Normy a mezinárodní doporučení

v oblasti elektronického podpisu a kryptografie

(*Jaroslav Pinkava, leden 2001)*

Obsah

1. Úvod

Dnešní kryptografie prochází v období posledních pětadvaceti let bouřlivým vývojem. Podstatně vzrostla mohutnost jejího záběru. Vyvinul se nový teoretický aparát, ale i zásadním způsobem se změnily i oblasti, ve kterých je kryptografie aplikována. Klíčovým momentem se stávají situace, kdy aparát kryptografie je zapotřebí využívat v rozsáhlých výpočetních sítích s množstvím jednotlivých účastníků.

Oproti klasickým užitím kryptografie (vojenství, diplomacie) zde dochází posunu především v charakteru požadavku na jeden základní moment při vlastním šifrování. Tím je utajení používaného kryptografického algoritmu. Jistě – potenciální protivník má při luštění zašifrované korespondence význačně ztíženou roli, pokud ani neví jaký algoritmus byl pro šifrování použit. Avšak tento moment utajení použitého algoritmu se při současných aplikacích stává nereálným. Aby se v rozsáhlých sítích mohli utajeně domluvit v zásadě libovolní dva účastníci této sítě, je zapotřebí, aby prostředky zabezpečující ochranu informace při přenosu, zabezpečující také např. vzájemnou autentizaci těchto účastníků, byly nějakým způsobem unifikovány. Takováto unifikace těchto prostředků je pak vlastně smyslem vytváření kryptografických norem a návazných doporučení. Například pro řešení takových aplikací jako jsou prostředky pro elektronický podpis (např. v rámci e-governmentu), prostředky pro bezpečný elektronický obchod atd. je existence obecných norem a doporučení nezbytná.

Historicky, pokud je autorovi známo, první takovouto (veřejnou) normou byla americká vládní norma DES z roku 1977. V brzké době na tuto normu navázali další dokumenty specifikující další postupy související s využíváním algoritmu blokové šifry, který je v DES definován. Posléze i např. se zaváděním prostředků asymetrické kryptografie se objevila celá řada vládních ale i průmyslových doporučení, která řeší dílčí okruhy kryptografické problematiky.

Předkládaný materiál má za cíl provést čtenáře množstvím dnes již existujících norem v oblasti kryptografie a elektronického podpisu, ukázat oblasti, kterých se tyto normy týkají a trochu podrobněji objasnit jejich smysl.

Samozřejmě, dnes existuje norem, které se nějakým způsobem kryptografie dotýkají, nepřeberné množství a dost těžko se hledají i kriteria, pomocí kterých by se tyto normy (a související doporučení) daly utřídit. Možná by se dalo začít i nějakou diskusí na téma samotného pojmu „norma“. Avšak pro pojetí tohoto materiálu bych se chtěl orientovat především na obsahovou stránku problematiky (a nikoliv formální). Vzniká otázka, jakou tedy zvolit konkrétní cestu výkladu.

Poznámka: Pokud čtenář má zájem vytvořit svoji vlastní normu (pro oblast kryptografie) určitě by se měl nejprve seznámit s doporučeními známého vývojáře v oblasti kryptogra-fického softwaru Petera Gutmanna (http://www.cs.auckland.ac.nz/~pgut001/pubs/pfx.html).

Daný materiál má tedy za cíl provést určitý analytický přehled situace v oblasti existujících a používaných norem v kryptografii a v návaznosti na to i pro elektronický (digitální) podpis. V materiálu budou popsány jak normy pro základní kryptografické algoritmy – symetrická kryptografie, tak také i normy pro asymetrické kryptografické algoritmy. Problematika se týká ovšem i všech návazných problematik jako je např. výměna tajných klíčů pro symetrickou kryptografii s využitím aparátu asymetrické kryptografie, vytváření digitálních podpisů ale i celé škály souvisejících norem (technický pomocný aparát – jako jsou např. hashovací funkce, problematika časových značek, nadstavbový aparát – kryptografické protokoly, digitální certifikáty, profily certifikátů, práce poskytovatelů certifikačních služeb atd.).

První otázkou, která při zpracování materiálu tohoto typu vzniká, je jaký zvolit způsob členění těchto norem. Existují dvě základní využitelné cesty. První z nich je rozčlenění norem dle cesty jakým byly tyto normy vydány, tj. fakticky dle vydávající strany. Tento způsob členění je použit v 2. kapitole. Byl také zvolen jako základní způsob vyčíslení norem v přehledu.

Přitom je třeba vzít do úvahy, že právě toto členění ukazuje dnešní vztah mezi způsobem vytváření a využívání norem v dané oblasti. Tyto normy lze takto vlastně rozčlenit na normy de jure a normy de facto. Do první třídy spadají normy vydávané takovými velkými organizacemi jako je ISO, ANSI, americké vládní instituce, evropské oficiální struktury atd. Tyto normy mají oficiální statut a tedy i jaksi z právního hlediska jsou závaznější. Na druhou stranu poměrně složitá a časově náročná cesta při jejich schvalování příslušnými orgány vede k určité nepružnosti, setrvačnosti. Protože dynamika norem v daných oblastech je v současné době opravdu vysoká, může být potom tato malá pružnost oficiálních norem určitou překážkou.

Druhou třídu norem (de facto normy) tvoří dlouhá řada dokumentů, které jsou vydávány byť třeba oficiálními organizacemi jako je IETF, mají však určitou zjednodušenou cestu při jejich formování. Tyto dokumenty podléhají obvykle veřejné diskusi ve formě tzv. draftu a pak jsou následně předkládány pro využití (IETF označuje vyledné dokumenty jako rfc – request for comment). V analyzovaných oblastech v tomto směru sehrávají velkou roli např. normy PKCS na jejichž vydávaní se podílí firma RSA Security. Dále jsou to výsledky práce několika skupin v rámci již zmíněné IETF jako jsou openpgp, pkix, smime, xmldsig atd.

Druhou logickou cestou členění takovýchto norem je samozřejmě členění dle jejich obsahového zaměření, tj. např. vydělení norem, které se zabývají algoritmy na bázi eliptických křivek, které slouží k vytváření digitálních podpisů atd. Tato cesta je popsána v kapitole 3. a zde slouží jako určitý doplněk přehledu v kapitole 2.

Integrální součástí materiálu je i pohled na problematiku certifikace a evaluace kryptografických a podpisových prostředků obsažený v kapitole 4.

2. Členění norem dle vydavatele

2.1. IEEE

V letošním roce (září 2000) byla vydána norma

1363-2000 IEEE Standard Specifications for Public Key Cryptography
Print: 228 pages [0-7381-1956-3] [SH94820-NYF]
PDF: [0-7381-1957-1] [SS94820-NYF] .

Tato norma je výsledkem několikaleté práce odborné skupiny IEEE P1363 v problematice asymetrické kryptografie. Jejím obsahem je popis tří základních skupin kryptosystémů s veřejným klíčem:

a) kryptosystémy založené na úloze faktorizace (RSA, Rabin-Williams),
b) kryptosystémy založené na problému diskrétního logaritmu (DSA, Diffie-Hellmanovo schéma pro výměnu klíčů, El-Gamalovo schéma pro šifrování),
c) Kryptosystémy založené na úloze diskrétního logaritmu pro eliptické křivky.

Jednotlivé kryptosystémy jsou zde hluboce rozebrány a popsány i z hlediska návaznosti na potřebné implementační vlastnosti. Materiál představuje z hlediska normotvorné činnosti základní východiska pro všechny navazující třídy norem v oblasti asymetrické kryptografie.

V hlavním dokumentu jsou nejprve uvedeny následující základní pojmy:

Kryptografická rodina (cryptographic family): v normě jsou prezentovány tři základní rodiny kryptografických zobrazení, která jsou založena na následujících (matematicky obtížných) problémech: diskrétní logaritmus v konečném poli (DL), diskrétní logaritmus v grupách eliptických křivek (EC) a na faktorizaci celých čísel (IF).

Parametry systému (**domain parameters):** informace o matematických objektech (jako tělesa či grupy) v jejichž kontextu existují dvojice veřejný a soukromý klíč. Více dvojic klíčů může mít tytéž systémové parametry.

Platné parametry systému (valid domain parameters): taková množina systémových parametrů, která splňuje navíc příslušné specifické matematické požadavky týkající se příslušných parametrů systému pro danou rodinu.

Platný klíč (valid key): klíč (soukromý či veřejný), který splňuje navíc příslušné specifické matematické požadavky klíčů pro danou rodinu.

Platná dvojice klíčů (valid key pair):dvojice veřejný a soukromý klíč, která splňuje navíc příslušné specifické matematické požadavky, kladené na dvojici klíčů pro danou rodinu.

Ověření platnosti (validation): proces, během něhož proběhne ověření platnosti klíče, dvojice klíčů či systémových parametrů.

Základní model:

Následující tříúrovňový model dává potřebnou abstrakci k rozlišení různých typů kryptografických technik:

- Primitivy - základní matematické operace. Tyto historicky vznikly z obtížných problémů teorie čísel. Primitivy samy o sobě nejsou určeny k získání hledané bezpečnosti, ale slouží jako stavební prvky pro schémata.

- Schémata – operace kombinující primitivy a doplňkové techniky (viz dále). Schémata mohou zajistit příslušnou bezpečnost (teoretické hledisko výpočtové složitosti) pokud jsou vhodně aplikována v protokolech.

- Protokoly – posloupnosti operací, které jsou prováděny více stranami za účelem dosažení určitého bezpečnostního cíle. Protokoly mohou dosáhnout požadovanou bezpečnost, pokud jsou správně implementovány.

Primitivy

Norma definuje následující primitivy:

— Odvození tajné hodnoty (Secret Value Derivation Primitives = SVDP) ve schématech pro dohodu na klíči.
— Podpis (Signature Primitives = SP) a verifikace podpisu (Verification Primitives = VP), součásti podpisových schémat.
— Šifrování (Encryption Primitives = EP) a dešifrování (Decryption Primitives = DP), součásti šifrovacích schémat.

Schémata

Norma definuje následující schémata:

— Schéma pro dohodu na klíči (Key Agreement Schemes = KAS), kde dvě strany použijí své dvojice veřejný a soukromý klíč resp. další informaci k vytvoření sdíleného tajného klíče.
— Podpisové schéma s přívěškem (Signature Schemes with Appendix = SSA), ve kterém jedna strana podepíše zprávu svým soukromým klíčem a libovolná jiná strana může ověřit tento podpis užitím zprávy, podpisu a veřejného klíče podepsané strany.
— Podpisové schéma s rozkrytím zprávy (Signature Schemes with Message Recovery = SSR), ve kterém jedna strana podepíše zprávu svým soukromým klíčem a libovolná jiná strana může ověřit tento podpis a rozkrýt samotnou zprávu (pokud podpis je verifikován) užitím podpisu a odpovídajícího veřejného klíče podepsané strany.
— Šifrovací schémata (Encryption Schemes = ES), kde libovolná strana může zašifrovat zprávu užitím veřejného klíče příjímající strany a pouze příjemce může zprávu dešifrovat užitím odpovídajícího svého soukromého klíče. Šifrovací schémata lze použít k dohodě na tajném klíči pro symetrickou kryptografii.

Skupina P1363 v současné době ve své práci pokračuje. Je zpracováván materiál P1363a (amendment), který doplňuje již zpracovaný materiál o navazující kryptografické protokoly. Rovněž tak se rozeběhly práce Public Key Study Group, která si za svůj cíl klade zpracování obdobným způsobem dalších tříd kryptosystémů s veřejným klíčem (v současné době je to např. kryptosystém NTRU).

Některé další podrobnosti lze nalézt v článku J. Pinkava: Eliptické křivky v kryptografii a mezinárodní normy, 7.konference SIS-PCS, březen 2000.
Následující normy IEEE jsou určeny pro kontrolu bezpečnosti výpočetních systémů (Viz kapitola 3.10):

IEEE P1003.1e *POSIX Part 1: System API - Protection, Audit and Control Interfaces (C language)*

IEEE P1003.2c *POSIX Part 2: Shell and Utilities - Protection and Control Interfaces*

2.2. ISO

Následuje jmenovitý seznam známých ISO (International Organization for Standardization - - http://www.iso.ch) norem pro problematiku kryptografie, elektronického podpisu a příbuzných problémů. Názvy norem jiz obvykle částečně charakterizují jejich konkrétní zaměření, přesto je k jednotlivým normám uvedena jejich stručná charakteristika a v kapitole tři pak jsou tyto normy znovu zmiňovány a zařazeny již ke konkrétním okruhům otázek. Jednotlivé normy jsou uvedeny v pořadí dle svého číslování - pro snazší vyhledávání.

- ISO/IEC 7816-1:1998 Identification cards -- Integrated circuit(s) cards with contacts -- Part 1: Physical characteristics
- ISO/IEC 7816-2:1999 Information technology -- Identification cards -- Integrated circuit(s) cards with contacts -- Part 2: Dimensions and location of the contacts
- ISO/IEC 7816-3:1997 Information technology -- Identification cards -- Integrated circuit(s) cards with contacts -- Part 3: Electronic signals and transmission protocols
- ISO/IEC 7816-4:1995 Information technology -- Identification cards -- Integrated circuit(s) cards with contacts -- Part 4: Interindustry commands for interchange
- ISO/IEC 7816-4:1995/Amd 1:1997 secure messaging on the structures of APDU messages
- ISO/IEC 7816-5:1994 Identification cards -- Integrated circuit(s) cards with contacts -- Part 5: Numbering system and registration procedure for application identifiers
- ISO/IEC 7816-5:1994/Amd 1:1996
- ISO/IEC 7816-6:1996 Identification cards -- Integrated circuit(s) cards with contacts -- Part 6: Interindustry data elements
- ISO/IEC 7816-6:1996/Cor 1:1998
- ISO/IEC 7816-6:1996/Amd 1:2000 IC manufacturer registration
- ISO/IEC 7816-7:1999 Identification cards -- Integrated circuit(s) cards with contacts -- Part 7: Interindustry commands for Structured Card Query Language (SCQL)
- ISO/IEC 7816-8:1999 Identification cards -- Integrated circuit(s) cards with contacts -- Part 8: Security related interindustry commands
- ISO/IEC 7816-9:2000 Identification cards -- Integrated circuit(s) cards with contacts -- Part 9: Additional interindustry commands and security attributes
- ISO/IEC 7816-10:1999 Identification cards -- Integrated circuit(s) cards with contacts -- Part 10: Electronic signals and answer to reset for synchronous cards
  Charakteristika: Norma ISO 7816 je v současné době desetidílný dokument věnující se čipovým kartám - viz odstavec 3.8.

- ISO/IEC 8372, "Information Technology - Modes of Operation for a 64-bit Block Cipher Algorithm"
  Charakteristika: Norma obsahuje módy blokových šifer - ECB, CBC, OFB a CFB, nejsou obsaženy techniky pro úpravy zpráv na potřebnou délku - padding. Módy operací, které jsou popsány v ANSI X3.106 a FIPS Pub 81 jsou speciální případy těchto módů. Norma také pracuje s libovolným 64-bitovým algoritmem blokové šifry (tj. ne pouze s DES).

