2001 v rámci projektu PKICUG (http://europa.eu.int/ISPO/ida/). Typické pro celý projekt je striktní dodržování všech standardů, norem a doporučení pro certifikační autority. Cílem je bezpečná komunikace a bezpečná výměna elektronicky podepsaných dokumentů mezi státními orgány jednotlivých členských zemích Společenství. V současné době je sdruženo v pilotní části tohoto projektu osm členských zemí: Belgie, Dánsko, Španělsko, Francie, Itálie, Holandsko, Švédsko, Velká Británie. Německo v tomto sdružení není. V současné době německé státní a správní orgány využívají k vzájemné komunikaci EBCA.

Standardy, podle kterých se ve výstavbě postupuje, jsou zejména standardy pro certifikační autority, které vydávají kvalifikované certifikáty, vyvíjené ETSI a CEN.

Z technického hlediska se vztah důvěry zajišťuje křížovou certifikací certifikačních autorit jednotlivých subjektů (národních certifikačních autorit) s IDA. Mezi subjekty se předávají opět důležité relevantní informace. Předávaný důvěryhodný seznam aktuálních informací o poskytovatelích jednotlivých certifikačních služeb se nazývá TSL (Trust Status List) a způsob jeho ověření je podrobně popsán v draftu standardu ETSI TS STF 220-1 (Draft ETSI TS STF 220-1 V0.1.5bis, 2002-12, Requirements for Trust Service Provider status information). Na obrázku č.3 je základní schéma využití TSL při ověření elektronické transakce.



Obr č.3 – Schéma využití TSL při ověření elektronické transakce

Tento draft standardu ETSI se stal základem pro dokument předpisové základny IDA, který shrnuje požadavky na důvěryhodnou komunikaci mezi můstkovou autoritou a jednotlivými národními certifikačními autoritami. Dokument vyšel ve formě doporuční teprve nedávno a to 12.9.2003 (A bridge certification authority for Europe's public administrations - Trust List Usage Recommendations).

Do sdružení IDA mohou být přijímány pouze ty certifikační autority, které byly schváleny podle jednotlivých národních legislativ jako důvěryhodné pro komunikaci se státní správou. V případě České republiky by to tedy mohla být pouze autorita, která vydává kvalifikované certifikáty a získala ve správním řízení akreditaci.

Odpovědnost za důvěryhodnost nově přijaté certifikační autority nenese můstková autorita, ale příslušný národní regulační orgán, který schválil, že certifikační autorita (zjednodušeně) odpovídá Směrnici 1999/93/ES o zásadách Společenství pro elektronické podpisy.

Z prezentací a informací, které jsou dostupné na webu, je zřejmé, že politika můstkové autority IDA ještě není zcela hotova. Při přípravě certifikační politiky dochází mezi jednotlivými členy Společenství k názorovým střetům na její postavení a přesnou podobu. Jedno je jisté (v tom se všichni diskutující shodují): tato autorita musí vzniknout, být funkční a bude hrát rozhodující úlohu v elektronické komunikaci v rámci státní správy EU a měla by být využita v projektu e-Europe 2005.

Závěr

Budování rozsáhlých můstkových autorit je nutností a je další vývojovou fází ve vytváření a propojování jednotlivých PKI. Představa budování osamocené certifikační autority, ať již pouze pro interní potřebu nebo pro blíže nespecifikovanou množinu uživatelů certifikátů, je již překonána.

Z tohoto důvodu je nutné sledovat tento obecný trend a připravit se na vstup do těchto nebo obdobných struktur.

