Příručka : Standardy a normy (ALG082, MFF UK, 2004)

Úvod do klasických a moderních metod šifrování ALG082
Standardy a normy

Ver 2.0

Pavel Vondruška

pavel.vondruska@ct.cz, pavel.vondruska@crypto-world.info
http://crypto-world.info

Cíl přednášky:

- seznámit posluchače se základními pojmy z oblasti standardů a norem, vytváření, přijímání
- seznámit posluchače s dělením norem a jejich závazností / vynutitelností
- seznámit s nejznámějšími systémy norem a de-facto norem (RFC, PKCS, ISO, ETSI, CEN, …)
- blíže představit úpravu národní technické normalizace a proces tvorby českých norem a přejímání cizích zahraničních norem
- představit přehled norem v oblasti bezpečnosti informačních technologií
- seznámit se základními kritérii hodnocení bezpečnosti IT (nejznámější normy pro hodnocení kryptografické bezpečnosti)

Obsah

I. Úvod
I.1 Základní pojmy
I.2 Jedno z možných členění

II. RFC (Request For Comment)
II.1 Úvod
II.2 Dostupnost dokumentů
II.3 Číslování dokumentů (RFC number)
II.4 Typy dokumentů
II.5 RFC - jiné členění
II.6 Přehled vybraných RFC pro PKI
II.7 Střípky

III. Standardy PKCS (Public-Key Cryptographic Standards)

IV. České technické normy a svět
IV.1 Právní úprava národní technické normalizace
IV.1.1 Charakteristika české technické normy
IV.1.2 Pojem "harmonizovaná česká technická norma"
IV.1.3 Zabezpečení tvorby norem

IV.2 Národní normalizační proces
IV.2.1 Tvorba norem
IV.2.2 Obecné zásady pro stavbu, členění a úpravu českých technických norem
IV.2.3 Přejímání evropských a mezinárodních norem

IV.2.4 Zásady přejímání norem
IV.2.5 Značka shody s českou technickou normou

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

V. Přehled norem v oblasti bezpečnosti informačních technologií (normy vyvíjené ISO/IEC JTC1 SC27 a ISO TC 68) zavedených do soustavy českých norem
V.1 Normy z oblasti bezpečnosti informačních technologií
V.2 Přehled ČSN z oblasti bezpečnosti informačních technologií

VI. Přehled mezinárodních a národních normalizačních institucí
VI.1 Mezinárodní standardizační instituty
VI.2 Regionální standardizační instituty
VI.3 Národní standardizační instituty

VII. Přehled některých základních kritérií hodnocení bezpečnosti IT
VII.1 Úvod
VII.2 Trusted Computer System Evaluation Criteria (TCSEC)
VII.3 Information Technology Security Evaluation Criteria (ITSEC)
VII.4 Canadian Trusted Computer Product Evaluation Criteria (CTPEC)
VII.5 Common Criteria
VII.6 Kritéria pro hodnocení bezpečnosti IT - ISO/IEC 15408
VII.7 Federal Information Processing Standard (FIPS 140-1 a FIPS 140-2)

I. Úvod

Existuje mnoho kategorií standardů (někdy nazývaných také *normy*), zabývajících se tvorbou bezpečných informačních systémů. Jde o standardy mezinárodní, regionální (např. evropské standardy), národní standardy, standardy státní správy některého státu, standardy určitého zájmového sdružení nebo průmyslové standardy.

Význam každého z těchto standardů zcela závisí na rozsahu jeho použití. Tento rozsah použití nemusí vždy odpovídat úmyslům tvůrců standardu (PKCS). Známe mnoho případů, kdy ambiciózní standardy upadly v zapomnění, nebo kdy původně zcela opomíjený standard získal celosvětový význam (RFC).

Zpravidla však platí, že nejširší platnost mají standardy mezinárodní a regionální. Použití národních standardů a standardů státní správy zpravidla nepřesahuje hranice státu, ve kterém byly tyto standardy vytvořeny. Výjimkou z tohoto pravidla jsou národní standardy USA (označované ANSI) a standardy státní správy USA (FIPS), které jsou někdy používány i mimo hranice USA.

I.1 Základní pojmy

Řešení, které je založeno na specifické formě vázanosti na jediného výrobce, dané nikoliv jeho monopolním postavením, ale neslučitelností jím používaného technického řešení s tím, které používají jiní výrobci se v angličtině označuje přívlastkem **proprietary**, stejně tak jako produkty, které z tohoto řešení vycházejí.

Prosadit vlastní řešení, a to ještě se ziskem, si však v dlouhodobém výhledu mohou dovolit jen ty největší firmy. Menší firmy se ve vlastním zájmu musely přizpůsobit těm řešením, které si zvolily velké firmy. Nešlo přitom ani tak o převzetí technologií či výrobních postupů (které jsou často pečlivě chráněné), jako spíše o převzetí konvencí, parametrů a protokolů, s cílem zajistit **kompatibilitu** (slučitelnost) vlastních produktů s produkty jiných výrobců. Názorným příkladem může být architektura osobních počítačů PC - zde se prakticky všichni výrobci přizpůsobili řešení, které si podle svého zvolila jediná firma - IBM.