- ISO/IEC 8731:1987, "Banking - Approved Algorithms for Message Authentication - Part 1: Data Encryption Algorithm (DEA)".
- ISO 9564-1:1991 Banking -- Personal Identification Number management and security -- Part 1: PIN protection principles and techniques
- ISO 9564-2:1991 Banking -- Personal Identification Number management and security -- Part 2: Approved algorithm(s) for PIN encipherment
  Charakteristika: Normy se zabývají problematikou autentizace zpráv a prací s PIN jsou určeny pro bankovnictví.

- ISO/IEC 8824-1:1998, Information Technology – Abstract Syntax Notation One (ASN.1): Specification of Basic Notation. Equivalent to ITU-T Rec. X.680 (1997).
- ISO/IEC 8824-2:1998, Information Technology – Abstract Syntax Notation One (ASN.1): Information Object Specification. Equivalent to ITU-T Rec. X.681 (1997)
- ISO/IEC 8824-3:1998, Information Technology – Abstract Syntax Notation One (ASN.1): Constraint Specification. Equivalent to ITU-T Rec. X.682 (1997).
- ISO/IEC 8824-4:1998, Information Technology – Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 Specifications. Equivalent to ITU-T Rec. X.683 (1997).
- 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). Equivalent to ITU-T Rec. X.690 (1997).
- ISO/IEC 8825-2:1998, Information Technology – ASN.1 Encoding Rules: Specification of Packed Encoding Rules (PER). Equivalent to ITU-T Rec. X.691 (1997).

Charakteristika: Normy popisující syntaxi ASN.1.

- ISO IEC 9594-8/ITU-T X.509, "Information Technology - Open Systems Interconnection - The Directory: Authentication Framework".
  Charakteristika: Klasická norma X.509, v současné době je podstatně doplňována.

- ISO 9735-5:1999 Electronic data interchange for administration, commerce and transport (EDIFACT) -- Application level syntax rules (Syntax version number: 4) -- Part 5: Security rules for batch EDI (authenticity, integrity and non-repudiation of origin)
- ISO 9735-7:1999 Electronic data interchange for administration, commerce and transport (EDIFACT) -- Application level syntax rules (Syntax version number: 4) -- Part 7: Security rules for batch EDI (confidentiality)
- ISO 9735-9:1999 Electronic data interchange for administration, commerce and transport (EDIFACT) -- Application level syntax rules (Syntax version number: 4) -- Part 9: Security key and certificate management message (message type- KEYMAN)

Charakteristika: Dokumenty EDIFACT - jsou to normy pro oblast elektronického obchodu.

- ISO/IEC 9796:1991 Information Technology – Security techniques – Digital signature scheme giving message recovery.
- ISO/IEC 9796-2:1997 Information technology -- Security techniques -- Digital signature schemes giving message recovery -- Part 2: Mechanisms using a hash-function
- ISO/IEC 9796-3:2000 Information technology -- Security techniques -- Digital signature schemes giving message recovery -- Part 3: Discrete logarithm based mechanisms (available in English only)
- ISO/IEC 9796-4 Information Technology – Security techniques – Digital signature schemes giving message recovery – Part 4: Methods based on the Discrete Logarithm,
  Charakteristika: Toto je klasická norma pro digitální podpisy s obnovou zprávy, dnes přepracovávaná. Čtvrtý dokument popisuje jak schémata založená na problému diskrétního logaritmu v prvočíselných tělesech, tak i schémata na bázi eliptických křivek v konečných tělesech.

- ISO/IEC 9797:1994 Information technology -- Security techniques -- Data integrity mechanism using a cryptographic check function employing a block cipher algorithm (available in English only)
- ISO/IEC 9797-1:1999 Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 1: Mechanisms using a block cipher (available in English only)
  Charakteristika: Normy se týkají problematiky neporušenosti, integrity zpráv. Tj. definují aparát pomocí kterého lze pokusy o změnu obsahu zpráv detekovat. Mechnismus je opřen o využití blokové šifry, pomocí nížž se spočte určitá kryptografická ověřovací hodnota (cryptographic check value), která se nazývá Ověřovací kód zprávy - Message Authentication Code (MAC). Mechanizmus výpočtu MAC je obecnější než jsou mechanizmy popsané v normách ISO 8731, ANSI X9.9 a ANSI X9.19. Hlavní rozdíl spočívá v možnosti použití libovolného algoritmu pro blokovou šifru, práce s posledním blokem zprávy a použití (případně) dalších postupů k zesílení vlastností MAC.

- ISO/IEC 9798-1:1997 Information technology -- Security techniques -- Entity authentication -- Part 1: General (available in English only)
- ISO/IEC 9798-2:1999 Information technology -- Security techniques -- Entity authentication -- Part 2: Mechanisms using symmetric encipherment algorithms (available in English only)
- ISO/IEC 9798-3:1998 Information technology -- Security techniques -- Entity authentication -- Part 3: Mechanisms using digital signature techniques (available in English only)
- ISO/IEC 9798-4:1999 Information technology -- Security techniques -- Entity authentication -- Part 4: Mechanisms using a cryptographic check function (available in English only)
- ISO/IEC 9798-5:1999 Information technology -- Security techniques -- Entity authentication -- Part 5: Mechanisms using zero knowledge techniques (available in English only)

Charakteristika: Tato norma v pěti svých částech popisuje různé autentizační techniky. Část 1 popisuje obecný model, část 2 techniky využívající symetrickou kryptografii,

část 3 techniky používající systéma s veřejným klíčem, část 4 používá krypografickou ověřovací funkci (autentizace proběhne tím, že ověřovatel zná příslušný kryptografický klíč) a v páté části jsou popsány techniky opírající se o protokoly s nulovou znalostí (zero knowledge protocols).

- ISO/IEC 9979, "Data Cryptographic Tecniques - Procedures for the Registration of Cryptographic Algorithms".
  Charakteristika: Mezinárodní norma, která specifikuje procedury k registraci kryptografických algoritmů a formáty registračních vstupů (aby bylo možné jednoznačně identifikovat kryptografické algoritmy jejich unikátním jménem).

- ISO/IEC 10116:1997 Information technology -- Security techniques -- Modes of operation for an n-bit block cipher (available in English only)
- Charakteristika: Norma obsahuje módy blokových šifer - ECB, CBC, OFB a CFB, nejsou obsaženy techniky pro úpravy zpráv na potřebnou délku - padding. Módy operací, které jsou popsány v ANSI X3.106 a FIPS Pub 81 jsou speciální případy těchto módů. Norma také pracuje s libovolným n-bitovým algoritmem blokové šifry (oproti ISO/IEC 8372, kde n=64).

- ISO/IEC 10118-1:2000 Information technology -- Security techniques -- Hash-functions -- Part 1: General (available in English only)
- ISO/IEC 10118-2:1994 Information technology -- Security techniques -- Hash-functions -- Part 2: Hash-functions using an n-bit block cipher algorithm (available in English only)
- ISO/IEC 10118-3:1998 Information technology -- Security techniques -- Hash-functions -- Part 3: Dedicated hash-functions (available in English only)
- ISO/IEC 10118-4:1998 Information technology -- Security techniques -- Hash-functions -- Part 4: Hash-functions using modular arithmetic (available in English only)

Charakteristika: Norma se ve svých čtyřech částech zabývá různými typy hashovacích funkcí. První část popisuje obecný model, druhá část se zabývá konstrukcí hashovací funkce z n-bitové blokové šifry (MDC - Manipulation -or Modification- Detection Code). V třetí části jsou specifikovány konkrétní hashovací funkce, jedna s délkou hashe 128 bitů, další s délkou hashe 160 bitů (jsou to RIPEMD-128, RIPEMD 160, SHA-1). Konečně v čvrté části jsou konstruovány dvě hashovací funkce MASH-1 a MASH-2 na základě použití aparátu modulární aritmetiky.

- ISO 10202-1:1991 Financial transaction cards -- Security architecture of financial transaction systems using integrated circuit cards -- Part 1: Card life cycle
- ISO 10202-2:1996 Financial transaction cards -- Security architecture of financial transaction systems using integrated circuit cards -- Part 2: Transaction process
- ISO 10202-3:1998 Financial transaction cards -- Security architecture of financial transaction systems using integrated circuit cards -- Part 3: Cryptographic key relationships
- ISO 10202-4:1996 Financial transaction cards -- Security architecture of financial transaction systems using integrated circuit cards -- Part 4: Secure application modules
- ISO 10202-5:1998 Financial transaction cards -- Security architecture of financial transaction systems using integrated circuit cards -- Part 5: Use of algorithms
- ISO 10202-6:1994 Financial transaction cards -- Security architecture of financial transaction systems using integrated circuit cards -- Part 6: Cardholder verification

- ISO 10202-7:1998 Financial transaction cards -- Security architecture of financial transaction systems using integrated circuit cards -- Part 7: Key management
- ISO 10202-8:1998 Financial transaction cards -- Security architecture of financial transaction systems using integrated circuit cards -- Part 8: General principles and overview

Charakteristika: Norma se zabývá jednotlivými aspekty karet používaných ve finančních transakcích.

- ISO 11568-1:1994 Banking -- Key management (retail) -- Part 1: Introduction to key management
- ISO 11568-2:1994 Banking -- Key management (retail) -- Part 2: Key management techniques for symmetric ciphers
- ISO 11568-3:1994 Banking -- Key management (retail) -- Part 3: Key life cycle for symmetric ciphers
- ISO 11568-4:1998 Banking -- Key management (retail) -- Part 4: Key management techniques using public key cryptosystems
- ISO 11568-5:1998 Banking -- Key management (retail) -- Part 5: Key life cycle for public key cryptosystems
- ISO 11568-6:1998 Banking -- Key management (retail) -- Part 6: Key management schemes

Charakteristika: Norma popisuje doporučené postupy pro klíčové hospodářství v bankovní sféře.

- ISO/IEC 11770-1:1996 Information technology -- Security techniques -- Key management -- Part 1: Framework (available in English only)
- ISO/IEC 11770-2:1996 Information technology -- Security techniques -- Key management -- Part 2: Mechanisms using symmetric techniques (available in English only)
- ISO/IEC 11770-3:1999 Information technology -- Security techniques -- Key management -- Part 3: Mechanisms using asymmetric techniques (available in English only)

Charakteristika: Norma se zabývá různými aspekty při zavádění klíčového hospodářství pro symetrickou a asymetrickou kryptografii (včetně např. využití pojmu třetí důvěryhodné strany).

- ISO 13492:1998 Banking -- Key management related data element (retail)

Charakteristika: Doplněk ISO 11568..

- ISO/IEC TR 13335-1:1996 Information technology -- Guidelines for the management of IT Security -- Part 1: Concepts and models for IT Security (available in English only)
- ISO/IEC TR 13335-2:1997 Information technology -- Guidelines for the management of IT Security -- Part 2: Managing and planning IT Security (available in English only)
- ISO/IEC TR 13335-3:1998 Information technology -- Guidelines for the management of IT Security -- Part 3: Techniques for the management of IT Security (available in English only)
- ISO/IEC TR 13335-4:2000 Information technology -- Guidelines for the management of IT Security -- Part 4: Selection of safeguards (available in English only)

Charakteristika: Norma se zabývá problematikou řízení bezpečnosti informací (IT-

Security management).

- ISO/TR 13569:1997 Banking and related financial services -- Information security guidelines
- ISO/IEC TR 13594:1995 Information technology -- Lower layers security

Charakteristika: Problematika bezpečnosti na nižších vrstvách OSI modelu.

- ISO/IEC 13888-1:1997 Information technology -- Security techniques -- Non-repudiation -- Part 1: General (available in English only)
- ISO/IEC 13888-2:1998 Information technology -- Security techniques -- Non-repudiation -- Part 2: Mechanisms using symmetric techniques (available in English only)
- ISO/IEC 13888-3:1997 Information technology -- Security techniques -- Non-repudiation -- Part 3: Mechanisms using asymmetric techniques (available in English only)

Charakteristika: Norma popisuje různé modely pro zabezepečení problematiky nepopiratelnosti (první část normy je obecného zaměření, druhá čast popisuje využití symetrických technik a třetí část popisuje využití asymetrických technik).

- ISO/IEC WD 14516: 1997 Information technology - Security techniques - Guideliness on the use and management of Trusted Third Party services

Charakteristika: Norma specifikuje problematiku třetí důvěryhodné strany.

- ISO/IEC 14888-1:1998 Information technology -- Security techniques -- Digital signatures with appendix -- Part 1: General (available in English only)
- ISO/IEC 14888-2:1999 Information technology -- Security techniques -- Digital signatures with appendix -- Part 2: Identity-based mechanisms (available in English only)
- ISO/IEC 14888-3:1998 Information technology -- Security techniques -- Digital signatures with appendix -- Part 3: Certificate-based mechanisms (available in English only)

Charakteristika: Norma popisuje řešení problematiky digitálního podpisu v dodatku zprávy.

- ISO/IEC WD 15292: 1998, Protection Profile registration procedures

Charakteristika: Ochranné profily pro objekty dle ISO/IEC 15408..

- ISO/IEC 15401-1 (SC 27 N1892, 11/1997), Information technology - Security techniques - Evaluation Criteria for IT Security - Part 1: Introduction and general model.

Charakteristika: Pravděpodobně starší verze (viz ISO/IEC 15408).

- ISO/IEC 15408-1:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model (available in English only)
- ISO/IEC 15408-2:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional requirements (available in English only)
- ISO/IEC 15408-3:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance requirements (available in English only)

Charakteristika: Norma obsahuje Common Criteria, verze 2.1.

- ISO/IEC WD 15443: 1998, A framework for IT Security assurance
  Charakteristika: Norma popisuje rámec, ve kterém mají probíhat evaluace dle ISO/IEC 15408.

- ISO/IEC WD 15446: 1998, Guide on the production of Protection Profiles and Security Targets
  Charakteristika: Norma popisuje způsob zpracování technické zprávy pro evaluace dle ISO/IEC 15408.

- ISO/IEC WD 15816: 1997, Security information objects

Charakteristika: Dokument popisuje syntaxi pro tzv. Security Information Objects.

- ISO/IEC 15945 Information technology - Security techniques - Specification of TTP services to support the Application of Digital Signatures.

Charakteristika:

- ISO/IEC 15946-1. Information technology - Security techniques - Cryptographic techniques based on elliptic curves - Part 1: General. 1998. Working draft.
- ISO/IEC 15946-2. Information technology - Security techniques - Cryptographic techniques based on elliptic curves - Part 2: Digital signatures. 1998. Working draft.
- ISO/IEC 15946-3. Information technology - Security techniques - Cryptographic techniques based on elliptic curves - Part 3: Key establishment. 1998. Working draft.

Charakteristika: Dle dostupných informací se jedná o draft normy popisující různé aspekty využití eliptických křivek.

- ISO/IEC WD 15947: 1998, IT intrusion detection framework

Charakteristika: Detekce průniků.