Literatura

[1] Vondruška, P.: Navázání vztahu důvěry mezi certifikačními autoritami, DSM 5/2003, Praha

[2] Vondruška, P.: Vztah důvěry mezi můstkovými certifikačními autoritami, DSM 6/2003, Praha

[2] Vondruška,P: Topologie certifikačních autorit, Crypto- World 11/2002

[4] Dočkal, J.: Federální PKI v USA, DSM 3/2000, Praha

[5] http://www.cio.gov/fpkipa

[6] http://www.bridge-ca.org/

[7] http://europa.eu.int/ISPO/ida/

[8] http://www.noie.gov.au/projects/confidence/Securing/Gatekeeper.htm

[9] ETSI:http://portal.etsi.org/sec/el-sign.asp

[10] CEN: http://www.cenorm.be/isss/CWAs/cwalist.htm

C. Kryptografie a normy - Digitální certifikáty
Požadavky na politiku poskytovatele, který vydává atributové certifikáty, které lze používat spolu s kvalifikovanými certifikáty (Technical report ETSI 102 158)
Část 1.

Jaroslav Pinkava, PVT a.s.

1. Úvod

V říjnu loňského roku byl vydán nový dokument *ETSI - Electronic Signatures and Infrastructures (ESI). Requirements for role and attribute certificates.* (lit. [1]). V dokumentu [3] - ETSI 102 044 - Requirements for role and attribute certificates, o jehož obsahu pojednávaly předchozí dva díly seriálu byla provedena identifikace souboru požadavků, které by následně byly základem chystané normy pro požadavky na politiku pro vydávání atributů. A to to ať již jsou atributy vydávány atributovými autoritami či certifikačními autoritami - jako součást atributového certifikátu či jako jedno z rozšíření digitálního certifikátu.

Cílem navazujícího dokumentu ETSI 102058 je specifikace základních požadavků politiky na prováděcí směrnice atributových autorit vydávající atributové certifikáty, které lze používat pro podporu kvalifikovaných elektronických podpisů a jsou tedy dostupné pro používání veřejností a jsou přiřazovány ke kvalifikovaným certifikátům podporujíce tak certifikační politiku "QCP public + SSCD".

2. Některé definice a zkratky

AA - atributová autorita (Attribute Authority);
AC - atributový certifikát (Attribute Certificate);
ACP - atributová certifikační politika (Attribute Certificate Policy) - soubor pravidel, která stanoví, jak je atributový certifikát použitelný v rámci nějaké konkrétní komunity a/nebo třídy aplikací se společnými bezpečnostními požadavky nebo, která stanoví základní pravidla pro registraci, doručení a odvolání atributů obsažených v atributových certifikátech;
ACPS - atributová certifikační prováděcí směrnice (Attribute Certification Practice Statement), obsahuje postupy, které atributová autorita používá při vydávání atributových certifikátů;
ACDS - atributová certifikační veřejná směrnice (Attribute Certification Disclosure Statement) - doplněk dokumentů ACP a ACPS, zjednodušený dokument, který má za cíl pomoci uživatelům atributových certifikátů přijímat rozhodnutí;
ACRL - seznam odvolaných atributových certifikátů (Attribute Certificate Revocation List);
AGA - zdroj atributů (v dokumentu TR 102 044 byl nazýván autorita vydávající atributy (Attribute Granting Authority);
CA - certifikační autorita (Certification Authority);
CSP - poskytovatel certifikačních služeb (Certification Service Provider);
PKC - certifikát veřejného klíče (Public Key Certificate);
PKI - infrastruktura veřejných klíčů (Public Key Infrastructure);
QC - kvalifikovaný certifikát (Qualified Certificate).
SSCD - prostředek pro bezpečné vytváření el.podpisu (Secure Signature Creation Device)

kvalifikovaný elektronický podpis - zaručený elektronický podpis založený na kvalifikovaném certifikátu a který je vytvořen prostřednictvím prostředku pro bezpečné vytváření el. podpisu (SSCD);

subjekt - entita identifikovaná v AC jako držitel atributů obsažených v certifikátů;

klient - entita, která je zákazníkem atributové autority.

3. Východiska

Atributová autorita certifikuje atributy prostřednictvím vydávání atributových certifikátů. Předtím však (a atributová autorita za to odpovídá) je nezbytné provést ověření, že v době registrace atributu je příslušný jedinec oprávněným nositelem tohoto atributu. Atributová autorita je poskytovatel certifikačních služeb (ve smyslu Směrnice EU o el.podpisu 1999/93/EC), který vydává atributové certifikáty. AA je zodpovědná za poskytování příslušných certifikačních služeb. Může využívat jiné strany k provádění části těchto služeb, vždy však má celkovou odpovědnost a zabezpečuje, že jsou naplněny požadavky politiky (identifikované v tomto dokumentu - ETSI TS 102 158).

Atributová autorita - následné rozlišení jednotlivých služeb je provedeno kvůli objasnění příslušných požadavků na politiku AA a neznamená žádné podmínky na členění implementace AA).

Akviziční služba:

A1) politika její činnosti je součástí politiky AA;

A2) přijímá a dle politiky vyhodnocuje žádosti o atributový certifikát (popř. posoudí další aspekty žádosti, jako např. zda byla provedena požadovaná platba atd.);

A3) pokud žádost splňuje požadavky politiky, zašle požadavek na AC službě pro generování certifikátů;

A4) přijme vygenerovaný certifikát od služby pro generování certifikátů (pokud není předáván prostřednictvím služby pro šíření);

A5) zašle atributový certifikát klientovi;

Služba pro generování certifikátů:

G1) přijímá požadavky na generování certifikátů;

G2) vygeneruje požadovaný atributový certifikát, dle politiky AA tento certifikát bude obsahovat formulace atributů, certifikát podepíše podpisovým klíčem AA (v politice AA musí být popsán způsob práce s tímto klíčem, jeho životní cyklus – generování, způsob uložení, ochrana, doba platnosti atd.);

G3) odešle vygenerovaný atributový certifikát- jsou možné dvě cesty – buď přes akviziční službu nebo přes službu pro šíření AC.

Služba registrace atributů (Atribute Granting Authority)

R1) politika její činnosti je součástí politiky AA;

R2) přijímá požadavky na registraci atributů (tady bude třeba říci, kdo k tomuto má oprávnění a zakotvit to v politice), atributy verifikuje a registruje;

R3) seznam registrovaných atributů slouží službě pro generování AC (nelze vygenerovat atributový certifikát, který by obsahoval jiný atribut než jeden z těch, které jsou zde registrovány);

Služba pro šíření :

D1) přijímá vygenerované atributové certifikáty;
D2) předává AC klientovi;
D3) předává AC ověřovateli (se svolením klienta);
D4) služba šíří také ujednání a podmínky AA, publikovanou politiku a prováděcí směrnici AA (klientům, spoléhajícím se stranám);

Služba pro správu odvolání atributů:

S1) zpracovává žádosti a zprávy, které se týkají odvolání (pozastavení) AC pocházející od klientů resp. jiných oprávněných subjektů a určí jaká má být podniknuta činnost. Výsledky činnosti této služby jsou distribuovány prostřednictvím služby pro revokační statut;

Služba pro revokační statut AC:

RS1) poskytuje informace o revokačním statutu AC ověřovatelům (spoléhajícím se stranám). Služba může probíhat v reálném čase (OCSP) nebo založená na ACRL (seznam odvolaných atributových certifikátů), které je v pravidelných intervalech obnovováno.

Poznámka: Subjekty mohou tedy získávat atributy dvěma způsoby - pomocí akviziční služby resp. prostřednictvím služby pro šíření.

4. Atributové certifikační politiky

V dokumentu jsou specifikovány dvě atributové certifikační politiky, které jsou vhodné pro použití v návaznosti na kvalifikované certifikáty. Tyto dvě politiky mají následující identifikátory:

1) Klientem je subjekt (klientem je buď sám subjekt nebo je jím osoba jednající jménem tohoto subjektu)

itu-t(0) identified-organization(4) etsi(0) attribute-certificate-policies(2158) ac-policy-identifiers(1) subject-as-subscriber(1)

- při použití tohoto identifikátoru mohou být do AC umístěny pouze atributy, které byly registrovány subjektem.