- ISO/IEC DIS 17799-1: Information security management. Code of practice for information security management.

Charakteristika:

- ISO/IEC Guide 23:1982 Methods of indicating conformity with standards for third-party certification systems
- ISO/IEC Guide 28:1982 General rules for a model third-party certification system for products
- ISO/IEC Guide 53:1988 An approach to the utilization of a supplier's quality system in third party product certification

Charakteristika: Různé příručky.

2.3. ANSI

Toto jsou normy vydávané institucí American National Standards Institute. Aktuální jsou zde zejména normy X9, z nichž je již dnes celá řada orientována na problematiku kryptografie a elektronického podpisu. Obdobně jako u norem ISO se k nim vracíme v kapitole 3, kde jsou (většina) již tyto normy přiřazeny k jednotlivým tématickým okruhům.

X3: Information processing systems

ANSI X3.92, "American National Standard, Data Encryption Algorithm", 1981.
(to je vlastně DES, v současnosti již určitě bude platná pouze nová verze normy na bázi 3-DES)
ANSI X3.106, "American National Standard, Information Systems - Data Encryption Algorithm - Modes of Operation", 1983.
(dnes již vlastně pouze „historické“ normy).

X9: Financial services

Orgány ANSI jsou rozčleněny do několika výborů, výbor ANSI X9 vyvíjí normy pro finanční průmysl (PIN management, zpracování šeků, elektronický převod plateb atd.). Podvýbory ANSI X9 pak zpracovávají jednotlivé dokumenty.

ANSI X9.8 Accredited Standards Committee X9. -1995*, Personal Identification Number (PIN) Management and Security*
ANSI X9.9 Accredited Standards Committee X9. -1986 (R-1994), *Financial Institution Message Authentication*
(Norma pro autentizaci finančních transakcí, popisovaný algoritmus nese označení DES-MAC a je založen na DES v módu CBC resp. CFB; ISO ekvivalent má číslo ISO 8730 a ISO 8731)
ANSI X9.17 ANSI. *American National Standard X9.17: Financial Institution Key Management (Wholesale).* 1985.
(Norma definuje protokoly pro finanční instituce, které slouží k převodu šifrovacích tajných klíčů symetrické kryptografie. Norma definuje tři hierarchie klíčů. - master key KKM, distribuován manuálně
- key encrypting key KEK, distribuce on-line
- data key KD, distribuovány rovněž on-line.
Norma rovněž definuje formáty zpráv k ustavení nových klíčů - CSM - cryptographic service messages. Dále definuje 3-DES s dvěma klíči, která je určena pro distibuci klíčů a obsahuje rovněž Diffie-Hellmanovo schéma. Doplňující pro tuto normu je ANSI X9.28, která řeší problematiku komunikace a distribuce klíčů ve velkých systémech, kde neexistuje jediné ústřední místo pro distribuci klíčů.)
ANSI X9.19 Accredited Standards Committee X9. *Message Authentication Codes*
(Detailnější verze X9.9, ISO ekvivalent má číslo ISO 9807)
ANSI X9.23 Accredited Standards Committee X9-1988 (R-1995), *Encryption of Wholesale Financial Messages*
ANSI X9.24 Accredited Standards Committee X9-1992, *Financial Services Retail Key Management*
ANSI X9.26 Accredited Standards Committee X9-1990 (R-1996), *Financial Institution Sign-On Authentication for Wholesale Financial Services*

ANSI X9.30 Accredited Standards Committee X9. *Part 1: Public Key Cryptography Using Irreversible Algorithms: Digital Signature Algorithm*
(Norma obsahuje popis algoritmu pro elektronický podpis DSA.)
ANSI X9.30 Accredited Standards Committee X9 *Part 2: Public Key Cryptography Using Irreversible Algorithms: Secure Hash Algorithm (SHA-1)*
ANSI X9.31 Accredited Standards Committee X9. *Public Key Cryptography Using Reversible Algorithms for the Financial Services Industry: Part 1: The RSA Signature Algorithm.*
(Norma obsahuje popis algoritmu pro elektronický podpis RSA, hashovací funkcí je MDC2, práce s adekvátními certifikáty je popsána v ANSI X9.57.)
ANSI X9.42 Accredited Standards Committee X9. *Public Key Cryptography for the Financial Services Industry: Management of Symmetric Algorithm Keys Using Diffie-Hellman*.
(Norma popisuje algoritmus Diffie-Hellmana pro výměnu klíčů.)
ANSI X9.44 Accredited Standards Committee X9. *Management of Symmetric Algorithms Keys Using Reversible Public Key Cryptography*
(Norma popisuje algoritmus RSA pro výměnu klíčů.)
ANSI X9.45 Accredited Standards Committee X9. *Enhanced Management Controls Using Digital Signatures and Attribute Certificates*
ANSI X9.49 Accredited Standards Committee X9. *Secure remote Access to Financial Svcs.* for Fin. Ind.: Guidelines for home banking; threat awareness & countermeasures.
ANSI X9.52 Accredited Standards Committee X9. *Triple Data Encryption Algorithms Modes of Operation*
ANSI X9.55 Accredited Standards Committee X9. *Extensions to Public Key Certificates and CRLs*
ANSI X9.57 Accredited Standards Committee X9. *Certificate Management*
ANSI X9.59 Accredited Standards Committee X9. *Signed payment objects for use in consumer-oriented, account-based transactions* (not limited to the internet).
ANSI X9.62 Accredited Standards Committee X9. *The Elliptic Curve Digital Signature Algorithm*
ANSI X9.63 Accredited Standards Committee X9. *Key Agreement and Key Management Using Elliptic Curve-Based Cryptography*
ANSI X9.65 Accredited Standards Committee X9. *Triple DEA Sec 4.0, Implementation Guidelines and Sec. 5.0 Key Management,*
ANSI X9.66 Accredited Standards Committee X9. *Security of Cryptographic Modules* (based on FIPS 140-1)
ANSI X9.68 Accredited Standards Committee X9.*Digital Certificates for High Transaction Volume Financial Systems*
ANSI X9.70-199x Accredited Standards Committee X9. *Symmetric Key Distribution Using Public Key*
ANSI X9.71 Accredited Standards Committee X9. *Keyed Hash for Message Authentication*
ANSI X9.72-199x Accredited Standards Committee X9.*Peer Entity Authentication Using Public Key*
ANSI X9.73 Accredited Standards Committee X9.*Cryptographic Message Syntax* (draft)
ANSI X9.74 Accredited Standards Committee X9. *Conformance Testing for Certification Path Processing*
ANSI X9.76 Accredited Standards Committee X9. *Partial Key Refreshing Mechanism for Threshold Digital Signatures*

ANSI X9.77 Accredited Standards Committee X9.*Public Key Infrastructure Protocols*
ANSI X9.78 Accredited Standards Committee X9. *Attribute Certificate Extensions*
ANSI X9.79 Accredited Standards Committee X9. *Framework and Format Standard for Certificate Policies*
ANSI X9.80 Accredited Standards Committee X9. *Prime Number Generation*
ANSI X9.82 Accredited Standards Committee X9. *Random Number Generation*
ANSI X9.84 Accredited Standards Committee X9 *Biometric Information Management and Security*

ANSI X9.TG-17 Public-Key Cryptography for the Financial Services Industry: Technical Guideline on Elliptic Curve Arithmetic, to appear.
ANSI X9.TG-19 Modes of Operation Validation System for Triple Data Encryption Algorithm

X12: Electronic business data interchange
X12.58 (version 2): EDI security structures

Poznámka. Status řady norem z čísly ANSI X9.7*, ANSI X9.8* není určitý, pravděpodobně řada z těchto dokumentů je dnes ještě v přípravném stadiu (drafty). ANSI totiž i za pouhý seznam svých norem (http://webstore.ansi.org/ansidocstore/product.asp?sku=ANSI+Catalog) požaduje poplatek 10 US $.

2.4. NIST

Americká vládní instituce National Institute of Standards je ústředním americkým orgánem pro vývoj a publikace v normativní sféře. Řada jí vydaných dokumentů je však široce používána i v mezinárodním měřítku.

FIPS PUB

FIPS PUB 46-3 National Institute of Standards and Technology. Data Encryption Standard, This revision to the standard specifies the use of Triple DES, as described in ANSI X9.52., November 1999
FIPS PUB 81 National Institute of Standards and Technology. Dec. 1980, DES Modes of Operation
FIPS 112 Password Usage, May 19858
FIPS 113: Computer Data Authentication, which specifies the generation of a Message Authentication Code (MAC), from ANSI X9.9,
FIPS 171: Key Management Using ANSI X9.17.
FIPS PUB 140-2 National Institute of Standards and Technology. Nov. 1999, Security Requirements for Cryptographic Modules
FIPS PUB 180-1 National Institute of Standards and Technology. Secure Hash Standard. April 17, 1995.

FIPS 181 Automated Password generator, Oct. 1993
FIPS PUB 186-2 National Institute of Standards and Technology. February 2000, Digital Signature Standard (DSS)
FIPS PUB 196 Entity Authentication Using Public Key Cryptography, Feb. 1997
FIPS PUB National Institute of Standards and Technology. June 1999 – Recommmended Elliptic Curves For Federal Government Use, (http://csrc.nist.gov/encryption/NISTReCur.doc)
FIPS PUB 74 Guidelines for Implementing and Using the NBS Data Encryption Standard, 1981.
TWG-98-07 Federal Public Key Infrastructure (PKI) X.509 Certificate and CRL Extensions Profile March 9, 1998

Poznámka: v návaznosti na výše uvedené normy funguje tzv. „The Cryptographic Module Validation (CMV) Program", který má za cíl provádění evaluace kryptografických modulů a algoritmů.(viz příloha A.).

AES

NIST ve spolupráci s průmyslem a kryptografickou veřejností provádí práce na vývoji nové normy pro blokovou šifru – symetrickou kryptografii. Práce na Advanced Encryption Standard byly zahájeny v roce 1998, kdy bylo přihlášeno celkem 15 algoritmů. Postupně bylo vybráno pět finalistů (Twofish, RC6, Serpent, Mars a Rijndael), z těchto byl pak vybrán vítězný algoritmus, kterým se stal **RIJNDAEL**. Tento vítězný algoritmus se stane normou FIPS blokové šifry. Algoritmy pracují s bloky v délce 128 bitů a umožňují používat tři různé délky klíče (128, 192 a 256 bitů).

RIJNDAEL je algoritmus, který byl vytvořen belgickými (tedy evropskými) autory Joan Daemen, Vincent Rijmen na základě jimi dříve rozpracovaného algoritmu SQUARE. Algoritmus jako jediný z finalistů nepoužívá Feistelovo schéma.

Tato norma má nepochybně ústřední význam pro budoucnost nejen americké ale i mezinárodní kryptografie. V současné době je znám samotný algoritmus, probíhají práce zaměřené na stanovení různých módů, v rámci kterých lze algoritmus používat (jako byly módy CBC, CFB, ECB atd. pro DES).

Serie 800:

Tyto dokumenty tvoří určitý doprovod norem NIST, dávají např. určitý teoretický přehled problematiky (SP 800-2) nebo jsou zde obsaženy některé další informace - např. k validaci módů blokových šifer (SP 800-17, SP 800-20) či to jsou příručky pro přípravu konkrétních implementací kryptografických metod (SP 800-2x).

(http://csrc.nist.gov/publications/nistpubs/index.html)

SP 800-2 Public-Key Cryptography, April 1991
SP 800-15 Minimum Interoperability Specification for PKI Components (MISPC), Version 1, January 1998
SP 800-17 Modes of Operation Validation System (MOVS): Requirements and Procedures, February 1998

SP 800-20 Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS): Requirements and Procedures, Revised April 2000
SP 800-21 Guideline for Implementing Cryptography in the Federal Government, November 1999
SP 800-22 A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications,
Poznámka: Na adrese
http://csrc.nist.gov/rng/rng2.html
lze stáhnout software k tomuto dokumentu obsahující snad téměř všechny současné statistické testy náhodnosti a také ověřovací data k tomuto software. Podrobnější informace k této publikaci a také k přiloženému softwaru - - viz příloha E.
SP 800-23 Guideline to Federal Organizations on Security Assurance and Acquisition/ /Use of Tested/Evaluated Products,
SP 800-25 Federal Agency Use of Public Key Technology for Digital Signatures and Authentication

2.5. IETF

2.5.1. Celkový přehled

V současné době pracuje v rámci mezinárodní organizace IETF (The Internet Engineering Task Force) celá řada pracovních skupin orientovaná na problematiku implementace kryptografických metod, resp. obecněji na problematiku bezpečnosti dat.

IETF Working Groups - Security Area
(http://web.mit.edu/network/ietf/sa)

An Open Specification for Pretty Good Privacy (openpgp)
Authenticated Firewall Traversal (aft)
Common Authentication Technology (cat)
IP Security Policy (ipsp)
IP Security Protocol (ipsec)
IP Security Remote Access (ipsra)
Intrusion Detection Exchange Format (idwg)
Kerberized Internet Negotiation of Keys (kink)
Kerberos WG (krb-wg)
One Time Password Authentication (otp)
Public-Key Infrastructure (X.509) (pkix)
S/MIME Mail Security (smime)
Secure Network Time Protocol (stime)
Secure Shell (secsh)
Securely Available Credentials (sacred)
Security Issues in Network Event Logging (syslog)
Simple Public Key Infrastructure (spki)

Transport Layer Security (tls)
Web Transaction Security (wts)
XML Digital Signatures (xmldsig)

Výsledky práce některých z těchto skupin popíšeme v oddělených odstavcích.

2.5.2. openpgp

Zpracované dokumenty lze nalézt na adrese:
http://www.ietf.cnri.reston.va.us/html.charters/openpgp-charter.html

RFC (Request for Comment):
OpenPGP Message Format (RFC 2440)

internetové drafty:
Multiple Signatures using Security Multiparts
MIME Security with OpenPGP

Jak již název pracovní skupiny napovídá, jsou výsledné dokumenty zaměřeny na vytváření standardizovaných přístupů v PGP. Ústřední je zde materiál RFC 2440, jehož cílem je dle anotace: zveřejnit veškerou informaci nezbytnou k vývoji interoperabilní aplikace založené na OpenPGP formátu. V současné době je toto rfc přepracováváno:

OpenPGP Message Format - draft-ietf-openpgp-rfc2440bis-02.txt

2.5.3. ipsec

Současné VPN (Virtual Private Networks), tj. oddělené sítě používající Internet jako přenosový kanál se ve své konstrukci podstatně opírají o použití IPSEC. Bezpečnostní protokol je konstruován na síťové vrstvě. Existují dva základní formáty protokolů: AH (Authentication Header) a ESP (Encapsulating Security Payload). Protokoly a techniky podporují rovněž řízení příslušného klíčového hospodářství (key management) potřebné pro bezpečnost síťové vrstvy. V současné době je používán protokol IKMP specifikovaný pro aplikační vrstvu (vychází z dřívějšího protokolu ISAKMP/Oakley). Příslušné dokumenty pracovní skupiny lze nalézt na adrese
http://www.ietf.cnri.reston.va.us/html.charters/ipsec-charter.html

Jako u dalších skupin, které využívají metody symetrické kryptografie, dochází i zde v současnosti k přípravám na začlenění normy AES:

RFC:
IP Authentication using Keyed MD5 (RFC 1828)
The ESP DES-CBC Transform (RFC 1829)
HMAC: Keyed-Hashing for Message Authentication (RFC 2104)
HMAC-MD5 IP Authentication with Replay Prevention (RFC 2085)
Security Architecture for the Internet Protocol (RFC 2401)
The NULL Encryption Algorithm and Its Use With IPsec (RFC 2410)

IP Security Document Roadmap (RFC 2411)
IP Authentication Header (RFC 2402)
The OAKLEY Key Determination Protocol (RFC 2412)
The ESP CBC-Mode Cipher Algorithms (RFC 2451)
The Use of HMAC-MD5-96 within ESP and AH (RFC 2403)
The Use of HMAC-SHA-1-96 within ESP and AH (RFC 2404)
The ESP DES-CBC Cipher Algorithm With Explicit IV (RFC 2405)
IP Encapsulating Security Payload (ESP) (RFC 2406)
The Internet IP Security Domain of Interpretation for ISAKMP (RFC 2407)
Internet Security Association and Key Management Protocol (ISAKMP) (RFC 2408)
The Internet Key Exchange (IKE) (RFC 2409)
The Use of HMAC-RIPEMD-160-96 within ESP and AH (RFC 2857)

internetové drafty:

A GSS-API Authentication Method for IKE
DHCP Configuration of IPSEC Tunnel Mode
A Hybrid Authentication Mode for IKE
A Framework for Group Key Management for Multicast Security
A PKIX Profile for IKE
IPSec Monitoring MIB
IPsec DOI Textual Conventions MIB
IPsec Interactions with ECN
Additional ECC Groups For IKE
ISAKMP DOI-Independent Monitoring MIB
Content Requirements for ISAKMP Notify Messages
IKE Base Mode
IKE Monitoring MIB
Fixing IKE Phase 1 & 2 Authentication HASH
OpenPGP Key Usage in IKE
The Candidate AES Cipher Algorithms and Their Use With IPsec
Using Isakmp Heartbeats for Dead Peer Detection
IKE Authentication Using ECDSA
More MODP Diffie-Hellman groups for IKE

2.5.4. pkix

Materiály této skupiny jsou stěžejní pro práci s digitálními certifikáty dle X.509, které opětovně mají zásadní význam pro moderní koncepce PKI. Důležitými jsou zejména dokumenty: RFC 2459 (profily certifikátů a CRL), RFC 2510 (protokol pro řízení práce s certifikáty), RFC 2560 (protokol k online určování statutu certifikátu), RFC 2511 (formát žádosti o certifikát), ale i další. V současné době například se rozběhly práce na atributových certifikátech (draft-ietf-pkix-ac509prof-05.txt), práce na alternativních revokačních metodách, kvalifikovaných certifikátech atd. Dokumenty lze nalézt na
http://www.ietf.cnri.reston.va.us/html.charters/pkix-charter.html

RFC:
Internet X.509 Public Key Infrastructure Certificate and CRL Profile (RFC 2459)
Internet X.509 Public Key Infrastructure Certificate Management Protocols (RFC 2510)

Internet X.509 Certificate Request Message Format (RFC 2511)
Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC 2527)
Internet X.509 Public Key Infrastructure Representation of Key Exchange Algorithm (KEA) Keys in Internet X.509 Public Key Infrastructure Certificates (RFC 2528)
Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2 (RFC 2559)
Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP (RFC 2585)
Internet X.509 Public Key Infrastructure LDAPv2 Schema (RFC 2587)
X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP (RFC 2560)
Certificate Management Messages over CMS (RFC 2797)
Diffie-Hellman Proof-of-Possession Algorithms (RFC 2875)

internetové drafty:
Internet X.509 Public Key Infrastructure Time Stamp Protocols (TSP)
Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols
Internet X.509 Public Key Infrastructure PKIX Roadmap
An Internet AttributeCertificate Profile for Authorization
Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv3
Simple Certificate Validation Protocol (SCVP)
Limited AttributeCertificate Acquisition Protocol
Internet X.509 Public Key Certificate Infrastructure and CRL Profile
Internet X.509 Public Key Infrastructure Technical Requirements for a non-Repudiation Service
Internet X.509 Public Key Infrastructure Qualified Certificates Profile
Internet X.509 Public Key Infrastructure Certificate Management Protocols
Internet X.509 Public Key Infrastructure Permanent Identifier
Transport Protocols for CMP
Internet X.509 Public Key Infrastructure Additional LDAP Schema for PKIs and PMIs
Internet X.509 Public Key Infrastructure Repository Locator Service
Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and CRI Profile
Delegated Path Validation
Online Certificate Status Protocol, version 2
Delegated Path Discovery with OCSP
Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)

Poznámka: Vzhledem k významu osnovy z RFC 2527 pro praxi certifikačních autorit (dokumenty CP - cerifikační politika a CPS - certifikační prováděcí směrnice) je tato uvedena v příloze 4 spolu s českým překladem.

2.5.5. smime

S/MIME (verze 3) lze používat k ochraně elektronické pošty (přijímané a odesílané). Jsou vytvářeny prostředky k zabezpečení příslušných doménových služeb (Domain Security Services). Jedním z ústředních problémů je i otázka interoperability použitých metod vzhledem k různorodosti bezpečnostních politik na jednotlivých doménách. Výchozími jsou následující dokumenty: RFC 2631 (Diffie-Hellman - dohoda na klíči) a RFC 2630 (syntaxe kryptografické zprávy – CMS) Jednotlivá rfc a drafy lze nalézt na

http://www.ietf.cnri.reston.va.us/html.charters/smime-charter.html

RFC:
S/MIME Version 2 Message Specification (RFC 2311)
S/MIME Version 2 Certificate Handling (RFC 2312)
Cryptographic Message Syntax (RFC 2630)
Diffie-Hellman Key Agreement Method (RFC 2631)
S/MIME Version 3 Certificate Handling (RFC 2632)
S/MIME Version 3 Message Specification (RFC 2633)
Enhanced Security Services for S/MIME (RFC 2634)
Methods for Avoiding the 'Small-Subgroup' Attacks on the Diffie-Hellman Key Agreement Method for S/MIME (RFC 2785)
Use of the KEA and SKIPJACK Algorithms in CMS (RFC 2876)

Internetové drafty:
Certificate Distribution Specification
Domain Security Services using S/MIME
Use of the IDEA Encryption Algorithm in CMS
Password-based Encryption for S/MIME
Use of the CAST-128 Encryption Algorithm in CMS
Use of ECC Algorithms in CMS
Compressed Data Content Type for S/MIME
Implementing Company Classification Policy with the S/MIME Security Label
S/MIME Symmetric Key Distribution
Electronic Signature Formats for long term electronic signature
Use of the RSAES-OAEP Transport Algorithm in CMS
Electronic Signature Policies
Reuse of CMS Content Encryption Keys

2.5.6. spki

Cílem pracovní skupiny je vytvořit pro určité aplikace vhodné zjednodušení problematiky PKI. V současné době práce skupiny nepokračují. Dokumenty lze nalézt na http://www.ietf.cnri.reston.va.us/html.charters/spki-charter.html

RFC:
SPKI Requirements (RFC 2692)
SPKI Certificate Theory (RFC 2693)

2.5.7. tls

Podstatou práce této skupiny je vytvoření nové varianty protokolu SSL – přitom je použito nové označení TLS (jedná se ale i o převzetí některých vlastností jiných protokolů jako SSH a PCT, tj. mechanizmy používající obvykle pro transport protokol TCP). Jedná se tedy o vytváření bezpečnostních postupů na transportní vrstvě. Dokumenty lze nalézt na http://www.ietf.cnri.reston.va.us/html.charters/tls-charter.html

RFC:
The TLS Protocol Version 1.0 (RFC 2246)
Addition of Kerberos Cipher Suites to Transport Layer Security (TLS) (RFC 2712)
Upgrading to TLS Within HTTP/1.1 (RFC 2817)
HTTP Over TLS (RFC 2818)

Internetové drafty:
TLS Extension for SEED and HAS-160
Addition of MISTY1 to TLS
AES Ciphersuites for TLS
Addition of the Camellia Encryption Algorithm to TLS
Kerberos Cipher Suites in Transport Layer Security (TLS)
Wireless Extensions to TLS

2.5.8. xmldsig

Zejména v návaznosti na práci s elektronickými dokumenty pro e-commerce se objevují požadavky využívat aktuálni XML struktury, tj. data, která se objevují na webu. Digitální podpisy těchto dokumenty zde slouží k zajišťěni příslušných bezepečnostních požadavků (to je kritické např. při elektronických platbách, atd.). Materiály lze nalézt na adreee:
http://www.ietf.cnri.reston.va.us/html.charters/xmldsig-charter.html

RFC:
XML-Signature Requirements (RFC 2807)

Internetové drafty:
XML-Signature Syntax and Processing
Canonical XML Version 1.0

2.5.8. nezařazené

Některá důležitá RFC nevznikla jako výsledek práce určité skupiny, ale byla zařazena vzhledem k své aktuálnosti. Z materiálů se vztahem ke kryptografii jsou to:

Rfc1319: The MD2 Message-Digest Algorithm. B. Kaliski. April 1992.
Rfc1320: The MD4 Message-Digest Algorithm. R. Rivest. April 1992.
Rfc1321: The MD5 Message-Digest Algorithm. R. Rivest. April 1992.
Rfc1810: Report on MD5 Performance, J. Touch, June 1995
Rfc1851: The ESP Triple DES Transform, P. Karn, September 1995
Rfc2144: The CAST-128 Encryption Algorithm, C. Adams, May 1997
Bruce Schneier; Peter Gutmann: draft-schneier-blowfish-00.txt, August 1999

Tato RFC jsou, jak je vidět z názvů, orientována na popis algoritmů (hashovacích funkcí MD, symetrických šifer Blowfish, CAST).

2.6. PKCS

Normy PKCS jsou vytvářeny v laboratořích světoznámé firmy RSA Security (dříve RSA) ve spolupráci s řadou vývojářů z celého světa. Poprvé tyto normy byly publikovány v roce 1991 jako výsledek jednání určité skupiny pracovníků, kteří implementovali technologii kryptografie s veřejným klíčem. Od té doby jsou tyto normy široce využívány a některá jejich doporučení se staly součástí celé řady dalších norem (oficiálních i de facto).
Dnes existují následující PKCS.

- **PKCS #1:RSA Cryptography Standard**
- **PKCS #3:Diffie-Hellman Key Agreement Standard**
- **PKCS #5:Password-Based Cryptography Standard**
- **PKCS #6:Extended-Certificate Syntax Standard**
- **PKCS #7:Cryptographic Message Syntax Standard**
- **PKCS #8:Private-Key Information Syntax Standard**
- **PKCS #9:Selected Attribute Types**
- **PKCS #10:Certification Request Syntax Standard**
- **PKCS #11:Cryptographic Token Interface Standard**
- **PKCS #12:Personal Information Exchange Syntax Standard**
- **PKCS #13: Elliptic Curve Cryptography Standard**
- **PKCS #15: Cryptographic Token Information Format Standard**

(Poznámka: PKCS **#**13 k eliptickým křivkám ještě nebyl zveřejněn, existuje zatím pouze projekt, norma je ve stadiu vývoje. Původní PKCS #2 a PKCS #4 byly následně včleněny do PKCS #1).
Obsah a význam jednotlivých dokumentů je hodnocen v Příloze 2.(na základě článků autora v Crypto-Worldu).

2.7. SECG

V roce 1999 vznikla iniciativa SECG (spolupráce kanadské firmy Certicom a University of Waterloo), která si za svůj cíl položila další rozpracování problematiky eliptických křivek, resp. umožnit interoperabilitu různých systémů pomocí výběru standardizovaných hodnot parametrů pro eliptické křivky. Je třeba říci, že význam iniciativy poklesl poté, co se stejnou resp.analogickou myšlenkou přišel i americký vládní NIST. Přesto práce pokračují a dnes jsou k dispozici následující dokumenty:

SEC 1: Elliptic Curve Cryptography
SEC 2 - Recommended elliptic curve domain parameters (version 0.7)
GEC 2 - Test Vectors for SEC 1 (version 0.3)
Draft ECC X.509 Specification

2.8. Evropská Unie

2.8.1. Přehled současných aktivit

Současné přípravné práce odborných skupin navazují na Final Report ICTSB European Electronic Signature Standardization (http://www.ict.etsi.org/eessi/Final-Report.pdf).
V návaznosti na tuto závěrečnou zprávu byla Evropskou komisí předložena a Evropským parlamentem přijata (30.11.1999) Směrnice Evropské Unie pro elektronické podpisy (http://www.ict.etsi.org/eessi/e-sign-directive.pdf).

Toto jsou dva základní dokumenty, ze kterých potom vychází další postupy. První z nich komplexně vytyčuje celkovou strategii Evropské Unie při řešení problematiky elektronických podpisů. Ukazuje nezbytné směry v legislativě a především v oblasti norem resp. dalších nezbytných aktivit. Jeho základní závěry jsou formulovány následovně:

1) převzetí resp. vývoj průmyslových norem by mělo maximálně zmenšit potřebu detailizace zákonů a vyhlášek v dané oblasti;

2) normy jsou nezbytně nutné a všude, kde je to možné, je třeba preferovat odkazy na existující mezinárodní normy před vývojem nových norem;

3) požadavky v oblasti norem jsou dvojího druhu: kvalitativní a procedurální normy týkající se informační bezpečnosti a technické normy vzhledem k interoperabilitě produktů;

4) podepisovací prostředky (produkty), pokud vyhovují požadavkům Direktivy, musí projít příslušným hodnocením (shoda produktu) a certifikací akreditovanou institucí pod EN 45000 (Evropské akreditační schéma);

5) je třeba vytvořit společný referenční bod na základě definice výchozí množiny technologických komponent, který bude tvořit technický rámec pro ověřování kvalifikovaných elektronických podpisů využívajících asymetrickou kryptografii a digitální certifikáty;

6) vzhledem k poskytovatelům certifikačních služeb je třeba použít vhodné bezpečnostní normy:
- obecné zásady v oblasti bezpečnosti (např. BS7799 č. 1 a č. 2),
- specifikace bezpečnostních požadavků vzhledem k důvěryhodným systémům, které tito poskytovatelé používají; první požadavky v této oblasti se týkají především kryptografických modulů (např. FIPS 140-1) a využití rizikové analýzy,
- výchozí certifikační politika pro poskytovatele certifikačních služeb – je doporučováno vyjít z materiálu IETF PKIX – rfc. 2527,
- obdobně pro poskytovatele služeb v oblasti časových razítek je třeba provést specifikaci požadavků vzhledem k jejich politice;

7) vzhledem k produktům sloužícím k vytváření podpisů a jejich ověřování je třeba mít k dispozici následující příslušné normy:
- specifikace bezpečnostních požadavků vzhledem k důvěryhodným hardwarovým zařízením, která jsou použita jako bezpečná zařízení pro vytváření podpisů (FIPS 140-1, Common Criteria – ISO 15408),

- specifikace pro vytváření elektronických podpisů (včetně uživatelova interface) a specifikace produktů a postupů k ověřování podpisů;

8) je nezbytná koordinace jednotlivých aktivit v oblasti norem;

9) z hlediska interoperability jsou nezbytné následující normy:
- technické normy pro syntaxi a kódování elektronických podpisů (včetně vícenásobných podpisů); je doporučováno vyjít z rfc.2315,
- operativní protokoly pro řízení PKI (rfc skupiny PKIX),
- profily kvalifikovaných certifikátů na bázi X.509.