2) Klientem je AGA

itu-t(0) identified-organization(4) etsi(0) attribute-certificate-policies(2158) ac-policy-identifiers(1) aga-as-subscriber(2)

- při použití AGA registračního identifikátoru mohou být do AC umístěny pouze ty atributy, které byly registrovány AGA.

AA může podporovat jednu z těchto politik či obě dvě současně.

5. Závazky a odpovědnost

A. Závazky klienta:

Prostřednictvím smlouvy AA musí zavázat klienta, že bude plnit následující závazky:

a) bude sdělovat AA přesné a úplné informace dle požadavků politiky AA, speciálně ve vztahu k registraci;
b) bez bezdůvodných průtahů sdělí AA, zda nastal některý z následujících momentů:
- nepřesnost informací udaných při registraci oznámená klientovi;
- změna informací udaných při registraci oznámená klientovi.

B. Závazky subjektu:

Prostřednictvím smlouvy AA musí zavázat klienta, že se dohodne se subjektem v tom smyslu, že konání subjektu je omezeno na:
- používání AC čistě za účelem, který je specifikován v ACPS;
- subjekt sdělí klientovi bez bezdůvodných průtahů, pokud je v obsahu AC nepřesnost - z jakéhokoliv důvodu - včetně změny vlastníka atributu.

C. Informace spoléhajícím se stranám:

ACDS musí obsahovat text, který říká, že pokud má být opodstatněný důvod spoléhat se na atributový certifikát, pak:
a) je nezbytné ověřit platnost, pozastavení nebo odvolání atributového certifikátu prostřednictvím informace o současném revokačním statutu spoléhající se stranou (mohou existovat zpoždění při distribuci informací o revokačním statutu)
b) vzít do úvahy jakákoliv omezení pro použití atributových certifikátů, která jsou obsažena buď přímo v AC nebo v dodaných podmínkách a
c) použít jakékoliv jiné preventivní opatření, které je popsáno ve smlouvě či na jiném místě.

AA vydávající atributové certifikáty odpovídá stranám, které se zdůvodněně spoléhají na atributové certifikáty. AA ve své ACPS specifikuje své odpovědnosti a jak tyto odpovědnosti pokrývá.

V druhé části článku budou popsány požadavky, které se týkají atributové certifikační prováděcí směrnice.

5. Literatura

[1] Electronic Signatures and Infrastructures (ESI); Policy requirements for Certification Service Providers issuing attribute certificates usable with Qualified certificates (ETSI TS 102 158, V.1.1), http://portal.etsi.org/esi/el-sign.asp

[2] rfc3281: An Internet Attribute Certificate Profile for Authorization

[3] Electronic Signatures and Infrastructures (ESI); Requirements for role and attribute certificates, ETSI TR 102 044, v1.1.1, December 2002

[4] J. Pinkava: Politika pro vydávání atributových certifikátů - požadavky, část 1+2, Crypto-World 10,11/2003

D. Archivace elektronických dokumentů
Část 2.
Jaroslav Pinkava, PVT, a.s.

1. Úvod

V minulém části (Crypto-World 11/2003) jsme informovali o tom, že byla zahájena činnost pracovní skupiny IETF: Long-Term Archive and Notary Services (ltans) - http://ltans.edelweb.fr/ . Jako součást této informace byl podán přehled úvodního draftu skupiny - draft-ietf-ltans-reqs-00.txt. V současné době existuje druhá verze tohoto draftu - http://ltans.edelweb.fr/draft-ietf-ltans-reqs-01.txt - úpravy jsou však jen velice dílčí (jsou zde podrobněji specifikovány některé požadavky).