Směrnice Evropské Unie pro elektronický podpis byla vyvíjena několik let – existovala v podobě draftu. Nakonec ji 30.11.1999 schválil Evropský parlament. Přitom členské země Eu jsou povinovány uvést své zákony, vyhlášky a administrativní postupy v platnost do souladu s touto Směrnicí do 19. července 2001. Směrnice byla formulována tak, aby byly naplněny následující tři základní principy:

I. Technologická neutralita
II. Vydávání oprávnění pro poskytovatele certtifikačních služeb není direktivně omezeno žádným schématem
III. Nezbytnost rozpoznání zákonné platnosti elektronických podpisů

Směrnice EU k elektronickým podpisům vytváří základní filosofii pro řešení této problematiky. V návaznosti na tento dokument je zpracovávána celá serie norem, které řeší konkrétní postupy pro řešení v jednotlivých oblastech (dokumenty ETSI a CEN ESSI).

2.8.2. ETSI

(ETSI Electronic Signatures and Infrastructures - EESSI Program)

V první fázi prací byl zpracován dokument určující osnovu dalších prací Electronic Signature Report (http://docbox.etsi.org/tech-org/security/open/el-sign/ESRep042.pdf) . Druhá fáze prací započala na počátku roku 2000 a zahrnuje (dokument Workplan) následující okruhy problémů:

Policy Requirements for CSPs Issuing Qualified Certificates;
Qualified Certificates Profile;
Time Stamping Profile;
Electronic Signature Formats.

První ze série norem „ETSI standard ES 201 733 (**Electronic Signature Formats**)" byla již schválena v květnu 2000. Obsahuje zejména definice různých formátů elektronických podpisů v návaznosti na používání časových značek (podrobněji např. v článku J. Pinkava: Moderní kryptografické algoritmy pro elektronický podpis, Seminář ČAČK, březen 2000).

Samotnému procesu vytváření časových značek je věnována norma **Time Stamping Profile**, která se opírá především o dokument Internet X.509 Public Key Infrastructure Time Stamp Protocols (v současné době je nejnovější draft-ietf-pkix-time-stamp-12.txt). Dokument

byl již také schválen, dostal označení TS 101 861 a bude opublikován jakmile se příslušný draft stane dokumentem RFC.

V normě **Qualified Certificates Profile** jsou na podobu kvalifikovaného certifikátu kladeny některé základní doplňující nároky. Např. v poli, kde je označen vydavatel certifikátu musí být obsaženo i jméno vydávající země (vpříslušném atributu). V profilu musí být obsaženy následující údaje:

- formulace, že certifikát je vydán jako kvalifikovaný certifikát;
- formulace omezující hodnotu transakce pro kterou lze certifikát využít;
- formulace ukazující časový interval po který je archivována informace poskytnutá uživatelem při registraci.

Dokument byl již schválen, dostal označení TS 101 861 a byl opublikován v prosinci 2000.

Posledním z těchto dokumentů je norma zabývající se požadavky na politiku poskytovatelů certifikačních služeb, kteří vydávají kvalifikované certifikáty - **Policy Requirements for CSPs Issuing Qualified Certificates.** Toto je samostatný dokument upřesňující požadavky na CP (certifikační politiku) a CPS (certifikační prováděcí směrnici) poskytovatelů certifikačních služeb - životnost klíčů, certifikátů, management certifikátů, bezpečnostní aspekty, atd. Svojí filosofií vychází dokument z RFC 2527: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.
Dokument byl již schválen, dostal označení TS 101 456 a byl opublikován v prosinci 2000.
S aktuálním stavem se lze seznámit na adrese http://www.etsi.org/sec/el-sign.htm.
ETSI v roce 2001 chystá vydání zhruba pěti nových dokumentů. K jejich obsahu jsou v současné době známy pouze následující informace.

Policy requirements for CSPs issuing trusted time stamps

Dokument bude vycházet z požadavků na politiku, které již byly v dokumentech ETSI zpracovány. Na službě časových značek je velice zainteresována komerční sféra a stávají se důležitou složkou problematiky elektronických podpisů (dokumentES 201733). Zde zformulovaná minima pro požadavky v oblasti bezpečnosti a kvality jsou nezbytná k zabezpečení důvěryhodného ověření dlouhodobých (long-term) elektronických podpisů.

Policy requirements for CSPs, according to Art. 5.2 of the Directive

Obsahem tohoto materiálu budou otázky řízení bezpečnosti a certifikační politika těch poskytovatelů certifikačních služeb, kteří fungují na bázi principů odlišných od principů pro poskytovatele certifikačních služeb (PCS), kteří vydávají kvalifikované certifikáty. Potřeba existence těchto PCS vyplývá z potřeb trhu (transakce elektronického obchodu střední úrovně – jako například mobilní elektronický obchod). Na základě analýzy provedené STF pro alternativní třídy certifikátů (dle článku 5.2 Směrnice EU o elektronických podpisech) budou stanoveny příslušné specifikace, které se mimo jiné budou odkazovat např. na dokument RFC 2527 a doplní zde potřebné specifické detaily.

XML electronic signatures

Norma se bude zabývat syntaxí a formáty kódování elektronických podpisů v XML na základě dokumentu ES 201733. První studie pro verzi XML je připravována v rámci STF 155 (Specialist Task Force). Současný formát XML podpisů dle W3C bude použit k převzetí formátů vyšších úrovní elektronických podpisů dle ETSI do světa XML. Tato aktivita vznikla v návaznosti na mezinárodní aktivity v dané oblasti, zejména W3C/IETF a práce v EDI. Hlavním důvodem pro toto spojení je uvedení specifikací XML na mezinárodní scénu.

Technical aspects of signature policies

Koncepce podpisové politiky je zde zvažována ve vztahu k ustavení společné základny elektronických podpisů. Dokument ETSI ES 201 733 již sice obsahuje určité specifické nástroje pro definice podpisových politik, avšak neobsahuje všechny takovéto aspekty (např. vícenásobné podpisy). Dokument bude navržen jako experimentální RFC pro IETF a posléze připraven jako norma.

Infrastructure and interoperability requirements for on-line validation of Certification Service Providers

Cílem těchto prací je stanovit doporučení pro podporu akcí spoléhající se strany ve směru ověření, že vydavatel došlého certifikátu je v dané době důvěryhodnou stranou transakce. Na základě existujících dokumentů EESSI lze zajistit, že strana spoléhající se na certifikát (například příjemce podepsané smlouvy či objednávky) získá dostatek informací potřebných pro kontrolu platnosti certifikátu. Existují tedy normy podporující takovouto kontrolu. Avšak podstatně obtížnější je ověřit, zda vydávající CSP je v době transakce v pořádku (např. CSP mohla ukončit svoji činnost nebo neprošla posledním auditem atd.). Tento typ informací je dodáván třetí stranou nezávislou jak na straně, která transakci podepsala, tak i na straně vydavatele certifikátu. Důležitost této informace je stěžejní zejména v transakcích překračujících hranice domén a států.
Existující národní schémata pro tuto problematiku nejsou harmonizována, totéž se týká odpovídajících protokolů a formátů dat. Dokument zohlední jak technické tak i akreditační aspekty problematiky a jeho cílem bude identifikace potřebných procedurálních a technických vlastností.

2.8.3. CEN ESSI

V současné době jsou prováděny práce pro zpracování následujících pěti dokumentů:

Security Requirements For Trustworthy Systems and Products
Security Requirements for Signature Creation Devices
Signature Creation Environment

Signature Verification Process nad Environment
Conformity Assessment of Products and Services for Electronic Signatures

Aktuální informace lze nalézt na adrese: http://www.ni.din.de. Zde došlo na posledním jednání (E-SIGn Workshop, 20-21.11.2000) k posuvu obsahu jednotlivých dokumentů, odsud pramení i změna jejich názvů.

První z dokumentů - **Security Requirements for Trustworthy Systems and Products** - se zabývá bezpečnostními požadavky na důvěryhodné systémy poskytovatelů certifikačních služeb, kteří vydávají kvalifikované certifikáty. Jedním ze závěrů projednaných v listopadu je rozhodnutí, že bude zpracován nový dokument - pracovní název „*Security Requirements for Cryptograhic Modules Suitable for trustworthy Systems*“. První draft bude k dispozici v lednu 2001 a v březnu 2001 bude tento materiál projednán. Bylo zde konstatováno, že je problém odkazovat se v Evropě na dokument (FIPS 140-1), který není uznáván jako evropská norma. Současně s tím vzniká i problém evaluace produktu dle dokumentu FIPS. Z hlediska obsahu FIPS 140-1 je otázkou nakolik lze požadavky v něm formulované vztáhnout i na specifika certifikačních autorit. nový dokument bude vycházet z formátu a obsahu ISO 15408 (Barcelona, říjen 2000) a měl by tvořit celosvětový základ pro evaluace. byly stanoveny oblasti, kterých se bude chystaný dokument týkat. Na zasedání 7.2.2001 již proběhlo rozdělení problematiky na dvě zmíněné části a byla zveřejněna nová verze první části pod názvem Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures.

Velice důležitou je norma **Security Requirements for Signature Creation Devices**, tj. norma stanovující požadavky na bezpečný podpisový nástroj (v duchu terminologie Směrnice EU o elektronickém podpisu a i našeho zákona o elektronickém podpisu).

Poznámka.: Momentálně existují dvě verze tohoto dokumentu – EAL 4 a EAL4+, které se tudíž (jak ukazuje název verze) liší v nárocích na bezpečné podpisové zařízení. Při jednání k tomuto dokumentu došlo totiž k rozporným stanoviskům při formulaci požadavku vzhledem k zranitelnosti evaluovaného podpisového prostředku. Podle EAL 4 (Common Criteria) stačí požadovat, aby objekt evaluace byl rezistentní vůči útokům narušitele „s nízkou schopností útočit“. Oproti tomu zpracovatelé dokumentu přišli s návrhem, aby zde byla použit požadavek, aby objekt evaluace byl rezistentní vůči útokům narušitele „s vysokou schopností útočit“. Na jednání nedošlo k dohodě a nakonec bylo rozhodnuto, že vedení EESSI má přijít před Evropskou komisi paralelně s oběma návrhy. Obě verze byly zveřejněny a nazývají se Secure Signatur-Creation Devices, version 'EAL 4' resp. Secure Signatur-Creation Devices, version 'EAL 4+'.

Problematika **Signature Creation Environment** - zde je k dispozici zatím pouze materiál „*Security Requirements for Signature Creation Systems*“ (říjen 2000) a shrnuty komentáře k tomuto materiálu, nová verze zatím není k dispozici.
V dokumentu je mimo jiné řečeno: Systém na vytváření podpisů (SCS) bude obsahovat specifické komponenty ve vztahu k důvěryhodnému prostředí a k vlastním aplikacím. Důvěryhodnými komponentami jsou všechny závazné komponenty jako:
· SDV - (Signer´s Document Viewer) používano pro prohlížení podepsaných dokumentů;
· SAV - (Signature Attributes Viewer) používano pro prohlížení atributů podpisu;
· SIC - (Signer Interaction Component) pomocí této komponenty probíhá interakce podpisující strany s SCS, tak, aby bylo vytváření podpisu pod kontrolou uživatele;

· SAC - (Signer´s Authentication Component) - to je např. čipová karta s PINem, která je používána k autentizaci podepisující strany na základě autentizujících dat anebo biometrických vlastností takovou cestou, že výsledek lze porovnat s hodnotou uloženou v SSCD.
· DHC - (Data Hashing Component) - vytváří dat, která mají být
· SSC - (SSCD/SCS Communicator) řídí interakce mezi SCS a SSCD;
· SSA - (SSCD/SCS Authenticator) ustavuje důvěryhodnou cestu mezi SSCD a SCS.
Poznámka : SSCD = Secure Signature Creation Device.
Aplikačními specifickými komponentami jsou:
-SDC - (Signer's Document Composer) - např. textový editor, sloužící pro vytváření, výběr dokumentu podepisující osoby a jejích atributů.
-CCV - (Certificate Content Viewer) - ten dokáže zobrazit úplný obsah certifikátu podepisující osoby.
-SDOC - (Signed Data Object Composer) - přetváří složky podepisovaného objektu do bitového řetězcea jeho výstupem je určitý normalizovaný formát (ETSI Electronic Signature Formats Document);
-CSPC - (Certification Service Provider Interaction Component) používán pro získání certifikátu podepisující strany či získání časové značky;
-SHI - (SSCD Holder Indicator) zobrazuje jméno majitele SSCD.

Požadavky na ověřování elektronického podpisu stanoví norma **Procedures for Electronic Signature Verification**. Jsou zde analyzovány různé aspekty verifikačního procesu (časové značky, kvalifikované certifikáty), popis jednotlivých komponent verifikačního systému, příklady různých prostředí a zformulovány požadavky na systém verifikující podpisy z řady hledisek (právní aspekty, atd.). Je zde také analýzována problematika vícenásobných podpisů a otázky dlouhodobé archivace podpisů.

Poslední materiál **EESSI Conformity Assessment Guidance** je věnován otázkám harmonizace implementací norem pro elektronické podpisy – slouží zejména jako příručka certifikujícím a testujícícm laboratořím.
Týká se čtyř základních oblastí:

- služeb CA a procesů navazujících na řízení PKI, informační bezpečnosti, organizační spolehlivosti ve vztahu ke kvalifikovaným certifikátům;
- systémů pro vytváření elektronických podpisů ;
- procedur pro verifikaci podpisu;
- bezpečných podpisových prostředků.

V současné době zatím ještě neexistují definitivní verze těchto dokumentů.

2.8.4. CRYPTONESSIE

V druhé polovině května se objevila na webu informace o nové aktivitě v rámci Evropské Unie. Jedná se o projekt NESSIE (New European Schemes for Signature, Integrity, and Encryption) programu IST Evropské komise (http://cryptonessie.org).

NESSIE je tříletý projekt, který byl zahájen 1.ledna 2000. Jeho hlavním cílem je přinést celé „portfolio“ bezpečných kryptografických modelů (tzv. „kryptografických primitivů“), které lze pak používat v rámci různých technologických platforem. Jednotlivé modely budou vytvářeny na základě veřejných návrhů a rovněž tak vyhodnocení těchto návrhů proběhne otevřenou a transparentní cestou. Celková koncepce tohoto portfolia je podstatně širší než obdobný projekt AES (Advanced Encryption Standard), který řídí americký NIST. Projekt zároveň navazuje na již získané výsledky v rámci evropských struktur. Zde lze zmínit např. Směrnici Evropské Unie pro elektronický podpis nebo čerstvě vydanou (květen 2000) normu k formátům elektronických podpisů – Electronic Signature Formats, ETSI 201 733.

Celkem se jedná o následujících deset tříd kryptografických primitivů:

1. Blokové šifry
2. Synchronní proudové šifry
3. Samosynchronizující se proudové šifry
4. Autentizační kódy zpráv (MAC)
5. Hashovací funkce rezistantní vůči kolizím
6. Jednosměrné hashovací funkce
7. Pseudonáhodné funkce
8. Asymetrická schémata pro šifrování
9. Asymetrická schémata pro digitální podpis
10. Asymetrická schémata pro identifikaci

V rámci každé třídy budou existovat dvě bezpečnostní úrovně (normální a vysoká), s vyjímkou blokových šifer, kde bude ještě třetí úroveň (historická-normální). Tj. například blokové šifry vysoké bezpečnostní úrovně mají pracovat s bloky textu v délce 128 bitů a sklíčem nejméně v délce 256 bitů. Blokové šifry normální bezpečnostní úrovně pracují rovněž s bloky otevřeného textu v délce 128 bitů a musí mít klíč dlouhý nejméně 128 bitů. Zmíněná třetí úroveň ponechává možnost existence blokových šifer, které pracují s bloky otevřeného textu v délce 64 bitů (jako je tomu u většiny současných algoritmů). Délka klíče i u této třetí úrovně však musí být minimálně 128 bitů.

Vyhodnocení jednotlivých návrhů bude probíhat na základě:

a) bezpečnostních kriterií (obtížnost útoků, zdůvodnění bezpečnosti,...)
b) implementačních kriterií (software, hardware, nároky na objem paměti, spolehlivost,...)
c) dalších kriterií, jako je jednoduchost a zřejmost návrhu atd.

V rámci prvního kola, které končí v září 2000, mají být odevzdány výchozí návrhy. V říjnu pak bude následovat jejich první projednání v rámci první „lochneské“ konference.

Aktuální přehled předložených návrhů v rámci tohoto projektu obsahuje Příloha C.

2.9. Jiné

ITU

International Telecommunications Union, ITU-T (dříve CCITT) je mezinárodní organizace, která vytváří normy pro telekomunikační zařízení a systémy.
Především je třeba zde zmínit jednu veledůležitou normu: ITU-T Recommendation X.509 (1997 E): Information Technology – Open Systems Interconnection – The Directory: Authentication Framework, International Telecommunications Union, June 1997. Viz též ISO IEC 9594-8/ITU-T X.509. Toto je základní norma pro popis tvaru, povinných a dobrovolných polí (rozšíření - extensions) digitálních certifikátů a rovněž tak popisuje základní vlastnosti CRL (seznamu odvolaných certifikátů).

Tato norma byla v roce 2000 kompletně přepracována a doplněna. Nová podoba však zatím existuje pouze ve formě draftu - Draft Revised ISO/IEC 9594-8. Nová verze se výrazně podrobněji zabývá problematikou certifikátů, PKI adresářů, atributových certifikátů a problematikou řízení privilegií.
Normy ITU X.400 a X.435 mají velký význam pro práci se zprávami EDI (Electronic business Data Interchange).

ECBS:

European Committee for Banking Standards, http://www.ecbs.org
např.:

- TR 400 Biometrics, 1996
- TR 401 Secure Banking over the Internet, March 1997
- TR 402 Certification Authorities, December 1997, update October 1999
- TR 405 Key recovery in Financial Systems, June 1998
- TR 406 GUIDELINES ON ALGORITHMS USAGE AND KEY MANAGEMENT, September 1999

Dokument **TR 400** – Biometrika - obsahuje tedy v zásadě určitý přehled problematiky (ovšem vývoj v této oblasti je rychlý – dokument je z roku 1996). Dále obsahuje určitá základní doporučení k používaná těchto metod (např. pro výběr biom. metody: sociální akceptovatelnost, snadnost manipulace, bezpečnost, náklady)
Dále **TR 401** – také tento dokument lze těžko nazvat normou,jeho cílem je spíše provést přehled metod pro zabezepečení dat (na internetu) a přehled možných útoků, vlastnosti firewallů, protokoly (SSL,S-HTTP, TSL,...), zabezpečení mailů, včlenění finančních dokumentů, el. obchod (SET, Homebanking) a jen velmi stručně obsahuje vlastnosti PKI.
Norma **TR 402** vzhledem k posledním úpravám respektujícím současné trendy je to již první modernější dokument. Obsahově pokrývá oblasti, zmíněné v současných dokumentech v dané problematice. Z hlediska bankovnictví jsou nesporně významná doporučení ECBS na závěr jednotlivých paragrafů. Příloha B obsahuje přehled certifikátů používaných v bankovnictví:
- X 509 certificate
- ISO 11 166 certificate
- UN/EDIFACT SJWG certificate
- EMV certificate

- EDI 5/ETEBAC 5 certificate -TELESEC certificate

Norma **TR 405** se zabývá problematikou Key Recovery, aktuální v době vydání normy, v současné době se díky legislativám v některých zemích upouští od používaní této metody – i když nemusí to platit všeobecně (ale např. z hlediska el.podpisu je uplatňována jednoznačně zásada nepopiratelnosti).

Dokument **TR 406** je vlastně určitý průvodce současnými algoritmy z hledisek:
- Definice;
- Implementace;
- Key management (celý životní cyklus klíčů);
- Odvolání (revokace) certifikátů;

Popis je opět doplněn určitými doporučeními ECBS

W3C

Konzorcium World Wide Web (W3C) vytvořilo normalizovanou syntaxi pro strukturalizaci webovských dokumentů – Extensible Markup Language – XML. (http://www.w3.org/DSig/). úkolem příslušné pracovní skupiny je provést vývoj syntaxe kompatibilní s XML, kterou lze použít pro reprezentaci podpisu zdrojů na webu a syntaxe pro části protokolů a procedur při výpočtu a verifikaci takovýchto podpisů.

Open Group Technical Standard

CDSA (http://www.opengroup.org/publications/catalog/c914.htm) *Common Data Security Architecture* je norma určená pro bezpečnost elektronického obchodování a jiných obchodních aplikací pomocí kryptografických metod, řízení práce s certifikáty, řízení politiky důvěry a obsahující možnost rozkrytí klíčů (*Key recovery facility*).

Obsahuje následující části:

Common Security: CDSA and CSSM, Version 2
Part1: Common Data Security Architecture (CDSA)
Part 2: Common Security Service Manager (CSSM) API
Part 3: CSSM Module Directory Service (MDS) Interface
Part 4: CSSM Key Recovery API
Part 5: CDSA Embedded Integrity Services Library API
Part 6: CDSA Signed Manifest
Part 7: CDSA OIDs for Certificate Library Modules
Part 8: CSSM Elective Module Manager
Part 9: Add-In Module Structure and Administration
Part 10: CSSM Cryptographic Service Provider Interface
Part 11: CSSM Trust Policy Interface
Part 12: CSSM Authorization Computation Interface
Part 13: CSSM Certificate Library Interface
Part 14: CSSM Data Storage Library Interface
Part 15: CSSM Key Recovery Interface

CDSA definuje čtyrvrstvou architekturu obsahující:
1) aplikace
2) služby dle vrstev
3) řízení infrastruktury - Common Security Services Manager (CSSM)
4) moduly pro Security Service Provider

Common Data Security Architecture (CDSA) ve verzi 2 byla vydána v květnu 2000.

3.3. Hashovací funkce

Pojem hashovací funkce se vyvinul z pojmu jednosměrné funkce v návaznosti na kryptografické aplikace. Norma ISO/IEC 10118 popisuje jednak obecné přístupy, jednak některé konkrétní technologie. V současné době jsou nejpoužívanějšími hashovacími funkcemi následující:
SHA-1 (norma z roku 1995 - http://csrc.nist.gov/fips/fip180-1.pdf),
MD5 (RFC1321: The MD5 Message-Digest Algorithm. R. Rivest. April 1992.),
RIPEMD. (ftp://ftp.esat.kuleuven.ac.be/pub/COSIC/bosselae/ripemd/) - evropské schéma hashovací funkce
Některé další byly navrženy v rámci projektu Cryptonessie a i NIST si vzhledem k AES pospíšil s předběžnou verzí **SHA-512**, což je hashovací funkce umožňující výstupy v délce až 512 bitů (http://csrc.nist.gov/cryptval/shs/sha256-384-512.pdf) atd.
Blízkou třídou norem jsou dokumenty popisující tzv. autentizační kódy zpráv (MAC - Message Authentication Code) - ISO/IEC 9797.

Staršími, dnes již ojediněle používanými hashovacími funkcemi jsou MD2 a MD4 (obě vychází z dílny RSA Security- RFC 1319 a RFC 1320).

3.4. Důvěryhodné třetí strany

Řada existujících protokolů se stále ještě obrací k pojmu tzv. třetí důveryhodné strany. Pokud mě paměť neklame, tento pojem se rozvinul z kdysi používaného pojmu střediska pro rozdělování klíčů (key distribution center). Toto středisko bylo využíváno v rozsáhlejších sítích v dobách, kdy asymetrická kryptografie ještě nebyla prakticky pro podobné situace využívána. V současné době se tento pojem objevuje např. v návaznosti na problematiku časových značek (time-stamping). Některé dokumenty (zatím však spíše v návaznosti na obecnou teorii nikoliv na konkrétní normy) se snaží i zde význam tohoto pojmu zredukovat. S jeho praktickým využíváním jsou vždy spojena určitá bezpečnostní rizika. Je totiž třeba zabezpečit skutečnou nestrannost této důvěryhodné třetí strany a to je v praktických situacích někdy nesnadné. Využíván je tento pojem však stále v stroze hierarchických sítích (např. ve vojenství). Některé tyto aspekty lze vidět v normách navazujících na známý systém Kerberos (viz výše zmíněné dokumenty IETF, pracovní skupiny cat, kink, krb-wg).

3.5. Digitální certifikáty.

Pojem digitálního certifikátu vychází dnes obvykle ze specifikace dané normou X.509, která pak byla rozpracována v dlouhé řadě dalších dokumentů (IETF-pkix, profily tzv. kvalifikovaných certifikátů, ANSI X9.55 - rozšíření certifikátů, ANSI X9.57 -řízení práce s certifikáty, ANSI X9.78 - atributové certifikáty, atd.). Nelze opominout ani pojem kvalifikovaného certifikátu zmíněného v jiných částech tohoto dokumentu. V současné době se objevují další analogické pojmy - jako je např. atributový certifikát.

3.6. Certifikační autority a související pojmy

Toto je relativně velmi nová oblast a proto se nelze divit, že takovéto normy teprve vznikají nebo jsou velmi svěží. Příkladem může být chystaná norma EU ETSI pro poskytovatele certifikačních služeb, kteří vydávají kvalifikované certifikáty. Nelze opomenout dokument RFC 2527, který v současné době slouží jako základ pro vytváření certifikačních politik (CP) a certifikačních prováděcích směrnic (CPS) pro jednotlivé certifikační autority. Směrodatná osnova z RFC 2527 pro vytváření CP (certifikační politika) a CPS (certifikační prováděcí směrnice) je uvedena v příloze 4.

3.7. Kryptografické protokoly

Jen vyjmenování používaných kryptografických protokolů na různých vrstvách modelu OSI by zde zabralo rozsáhlé místo - jako příklad zde vezměmě proto jen některé známé modely: IPSEC (včetně všech dílčích variant), SSL, autentizační protokoly, protokoly pro práci s digitální certifikáty, pro práci s formáty S/MIME atd. Ty nejdůležitější lze nalézt např. v odstavci 2.5 k IETF.

Problematikou klíčového hospodářství se zabývá norma ISO/IEC 11770, problematikou nepopiratelnosti ISO/IEC 13888.

3.8. Čipové karty

Zde se jedná vlastně o určitou samostatnou oblast, kromě norem ISO existuje zde dlouhá řada průmyslových norem souvisejících s bezpečností technologických postupů. Zejména důležitou je zde norma ISO/IEC 7816, která má dnes již deset dílů. Některé informace o normě ISO/IEC/7816 vztahující se bezprostředně k čipovým kartám a navazujících normách PKCS#11 (CRYPTOKI) a PKCS#15 obsahuje příloha B.

3.9. Normy metodologického charakteru

Zde lze zmínit např. normy ISO/IEC 8824, ISO/IEC 8825 zabývající si ASN.1 - pravidly abstraktního popisu datových struktur (platformově nezávislého popisu odpovídajících datových struktur).

3.10. Obecně bezpečnostní normy

Výchozím dokumentem pro navazující normy jsou tzv. **Common Criteria**, což jsou mezinárodně uznávaná kriteria pro problematiku bezpečnosti IT. Obecně řečeno, tato kriteria ověřují:

- zdali jsou správně definovány požadavky na příslušný produkt

- zdali tato požadavky byly správně implementovány
- a zda v procesu vývoje produktu a zpracování dokumentyce byla splněna určitá kriteria.

Na rozpracování dokumentu Common Criteria - také viz

- ISO/IEC 15408:1999 *Information technology -- Security techniques -- Evaluation criteria for IT Security*
  - Part 1: *Introduction and general model*
  - Part 2: *Security functional requirements*
  - Part 3: *Annexes*

se podílelo celkem šest zemí: USA, Kanada a z evropských zemí to byly Velká Británie, Francie, Německo a Nizozemsko. Tyto země mají v současné době praktické zkušenosti a funkční organizace zabývající se problematikou certifikace bezpečnostních produktů. Dokument navazuje na známou Orange Book. Poslední verze Dokumentu CC je ze srpna roku 1999 a nese číslo 2.1. Na CC navazuje dokument Common Evaluation Methodology (CEM) .
Norma ISO/IEC TR 13335 - je v několika svých postupně opublikovaných částech (1996-2000) formována jako příručka pro řízení informační bezpečnosti:

ISO/IEC TR 13335:1996 *Information technology - Security techniques - Guidelines for IT Security (GMITS)*
Part 1: *Concepts and models for IT Security*
Part 2: *Managing and Planning IT Security*
Part 3: *Techniques for the Management of IT Security*
Part 4: *Selection of safeguards*

BS7799 č.1 a č.2 (1995, 1998)

- BS 7799-1:1999 *Code of practice for information security management*
- BS 7799-2:1999 *Specification for information security management systems*

Britská norma BS 7799 (British Standard for Information Security Management) je referenčním dokumentem pro manažery a zaměstnavatele, kteří zodpovídají za informační bezpečnost organizace. Odkaz: http://www.c-cure.org/.
Norma byla v prosinci 2000 přijata ISO a IEC jako mezinárodní norma: *ISO/IEC 17799:2000 Information technology -- Code of practice for information security management* (http://www.iso.ch/cate/d33441.html) což je vlastně první část BS 7799, druhá část *Specification for information security management systems,* bude brzo rovněž touto cestou schválena jako mezinárodní norma.