V tomto pokračování se budeme věnovat materiálu českých autorů - *Libor Dostálek, Marta Vohnoutová* (PVT a.s) : *Long Term Archive Architecture* (lit. [1]).

2. Proč, co a jak archivovat

Po řadě úvodních poznámek, které se zabývají i některými historickými návaznostmi (archivace klasických papírových dokumentů) a potřebou archivovat některé důležité elektronické dokumenty (uvedeny jsou příklady) diskutují autoři kriticky některé nedávno navržené postupy (rfc.3126 resp. ETSI TS 101 733).

Pojem *důvěryhodného archivu,* tím je rozuměna autorita, kam předáme naše (digitální) dokumenty a věříme, že tyto dokumenty nebudou pozměněny, ztraceny a neoprávněným osobám nebude povolen přístup k těmto dokumentům. Pokud je dokument digitálně podepsán, důvěryhodný archiv tento podpis ověří (při převzetí dokumentu), pak digitální podpis by měl zůstat v platnosti také následně při jeho vyzvednutí z archivu. Autoři dále se zabývají otázkou nakolik je tato představa reálná. Na základě proběhlé diskuse s dnešními faktickými archiváři soudí, že ve skutečnosti žádný archiv nelze považovat za absolutně důvěryhodný. Archivy jsou vlastně pouze úložišti dokumentů. Pouze soud může vynést výrok o pravosti nějakého konkrétního dokumentu.

Při archivaci digitálních dokumentů je jednou ze základních otázek problém použitého formátu elektronického dokumentu a migrace takovéhoto formátu v rámci různých platforem. Nevhodný je proto například formát MS Word, naopak pro zachování stálé hodnoty dokumentu je vhodné používat obyčejný textový formát. Nezbytné je rovněž zabývat se formátem podporovaných digitálních podpisů (dnes PKCS#7 nebo XML).

3. Archivované dokumenty

Autoři rozlišují tři typy digitálních dokumentů:

- dokumenty bez digitálních podpisů a časových značek;
- digitálně podepsané dokumenty (včetně těch co obsahují pouze časové razítko);
- oskenované dokumenty;

Tyto typy dokumentů se mohou stát součástí archivu. Zde k nim může být přidána časová značka, resp. digitální podpis. Důležité je rovněž uspořádání dokumentů v archivu tak, aby následně s nimi bylo možné v případě potřeby spolehlivě pracovat. Z uživatelského hlediska jsou pro práci s archivem hlavními následující funkce:

- ukládání dokumentu do archivu a získání důvěryhodného potvrzení této skutečnosti;
- skartování dokumentu;
- vyhledávání dokumentu včetně příslušných dig.podpisů a časových razítek;
- zrušení celého archivu (např. vzhledem k úmrtí).

Tedy samotný archiv musí umět vydávat některá potvrzení, musí být funkční z hlediska samotného ukládání dokumentů (tuto vlastnost lze samozřejmě rozmělnit do dalších podrobností) a obdobně být funkční i z hlediska vyhledávání dokumentů a jejich vydávání oprávněným osobám. Jako vhodný přístupový protokol po vhodné modifikaci doporučují autoři protokol TAP.

Ve zbývající části materiálu diskutují autoři použitelné formáty (formát CMS, jiné formáty jako TIFF), dále vlastnosti a využitelnost celé řady existujících dokumentů normativního typu (rfc.3126, rfc 3161, rfc.3029, DVC dle 3026, rfc.3281).

Literatura:

[1] Libor Dostálek, Marta Vohnoutová: Long Term Archive Architecture
[2] webovská stránka ltans: http://ltans.edelweb.fr/ .
[3] Long-term Archive Service Requirements draft-ietf-ltans-reqs-01.txt

E. ETSI a CEN/ISSS - nové normativní dokumenty
Jaroslav Pinkava, PVT, a.s.

V posledním čtvrtletí roku 2003 se na webovském portálu ETSI (http://portal.etsi.org/esi/el-sign.asp) objevilo několik nových dokumentů.