Bezpečností pro vrstvy OSI modelu se zabývají následující dvě normy:

- ISO/IEC 10181:1996 *Information technology -- Open Systems Interconnection -- Security frameworks for open systems*
  - Part 1: *Overview*
  - Part 2: *Authentication framework*
  - Part 3: *Access control framework*
  - Part 4: *Non-repudiation framework*

    - Part 5: *Confidentiality framework*
    - Part 6: *Integrity framework*
    - Part 7: *Security audit and alarms framework*
- ISO/IEC 11586:1996 *Information technology -- Open Systems Interconnection -- Generic upper layers security*
    - Part 1: *Overview, models and notation*
    - Part 2: *Security Exchange Service Element (SESE) service definition*
    - Part 3: *Security Exchange Service Element (SESE) protocol specification*
    - Part 4: *Protecting transfer syntax specification*
    - Part 5: *Security Exchange Service Element (SESE) Protocol Implementation Conformance Statement (PICS) proforma*
    - Part 6: *Protecting transfer syntax Protocol Implementation Conformance Statement (PICS) proforma*

Kontrolou bezpečnosti výpočetních systémů se zabývají následující normy:

ISO/IEC 10164 *Information technology - Open Systems Interconnection - Systems Management*
Part 7 (1992): *Security alarm reporting function*
Part 8 (1993): *Security audit trail function*
Part 9 (1995): *Objects and attributes for access control*
IEEE P1003.1e *POSIX Part 1: System API - Protection, Audit and Control Interfaces (C language)*
IEEE P1003.2c *POSIX Part 2: Shell and Utilities - Protection and Control Interfaces*
US DoD 5200.28-STD (December 1985): *Department of Defense (DoD) Trusted Computer System Evaluation Criteria*
NCSC-TG-005: *Trusted Network Interpretation*
NCSC-TG-021: *Trusted Database Management System Interpretation*

Poznámka: Pro některé další speciální normy lze nalézt adekvátní popis na adrese: http://www.diffuse.org/secure.html#users

3.11. Finančnictví

Pro finanční a bankovní sektor platí celá řada specifických norem. Jsou to např. ISO 9564 - normy související s používáním PIN (Personal Identification Number), dále ISO 10202 popisující karty používané k finančním transakcím. Problematikou klíčového hospodářství v bankovnictví se zabývají normy ISO 11568. Řízením informační bezpečnosti v bankovním sektoru se zabývá ISO/TR 13569. Jinak do finanční sféry jsou orientovány normy ANSI X9 (viz příslušný přehled) - mají ovšem i širší využití, např. ANSI X9.42 je v současné době pravděpodobně nejlepší popis Diffie-Hellmanova schématu pro výměnu tajného klíče (pro symetrickou kryptografii) a je proto používán i v řadě jiných praktických aplikací. Obdobně lze zmínit i normy ANSI X9.62 a ANSI X9.63, které tvoří aktuální materiál v oblasti norem pro asymetrickou kryptografii využívající eliptické křivky.

3.12. Elektronické platba, elektronický obchod

Dnes i velice „módní“ problematika, která je v současnosti vlastně jednou z nejčastějších aplikací postupů elektronických podpisů (i v širším slova smyslu). Dnes zde již rovněž existuje škála cest, které již jsou obsaženy v příslušných normách (EMV, SET, EDI - např. ISO 9735). Pro zpracování této oblasti by však bylo vhodné zvolit samostatnou studii (viz http://www.semper.org/sirene/outsideworld/ecommerce.html#syst).

4. Problematika certifikace (evaluace) podpisových prostředků, akreditace příslušných institucí.

Toto je relativně samostatná problematika. Níže je je přiložena rozšířená verze článku autora „Certifikace kryptografických prostředků“ (DSM 6/2000).

I pro tuto oblast existují dnes standardizované postupy obsažené v příslušných normách (EN 45010, EN 45011, EN 45012). Normy EN 45010, EN 45011 a EN 45012 specifikují cesty akreditace institucí, které se hodlají zabývat certifikací výrobků a řídících systémů. Tyto normy jsou rovněž opublikovány ISO/IEC jako tzv. Guides 61, 66 a 62. V Evropské Unii má každý členský stát příslušnou akreditační instituci, která je v tomto státě uznávána a provádí tyto akreditace (např. SWEDAC, COFRAC, UKAS, RvA).

V rámci Evropské Unie má být pro problematiku podpisových prostředků a příslušných evaluačních institucí připravováno tzv. jednotné akreditační schéma (dokument Final Report). Pokud se týká problematiky evaluace kryptografických prostředků obecně, pak Evropská Unie bude připravovat jednotnou metodologii v rámci projektu Cryptonessie (odstavec 2.8.).

4.1. Úvod

Tato kapitola se věnuje problematice prostředků kryptografické ochrany dat a prostředků pro elektronický podpis. To jsou prostředky, které jsou používány k pokrytí určitých speciálních oblastí ochrany informací v datových (informačních) systémech. Přitom cílem materiálu je provést určitý přehled existujících postupů v oblasti *certifikace* těchto prostředků a existujících mezinárodních zkušeností v dané oblasti. To je užitečné především ze dvou důvodů. Prvních z nich je možnost určitého převodu (do analogické problematiky v ČR) již získaných zahraničních zkušeností. Druhým je pak zaměření na cesty budování takové celkové struktury certifikačních postupů, aby byla získána maximální možná interoperabilita (převoditelnost) získaných výsledků v mezinárodním měřítku.

V první části proto budou shrnuty některé obecně používané přístupy v dané oblasti. V návaznosti pak budou uvedeny informační zdroje (spolu s odkazy) k existujícím postupům v zemích, kde certifikace kryptografických prostředků má již dostatečnou tradici. Stav řešení problematiky v České republice bude zmíněn jen okrajově – zkušenosti zde teprve vznikají.

Pokud se týká oblasti certifikace podpisových prostředků, pak je třeba říci, že tato oblast je nová v celém světě, nejen u nás a příslušné metodiky jsou teprve vytvářeny. Vzhledem však k tomu, že v současnosti jsou ústřední využívanou metodou elektronických podpisů právě prostředky asymetrické kryptografie (systémy s veřejným klíčem) jsou tyto oblasti velice blízké a používají se často společné postupy.

Instituce

Ve světě je běžné, že postupy vedoucí k certifikaci krypt. prostředků (resp. obecně - bezpečnostních prostředků IT) jsou formulovány ve dvou základních úrovních. První z nich je stanovení centrální certifikační instituce, která dohlíží nad celým certifikačním procesem. Druhou úroveň pak tvoří vlastní vyhodnocovací procesy, které jsou svěřovány jiným (nezávislým nebo i komerčním) organizacím.

Úkoly centrální certifikační instituce spočívají v celkovém organizačním zabezpečení certifikačního procesu, který obsahuje:

- převzetí požadavku na certifikaci;
- předání požadavku schválené vyhodnocovací instituci (ve spolupráci se zadavatelem);
- převzetí výsledků vyhodnocení;
- uzavření certifikačního postupu vydáním (resp. zamítnutím) certifikačního osvědčení.

Centrální certifikační instituce k tomu:

- vydává seznam schválených norem, včetně zahraničních;
- stanoví postupy při provádění konkrétních vyhodnocení, které jsou závazné pro vyhodnocovací instituce (v závislosti na požadované bezpečnostní úrovni);
- vydává seznam certifikovaných prostředků;
- podílí se na akreditaci hodnotících organizací.

Vyhodnocovací instituce pak na základě podkladů získaných od zadavatele provádí konkrétní vyhodnocení příslušných bezpečnostních vlastností. Cílem je vyhodnotit slučitelnost vyhodnocovaného produktu s bezpečnostními normami, které jsou stanoveny centrální certifikační institucí.

Oddělení certifikační instituce od vlastního vyhodnocování vzniklo na základě mezinárodních zkušeností. Smyslem je především zabezpečit objektivnost prováděných postupů.

Je třeba si také uvědomit, že ne všechny bezpečnostní aspekty lze zachytit soustavou norem. Existují i určitá specifika, která vyhodnocovací instituce uplatňuje výlučně na základě svého know-how a také na základě aktuálních znalostí, které ještě nejsou začleněny do norem.

Při přebírání norem i při jejich novém rozpracování je nezbytné zajistit jejich slučitelnost s dokumentem Common Criteria. Tento dokument je v současnosti výchozím ideovým materiálem v oblasti posuzování bezpečnostních aspektů prostředků IT.

4.2. K obsahové stránce certifikace

Proces certifikace kryptografických prostředků lze charakterizovat z hlediska cílů tohoto procesu a z hledisek užívaných postupů.

Cíle

a) Vytvoření certifikačního schématu pro efektivní (z hlediska vynaložených nákladů) a účelné bezpečnostní vyhodnocení (evaluaci) a certifikaci kryptografických prostředků.
b) Naplnění odpovídajících požadavků hospodářského sektoru a státní administrativy.
c) Vytvoření podmínek pro mezinárodní uznávání příslušných certifikátů.

Používané postupy

a) V rámci certifikačního schématu se zřizuje státní certifikační pracoviště, jehož úkolem je provést certifikaci provedených vyhodnocení kryptografických prostředků a systémů a spolupracovat s jinými státy v dané oblasti při vzájemném uznávání takovýchto certifikátů. Za tímto účelem je certifikační pracoviště budováno tak, aby vyhovělo normě EN 45011 (ISO/IEC Guide 65:1996) – ČSN EN 45011, listopad 1998.
   Toto pracoviště zároveň určuje organizační a procedurální rámec pro provádění vyhodnocení (evaluací), včetně výběru komerčních hodnotících organizací (KHO), které provádí vyhodnocení a zároveň stanoví schválené techniky a procedury.

b) Pracoviště KHO (resp. státní vyhodnocovací pracoviště) provádějící vyhodnocení podléhají akreditaci u státního certifikačního pracoviště. Tato akreditace stanoví požadavky na základě následujících 4 principů:
   - nestrannost;
   - objektivnost;
   - opakovatelnost;
   - prokazatelnost.

Zároveň musí být ověřena spolehlivost tohoto vyhodnocovacícho pracoviště.

c) Podstatou certifikace je nezávislé stvrzení platnosti závěrů provedených vyhodnocení a zajištění srovnatelnosti těchto výsledků s výsledky jiných vyhodnocovacích institucí. Provedená certifikace stvrzuje, že:
   - kryptografický prostředek (systém) splňuje stanovené bezpečnostní cíle (při definované úrovni bezpečnosti);
   - vyhodnocení bylo provedeno na základě norem a ve shodě s nimi, které definuje certifikační schéma.

d) Státní certifikační pracoviště stanoví příslušný seznam norem pro vyhodnocování bezpečnostních vlastností kryptografických prostředků (systémů). Tento dokument obsahuje:
   - seznam schválených kryptografických algoritmů (symetrická a asymetrická kryptografie, hashovací funkce, generátory pseudonáhodných posloupností, kryptografické protokoly např. pro výměnu klíčů atd.);
   - normy pro posouzení bezpečnostních vlastností konkrétních implementací kryptografických modulů, jako je např. FIPS-140. Těmito moduly mohou být např.:
   - fyzicky oddělená šifrovací zařízení;
   - samostatné desky v počítačové jednotce;
   - čipové karty obsahující kryptografický algoritmus;
   - softwarové moduly pro různá prostředí;
   - hardwarové moduly pro další různá prostředí (např. HW nosiče klíčů);
   - komplexní návrhy klíčového hospodářství (např. v rámci PKI.)

e) Státní certifikační pracoviště stanoví závazné postupy při vyhodnocování kryptografických prostředků pro práci jednotlivých hodnotících pracovišť. Tyto postupy obsahují:
   - odkazy na příslušné normy, jejichž splnění je nezbytné pro daný typ prostředku při dané ověřované úrovni bezpečnosti;
   - formulované cíle vyhodnocování bezpečnostních vlastností pro daný typ prostředku a při dané ověřované úrovni bezpečnosti.

f) Státní certifikační pracoviště stanoví obsah podkladů, které zadavatel musí dodat při žádosti o certifikaci. Vyhodnocovací pracoviště si může vyžádat doplnění těchto podkladů.

g) Vyhodnocovací pracoviště vychází pří své činnosti z metodologie dané v dokumentu Common Criteria provádí ji na základě norem schválených státním certifikačním pracovištěm a v souladu s cíly definovanými tímto pracovištěm.

h) Součástí postupů obvykle bývá i detailnější organizační uspořádání - úloha managementu, administrativní otázky (evidence provedených certifikací), další vývoj certifikačních metodologických postupů v návaznosti na nové výsledky vědy a techniky, audity vyhodnocovacích pracovišť, atd.

i) Někde ve světě vstupuje do vyhodnocovacího procesu i tzv. „sponzor“. Tím se míní např. instituce, která chce např. vyhodnocovaný prostředek zakoupit pro své potřeby a financuje celý proces certifikace nebo jeho část.

4.3. Obsahová stránka certifikace (evaluace) vlastního kryptografického algoritmu

Certifikační instituce má seznam jí schválených (certifikovaných) algoritmů, který vzniká, resp. je doplňován, následovně:

a) schválení převzetí některých algoritmů z mezinárodních norem
(lze provést i nezávislou analýzu – její obsah popisuje bod b)

b) kryptografický a kryptoanalytický rozbor nově navrhovaného algoritmu (týká se symetrické kryptografie, asymetrické kryptografie a hash. funkcí, ale i např. generátoru náh. čísel) – tj. matematickou analýzu zahrnující mimo jiné:
   - algebraické a statistické vlastnosti kryptoschematu;
   - odolnost vůči kryptoanalytickým metodám (velice rozsáhlá oblast zahrnující např. diferenciální a lineární kryptoanalýzu blokových šifer, objektivní odhady výpočetní složitosti existujících kryptoanalytických metod – např. pro účely faktorizace velkých čísel, hledání diskrétního logaritmu atd., vývoj specifických metod pro dané kryptoschema a další) ;
   - stanovení doporučovaných délek klíčů;
   - posouzení implementačních vlastností v různých prostředích;
   - matematické přístupy ke generování parametrů algoritmu;
     (např. generování náhodných parametrů pro eliptické kryptosystémy, generování náhodných prvočísel, použité S-boxy atd.);
   - komplexní posouzení algoritmů (např. práce jednotlivých módů blokových šifer, tzv. „paddings“ – zpracování krátkých bloků);
   - zadání verifikačních postupů (testovací vektory, příkladem může být velice rozsáhlá soustava testů zpracovaná nyní pro US normu 3-DES v dokumentu NIST Special Publication 800-20: Modes of Operation Validation System for Triple Data Encryption Algorithm. Requirements and Procedures)

Evaluace implementace kryptografického algoritmu:

Bývají rozlišovány následující dvě základní úrovně této evaluace.