O dokumentu **TS 102 158** pojednává jiný článek autora (toto a následující číslo Crypto-Worldu) - jedná se o materiál definující požadavky na základní dokumenty poskytovatele certifikačních služeb, který bude vydávat atributové certifikáty ve spojení s využíváním kvalifikovaných certifikátů. Těmito dokumenty jsou Certifikační politika, Certifikační prováděcí směrnice a Certifikační veřejná směrnice (v originále certification disclosure statement).

Souběžně s tímto dokumentem se v říjnu objevil materiál **TS 102 231** - Harmonized TSP status information. Cílem dokumentu je poskytnout harmonizovaný postup, kterým schémata vykonávající dohlížitelskou funkci vzhledem k důvěryhodným službám a jejich poskytovatelům mohou zveřejňovat informace o těchto službách a také o důvěryhodných poskytovatelích služeb, nad kterými současně vykonávají resp. v minulosti vykonávali dozor.

V prosinci 2003 byla vydána inovovaná verze materiálu k formátům elektronických podpisů - **TS 101 7333 v.1.5.1.** Toto je rozsáhlý dokument specifikující formáty elektronických podpisů zejména z hlediska dlouhodobé platnosti takovýchto elektronických podpisů. Dřívější dokument byl nyní rozdělen na dva - současná verze se věnuje již pouze aspektům formátů elektronických podpisů, aspektům, které se týkají politik pro vydávání el. podpisů se věnuje souběžně vydaný dokument **TR 102 272** - ASN.1 format for signature policies.

Konečně v lednu 2004 se objevil (jako **draft ETSI TS 102 280**) materiál X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons. Jedná se o profil jak kvalifikovaných certifikátů, tak i o profil "obyčejných" certifikátů a to pro takové certifikáty, které jsou vydávány *fyzickým* osobám. Cílem specifikace je primárně umožnit interoperabilní zpracování a zobrazování informace obsažené v certifikátech. V příloze A jsou shrnuty důležité odkazy na normativní dokumenty obsahující příslušné podmínky týkající se profilu certifikátu.

Také v rámci pracovní skupiny CEN/ISSS (od loňského roku jsou dokumenty skupiny zveřejňovány na nové adrese - http://www.uninfo.polito.it/WS_Esign/docs.htm) bylo zveřejněno několik nových materiálů.

Prvním z nich je příručka k verifikaci elektronických podpisů (**CWA 14171** - General Guideliness for Electronic Signature Verification) - oproti předcházející verzi, která neprošla hlasováním, zde však nedošlo k žádným úpravám.

Následují tři ochranné profily pro:

- kryptografický modul pro podpisové operace PCS se zálohováním (**CWA 14167-2** - Cryptograpic Module for CSP Signing Operations with Backup - Protection Profile CMCSOB-PP)
- kryptografický modul pro podpisové operace PCS (**CWA 14167-4** - Cryptograpic Module for CSP Signing Operations - Protection Profile CMCSO-PP)

- kryptografický modul pro služby CSP generování klíče (**CWA 14167-3** - Cryptographic Module for CSP Key Generation Services - Protection Profile - CMCKG-PP);

Dva profily pro totéž TOE (kryptografický modul pro podpisové operace PCS) vznikly v důsledku nezbytnosti popsat obě situace (modul se zálohováním a bez zálohováním) ve shodě s podmínkami dokumentu Common Criteria 2.1. Oba ochranné profily prošly úspěšně evaluací a byly certifikovány.

V případě, že poskytovatel certifikačních služeb zároveň poskytuje službu generování klíče, jsou v dokumentu CWA 14167-3 definovány podmínky, které musí splňovat kryptografický modul obstarávající tuto službu.
Dále vyšel draft, který bude zajímat především právníky (ale nejenom je). Týká se důkazní hodnoty elektronických podpisů (Evidential Value of Electronic Signatures, **WSES_N_O383**). Je zde podrobně rozebírána celá řada situací, které vznikají při používání elektronických podpisů z hlediska příslušných právních aspektů. Autoři přitom vychází ze situací, které jsou dány existujícími technologiemi a používanými normativními dokumenty a uvádí jejich právní dopady.