Evaluace v užším smyslu

Týká se bezpečnostních vlastností implementace samotného algoritmu. Jsou samozřejmě rozlišovány hardwarové a softwarové implementace, dále např.:

a) musí existovat definovaný seznam používaných (mezinárodních) norem a doporučení pro tyto účely (např. FIPS-140, ASNI X9.66)

b) vlastní postupy obsahující např. vyhodnocení:
   - vlastnosti použitých generátorů náhodných znaků (GNZ - včetně tzv. seed – základního zdroje „náhodnosti“), použité algoritmy, hashovací funkce, atd.;
   - generování náhodných nepredikovatelných klíčů, inicializačních vektorů, atd.;
   - bezpečná distribuce klíčů;
   - bezpečnost uložení klíčů a cesty jejich likvidace po ukončení doby platnosti klíčů;
   - vlastnosti použitých protokolů (výměna symetrických klíčů, podpisová schémata, atd.);
   - typy kryptografických algoritmů (symetrické, asymetrické);
   - použití hesla (password, passphrase, PIN, atd.);

- z technických vlastností např.
  - typ použité komunikace;
  - způsob upgrade prostředku;
  - hardwarové vlastnosti GNZ;
  - vlastnosti použité technologie (odolnost proti poruchám – i záměrným, vyzařování, neoprávněným zásahům, měření spotřeby - power analysis, atd.);
  - vlastnosti použité konstrukce (např. zdvojení obvodů, oddělení bezpečnostních oblastí, atd.);
  - vlastnosti při počátečním nastavování;
  - implementované vnitřní testy, diagnostika;
  - bezpečnostní opatření při výrobě, servisu;
  - technické vlastnosti a práce se směnnými prvky;
- vlastnosti zdrojového kódu, při vývoji použité kryptografické softwarové jádro
- použité délky klíčů;
- obnova klíče (key recovery, key escrow);
- použité normy;
- přiložená dokumentace (její kvalita, dostatečnost manuálů, atd.);
- přiložené směrnice pro používání kryptografického prostředku (doba platnosti klíčů, bezpečnostní aspekty lidského činitele, atd.);
- testy metodou černé skříňky (black box);
- bezpečnostní rozbor (ochrana kryptograficky důležitých informací, např. při softwarové realizaci ochrana klíčů, otevřeného textu, atd..), kryptografická odolnost proti tech. poruchám (analýza rizik);
- deinstalace prostředku;
- minimální požadavky na obsluhu.

Evaluace v širším smyslu

Provádí se včetně okolí, ve kterém je algoritmus začleněn (sem spadá např. celkové posouzení PKI). Jejím obsahem je např. komplexní posouzení klíčového hospodářství, kryptografických protokolů, vlastnosti vydělených bodů počítačové sítě (servery, sklady klíčů, práce s digitálními certifikáty, autentizace a identifikace uživatelů, přístupové mechanizmy, riziková analýza, atd.)

Celkový postup evaluace pro konkrétní prostředek bývá tedy následovný:
Krok 1. Evaluační instituce projde všechny použité kryptografické algoritmy - pokud jsou všechny na seznamu certifikovaných, přechází se ke kroku 2 . Pokud nejsou, pak je buď zamítána evaluace (a tedy i certifikace) prostředku (z hlediska tohoto algoritmu) nebo je prováděna celková kryptoanalýza nových algoritmů a na základě jejího výsledku jsou tato zařazeny či nezařazeny do seznamu certifikovaných algoritmů (samozřejmě někdo to musí zaplatit a i doba vyhodnocení bude výrazně vyšší).
Krok 2. Provede se evaluace konkrétního prostředku na základě dodaných podkladů (přitom je předem specifikováno, co všechno takové podklady musí obsahovat).
Krok 3. Po pozitivním uzavření evaluace rozhodne certifikující instituce zda vydá potřebný certifikát (evaluaci obvykle provádí jiná instituce – ta ji ovšem provádí dle definovaných postupů, které schválila certifikační instituce)

Pozn.: Certifikující instituce (např. v ČR NBÚ) může mít k dispozici další informace, které hodnotící organizace nemají a také právě ona nese odpovědnost za certifikaci.

V procesu certifikace jsou centrálním bodem tzv. kritéria - tím jsou míněny vlastně jakési „normy“, proti nimž probíhá příslušná evaluace. Kriteria stanoví obvykle několik stupňů „přísnosti“ prováděného testování a na základě toho získaných úrovní důvěryhodnosti. V současné době jsou používána především tzv. Common Criteria (CC – k historii jejich vzniku viz článek L. Nováka v tomto čísle DSM).

Kritéria CC upravují základní filosofii, která je při vyhodnocování bezpečnostních vlastností (nejen) kryptografichých prostředků používána. Nejsou to však samozřejmě jediné normy, o které se vlastní průběh evaluace opírá. Ke zhodnocení vlastností konkrétního prostředku je používána celá další široká škála norem. Jsou to např. normy, které specifikují použité kryptografické algoritmy, hashovací funkce, kryptografické a autentizační protokoly, atd.

4.4. Certifikace kryptografických prostředků ve světě

V přiložené tabulce je proto uveden určitý přehled webovských stránek, kde lze získat další informace.

USA

National Institute of Standards and Technology: http://www.niap.nist.gov/
NIST certifikované produkty: http://csrc.nist.gov/cryptval/140-1/1401val.htm
ICSA (soukromá certifikující instituce): http://www.icsa.net/index.shtml

Kanada

Communication Security Establishment: http://www.cse.dnd.ca/
Common Criteria Evaluation and Certification Scheme:
http://www.cse-cst.gc.ca/cse/criteria/english/index.htm
CSE certifikované produkty: http://www.cse.dnd.ca/cse/criteria/english/cpl.htm

Německo

Bundesamt für Sicherheit in der Informationstechnik: http://www.bsi.de
Certifikované produkty: http://www.bsi.de/aufgaben/ii/zert/index.htm
Další informace: http://www.dud.de
TÜV-Informationstechnik GmbH: http://www.tuevit.de
Der Deutsche AkkreditierungsRat: http://www.dar.bam.de

Velká Británie

UK IT Security Evaluation and Certification Scheme
http://www.itsec.gov.uk/
http://www.cesg.gov.uk/
ITSEC certifikované produkty: http://www.itsec.gov.uk/products/
Jedna z evaluačních institucí (Rycombe Consulting): http://www.rycombe.com/

Francie

Service de Certification de la Sécurité des Technologies de l'Information
http://www.scssi.gouv.fr/
SCSSI certifikované produkty: http://www.scssi.gouv.fr/present/chiffre/liste.html

Nizozemí

Netherlands National Communications Security Agency
Postbus 20061; NL 2500 EB Den Haag; Netherlands; Tel: +31 70 348 5637
Email: criteria@nlncsa.minbuza.nl

Australie – Nový Zéland

Defence Signals Directorate: Australasian Information Security Evaluation Programme
http://www.dsd.gov.au/infosec/services/aisep2.html
AISEP certifikované produkty
http://www.dsd.gov.au/infosec/aisep/EPL.html

USA

National Institute of Standards and Technology: http://www.niap.nist.gov/
NIST certifikované produkty: http://csrc.nist.gov/cryptval/140-1/1401val.htm
ICSA (soukromá certifikující instituce): http://www.icsa.net/index.shtml

Kanada

Communication Security Establishment: http://www.cse.dnd.ca/
Common Criteria Evaluation and Certification Scheme:
http://www.cse-cst.gc.ca/cse/criteria/english/index.htm
CSE certifikované produkty: http://www.cse.dnd.ca/cse/criteria/english/cpl.htm

Německo

Bundesamt für Sicherheit in der Informationstechnik: http://www.bsi.de
Certifikované produkty: http://www.bsi.de/aufgaben/ii/zert/index.htm
Další informace: http://www.dud.de
TÜV-Informationstechnik GmbH: http://www.tuevit.de
Der Deutsche AkkreditierungsRat: http://www.dar.bam.de

Velká Británie

UK IT Security Evaluation and Certification Scheme
http://www.itsec.gov.uk/
http://www.cesg.gov.uk/
ITSEC certifikované produkty: http://www.itsec.gov.uk/products/
Jedna z evaluačních institucí (Rycombe Consulting): http://www.rycombe.com/

Francie

Service de Certification de la Sécurité des Technologies de l'Information
http://www.scssi.gouv.fr/
SCSSI certifikované produkty: http://www.scssi.gouv.fr/present/chiffre/liste.html

Nizozemí

Netherlands National Communications Security Agency
Postbus 20061; NL 2500 EB Den Haag; Netherlands; Tel: +31 70 348 5637
Email: criteria@nlncsa.minbuza.nl

Australie – Nový Zéland

Defence Signals Directorate: Australasian Information Security Evaluation Programme
http://www.dsd.gov.au/infosec/services/aisep2.html
AISEP certifikované produkty
http://www.dsd.gov.au/infosec/aisep/EPL.html

Evropská Unie

Kromě již zmíněného unifikovaného přístupu na základě dokumentu Common Criteria připravuje Evropská Unie podrobnější jednotný přístup k řešení problematiky certifikace kryptografických (ale i podpisových) prostředků v rámci projektu Cryptonessie: https://www.cosic.esat.kuleuven.ac.be/nessie/. Jedním z cílů tohoto projektu je zpracování návrhu metodologie pro bezpečnostní a spolehlivostní vyhodnocování tzv. kryptografických primitivů. To jsou vlastně základní bloky kryptografických operací (např. podpis pomocí zadaného algoritmu atd.). Předpokládá se, že rovněž bude zpracována určitá evropská varianta metodologie obsažené v dokumentu FIPS-140, tj. vlastně mezistupeň mezi výše zmíněnými dvěma postupy (Common Criteria a vyhodnocování samotných kryptografických primitivů). Podrobnější informace k prokektu NESSIE lze získat v článku autora v Crypto-Worldu 12/2000.

Nepochybně tento postup bude svázán s již vyhlášenými pravidly pro celkovou infrastrukturu míst provádějících akreditaci, certifikaci, inspekci, zkoušení, kalibraci atd. Komise ES svůj postoj k této otázce specifikovala v globální koncepci přístupu ke zkoušení a certifikaci, kde se mimo jiné uvádí:

- nebude budován žádný evropský nadnárodní systém, ale budou uznávány národní systémy akreditace, certifikace, inspekce, zkoušení, kalibrace atd.,
- akreditační orgány, certifikační orgány, inspekční orgány, zkušební a kalibrační laboratoře se budou řídit ustanoveními evropských norem EN řady 45000,
- systémy zabezpečující jakost výrobků musejí odpovídat požadavkům norem ISO řady 9000,
- odpovědnost za jakost výrobků nese jednoznačně výrobce,
- specifikuje se používání značky CE,
- upravuje se vzájemné uznávání zkoušek, kalibrací a certifikátů.

Přitom v regulované sféře bude ES v souladu se svými zákony a mezinárodními závazky podporovat mezinárodní obchod a uzavírat s třetími zeměmi dohody o vzájemném uznávání za předpokladu, že:

- místa třetích zemí zapojená do prohlašování shody poskytují záruky jako místa ES,

vzájemné uznávání je omezeno na zkušební protokoly, certifikáty a značky shody.

V neregulované sféře je vše ponecháno na smluvních vztazích.

Základem jednotných pravidel akreditace využívaných pro poskytování průkazu shody jsou ČSN EN řady 45000. Tyto evropské normy jsou ve svém znění obecné a proto každý národní akreditační orgán podává výklad ke znění jejich jednotlivých ustanovení.
Viz Český institut pro akreditaci, o.p.s.: http://www.cai.cz.

Řešení problematiky certifikace (včetně certifikace kryptografických a podpisových prostředků formulují dokumenty EU takto. Budou existovat určité závazné evropské dokumenty, kriteria, normy pro všechny členské (resp. spolupracující) země. Přitom vlastní certifikaci si však budou provádět samotné členské země na základě vlastních předpisů, které ovšem musí být ve shodě s těmito evropskými dokumenty.

4.5. Podpisové prostředky

K problematice podpisových prostředků platí prakticky vše o čem již bylo výše hovořeno.
Navíc je třeba zmínit některé současné dokumenty, které jsou zpracovávány pověřenými orgány EU. Směrnice EU k elektronickým podpisům vytváří základní filosofii pro řešení této problematiky. V návaznosti na tento dokument je zpracovávána celá serie norem, které řeší konkrétní postupy pro řešení v jednotlivých oblastech (viz výše uvedené dokumenty ETSI a CEN ESSI).

4.6. Česká republika

V České republice základní přístupy k certifikaci kryptografických prostředků upravuje vyhláška NBÚ č.76/1999 (Vyhláška o zajištění kryptografické ochrany utajovaných skutečností, provádění certifikace kryptografických prostředků a náležitostech certifikátu) v návaznosti na zákon č.. 148/1998 Sb.(o ochraně utajovaných skutečností a o změně některých zákonů, ve znění zákona č. 164/1999 Sb.)

Problematiku elektronického podpisu řeší zákon 227/2000 Sb. (zákon o elektronickém podpisu). Současným úkolem Úřadu na ochranu osobních údajů je připravit v návaznosti na tento zákon soubor vyhlášek, které budou upravovat faktické fungování problematiky elektronických podpisů. Vzhledem k formulacím zákona ukládajícím nezbytnost provádění certifikace tzv. bezpečných podpisových prostředků; budou se tyto vyhlášky zabývat i metodologií certifikace podpisových prostředků v ČR.

5. Další literatura, zdroje na webu

Jaroslav Pinkava: Normy v kryptografii, Crypto-World (zatím neukončený seriál, první díl opublikován v čísle 9/2000) – http://www.mujweb.cz/veda/gcucmp
V současné době jsou připravovány další díly tohoto seriálu.
Poznámka: V češtině zatím k dané problematice existuje málo titulů, samozřejmě většina literaratury komentující a analyzující danou problematiku je v angličtině (nebo např. v německém jazyce). Některé z těchto informací jsou však obtížněji dostupné (organizace vydávající normy požadují za své služby příslušné poplatky), některé však existují v určité podobě i na webu. Příkladem jsou následující reference

SEMPER, Sirene
http://www.semper.org/sirene/outsideworld/standard.html

Webstart Communications:
http://www.cmpcmm.com/cc/standards.html

E U R O P E A N C O M M I T T E E F O R S T A N D A R D I Z A T I O N
http://www.cenorm.be/standardization/standardization.htm

CEN/ISSS Information Society Standardization System
http://www.cenorm.be/isss/

Electronic Signatures (E-SIGN) Workshop
http://www.cenorm.be/isss/Workshop/e-sign/Default.htm

ETSI: Electronic Signatures and Infrastructures
http://www.etsi.org/sec/el-sign.htm

Information Security Standards
http://www.diffuse.org/secure.html#users

Dále - samozřejmě pokud se týká norem z problematiky obecné ochrany dat (ITSEC, Common Criteria, existuje i v českém jazyce celá řada článků věnující se této problematice (řadu z nich lze nalézt např. v DSM ale i v jiných časopisech).