Konečně to jsou dva díly materiálu zabývajícího se vlastnostmi aplikačního rozhraní pro čipové karty, které jsou používány jako prostředek pro bezpečné vytváření elektronických podpisů. První z nich (**CWA 14890**-1:2004, Application Interface for smart cards used as Secure Signature Creation Devices - Part 1 - Basic requirements) obsahuje ve své rozšířené verzi (předcházející se objevila v první polovině loňského roku) základní požadavky na toto rozhraní. Druhý díl (Application Interface for smart cards used as Secure Signature Creation Devices - Part 2 - Additional services - **WSES_N_O393**) se pak zabývá dalšími službami, které mohou fungovat v rámci tohoto rozhraní.

F. Letem šifrovým světem
(připravil Pavel Vondruška)

I. Kolik stojí PKI?

Odpověď můžete nalézt v dokumentu General Accounting Office (Information Security: Status of Federal Public Key Infrastructure Activities at Major Federal Departments and Agencies, http://www.gao.gov/new.items/d04157.pdf). Tento dokument byl publikován koncem roku 2003 a jsou v něm k dispozici předběžné rozpočty na PKI za rok 2003 ve dvaceti čtyřech vybraných odvětvích USA (obrana, zdravotnictví, školství, doprava,…) .

II. WAPI - nový čínský kryptografický standard zabezpečení pro Wi-Fi

Všechny adaptéry pro Wi-Fi prodávané v Číně budou muset od 1.6.2004 obsahovat šifrovací technologii WAPI. Čínský standardizační úřad SAC (Standardization Administration of China) schválil v květnu 2003 vlastní národní normu GB15629.11-2003. Součástí normy je standard pro kryptografické zabezpečení - označovaný jako Wired Authentication and Privacy Infrastructure (WAPI). Povinné použití šifrování při využívání bezdrátové sítě je jistě přínosem, problematické je pouze použití jediného kryptografického standardu bez možnosti výběru. Diskusi vyvolává především to, že se jedná o standard, který doposud nebyl podroben důkladné bezpečnostní analýze.

O tom, že by v tomto algoritmu mohla být zadní vrátka, se najde na Internetu několik spekulativních článků. Jeden takový dobře napsaný (ač v některých závěrech poněkud diskutabilní) článek na toto téma najdeme i na českém serveru.

Petr Nachtmann : Čína přichází s vlastní verzí šifrování pro Wi-Fi, následky mohou být dalekosáhlé**,** http://mobil.idnes.cz/mobilni_komunikace/wifi/wifiwapicina031215.html .

III. Příručka „pro řešení incidentů“ SP 800-3 nahrazena

Na adrese http://csrc.ncsl.nist.gov/publications/nistpubs/800-61/sp800-61-pdf.zip lze stáhnout nově dokončenou příručku "Computer Security Incident Handling Guide. Příručka nahrazuje příručku SP 800-3 "Establishing a Computer Security Response Capability.

Dle citace: Publikace má za cíl pomoci existujícím i nově ustanovovaným týmům, které zodpovídají za řešení incidentů, odpovídat efektivně a dostačujícím způsobem na širokou škálu incidentů. Konkrétně jsou v publikaci diskutovány následující okruhy:
1) vytváření kapacit pro řešení bezpečnostních incidentů;
2) ustavení politik a procedur pro řešení incidentů;
3) jakou má mít strukturu tým pro řešení incidentů;
4) jak incidenty řešit - od počáteční přípravy až po závěrečném vytěžení získaných zkušeností.

Dále publikace diskutuje kroky jako: prevence, příprava, kontrola, eradikace a obnova - pro řešení široké škály incidentů, jako jsou: odepření služby, kód softwaru obsahující nějaký typ útoku, neoprávněný přístup, nepatřičné použití, incidenty s více komponentami a dále potenciální scénáře, které si lze ověřit v rámci přípravy na větší incidenty.

IV. Najdete v archivu IACR

V rozsáhlém elektronickém archívu IACR (International Association for Cryptologic Research) Cryptology ePrint archive (http://eprint.iacr.org/index.html) můžete od 10.1.2004 nalézt aktualizovaný příspěvek známého českého kryptologa Tomáše Rosy - *Tomas Rosa*: Key-collisions in (EC)DSA: Attacking Non-repudiation (http://eprint.iacr.org/2002/129/) . Autor do své starší práce zapracoval některé myšlenky, které zazněly v referátu o k-kolizích předneseného na Rump Session na Crypto 2002. Velice zajímavý problém autor nastínil ve své práci v odstavci 2.2, kde naznačuje „kacířskou" myšlenku, že (zjednodušeně) zaručený elektronický podpis (advanced electronic signature) nelze zajistit pomocí digitálního podpisového schématu, neboť by nemusela být splněna jedna se základních vlastností zaručeného elektronického podpisu a to, že elektronický podpis je jednoznačně spojen s podepisující osobou (právě vzhledem k možným kolizím).

V. Chcete získat peníze na výzkumný úkol z oblasti steganografie?

U.S. Air Force (USAF) vypsal začátkem ledna dlouhodobé výzkumné úkoly. Mezi nimi je i úkol, který se má zabývat automatickou detekcí steganograficky předávaných informací (AF04-T008, Automated Detection of Steganographic Content). Předpokládá se využití výsledků při rozsáhlém scanování příloh e-mailů a souborů, které jsou volně ke stažení. Součástí úkolu má být především vypracování metody, která umožní detekovat, že v předávaném dokumentu je steganografickými metodami (i proprietárními) ukrytá informace.

Více lze nalézt např. v článku : "USAF Wants To Find Steganographic Content" http://slashdot.org/article.pl?sid=04/01/10/2358247

VI. Jak se zbavit nastavení ochrany heslem dokumentů MS Word

V článku je uvedeno, jak dokument napsaný v MS Wordu s nastavenou ochranou heslem proti neautorizovaným změnám obsahu (postup nastavení v české verzi : Nástroje / Zámek/ Heslo) lze této ochrany velice jednoduchým způsobem zbavit http://www.securityfocus.com/archive/1/348692/2004-01-02/2004-01-08/0 .

VII. Konference ZNALOSTI 2004

Organizátoři Vás srdečně zvou k účasti na 3. ročníku interdisciplinární konference, věnované aktuálním problémům získávání, zpracování, zpřístupňování a využívání znalosti.
Termín konaní konference: 25.2. - 27. 2. 2004
Místo konaní konference: Hotel SANTON, Brno
Podrobné informace viz: www.fi.muni.cz/znalosti2004/
Pozor: 29.1.2004 - uplyne termín možnosti redukovaných plateb.

VIII. O čem jsme psali v lednu 2000 - 2003

Crypto-World 1/2000

Crypto-World 1/2001

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

Crypto-World 1/2002

Crypto-World 1/2003

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

G. 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://crypto-world.info

2. Registrace / zrušení registrace

Zájemci **o zasílání** tohoto sešitu se mohou zaregistrovat pomocí e-mailu na adrese na e-mail pavel.vondruska@crypto-world.info (předmět: Crypto-World) nebo použít k odeslání žádosti o registraci formulář na http://crypto-world.info . 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@crypto-world.info (předmět: ruším odběr Crypto-Worldu!) nebo opět použít formulář na http://crypto-world.info . 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@crypto-world.info
pavel.vondruska@post.cz
pavel.vondruska@ct.cz