Řešení, kterému se přizpůsobují různí výrobci a které tak představuje určitou společnou konvenci, zajišťující vzájemnou kompatibilitu produktů od různých výrobců, si již zaslouží přívlastek **standardní**, jako protipól anglického **proprietary**. Samotný obsah resp. podstata tohoto řešení se pak v širším slova smyslu označuje jako **standard.**

Standardní řešení resp. standard může vniknout tak, že se z podnětu či pod záštitou určité instituce, která je k tomu příslušná, sejde skupina odborníků a vypracuje návrh příslušného řešení. Ten je posléze kodifikován (tj. dostane formu oficiálního dokumentu příslušné instituce), a pak je prosazován do praxe. Podstatné přitom je, že zmíněné standardizační instituce obvykle nereprezentují přímo jednotlivé výrobce (i když tito se na jejich práci mohou významně podílet).

Standard, který je kodifikován, je standardem **de jure**. Jeho závaznost pro výrobce i uživatele je ovšem různá podle toho, jaký má právní statut resp. jaký je statut toho, kdo jej formálně vydává.

Například standardy, vypracované a vydávané mezinárodními standardizačními institucemi, mají často pouze formu **doporučení** a po formální stránce nejsou právně závazné.

Právní závaznost pak mívají až návrhy ve formě **norem**, které v rámci jednotlivých zemí vypracovávají k tomu oprávněné instituce, často na základě doporučení, přijatých mezinárodními organizacemi. Právní závaznost tyto normy mít však nemusí – záleží na postavení národní normotvorné instituce a konkrétní národní legislativy.

Samotní výrobci nemají možnost vydávat standardy *de jure,* neboť obvykle nemohou vydávat oficiální doporučení či dokonce normy, závazné pro jiné výrobce. Pokud jejich vlastní řešení spontánně a na dobrovolném základě přebírají i jiní výrobci, stává se toto řešení standardardem **de facto**.

Jsou ovšem i případy, kdy se vlastní ("proprietary") řešení určitého výrobce může stát "oficiálním" standardem (standardem *de jure*). Jde o taková řešení, která se ukáží být natolik životaschopná, že se nejprve stanou standardy *de facto*, a posléze je příslušné standardizační instituce převezmou jako "své" standardy - buď bez jakýchkoli změn, nebo s určitými úpravami. Příkladem může být koncepce sítí Ethernet, která původně vznikla jako vlastní řešení firmy Xerox, záhy se stala standardem *de facto*, a posléze se s drobnými úpravami stala i standardem *de jure* (standardem IEEE 802.3).

Standardy v průmyslovém světě znamenají jednu ze zásadních cest předávání znalostí, snižování nákladů a k umožnění vzájemné spolupráce a kompatibility produktů.

I.2 Jedno z možných členění

V bezpečnosti IT lze standardy členit do skupin:
-- základní standardy -- pro obecné požadavky uživatelů -- např. bezpečnostní architektura OSI, mechanismy autentizace entit atd.,
-- funkční standardy -- pro zajištění a certifikaci produktů, pro služby -- vysvětlují obecný přístup k využití základních standardů (např. požadavky k autentizaci dat, základům integrity atd.),
-- kritéria hodnocení -- pro hodnocení produktů a systémů (např. TCSEC, ITSEC, CC),
-- průmyslové standardy a postupy -- technické a procedurální standardy vyžadované specifickými skupinami uživatelů nebo společností (např. bankovní standardy),
-- výkladové dokumenty -- průvodce, slovníky pro informovanost a vzdělání (pokyny k ochraně soukromí, seznamy termínů atd.).

Poznámka:
Při přípravě tohoto a následujících sedmi kapitol jsem použil mimo vlastních článků a originálních dokumentů i materiály autorů:
Beneš, Hanáček, Pužmanová, Peterka, Pinkava, Staudek, Wallenfels

II. RFC (Request For Comment)

II.1 Úvod

Historickým vývojem vznikla tradice publikování dokumentů RFC. Její vznik se datuje do roku 1969 a souvisí se zprovozněním ARPANETu, ze kterého se později vyvinul dnešní Internet.

Postgraduální studenti a další řešitelé ARPANEtu, jejichž postavení jim neumožňovalo, aby své četné nápady a podněty, mnohdy velmi užitečné a podnětné, nějak vnucovali svým profesorům a intenzivněji se domáhali jejich pozornosti, vé návrhy proto začali sepisovat ve formě dokumentů, kterým dali výstižné pojmenování Request For Comment (doslova: žádost o komentář). Tyto dokumenty předkládali těm, kterých se týkaly, resp. kteří byli kompetentní je posuzovat, přijímat požadovaná rozhodnutí apod.

Tradice publikování dokumentů RFC vydržela až do dnešních dnů. Změnil se ale věcný obsah a celkový smysl dokumentů RFC - s postupem času to stále méně byly náměty a nápady, usilující o vznik nějakého řešení, a čím dál tím více to byla tato řešení jako taková.

Dnes jsou dokumenty RFC používány jako specifická forma dokumentace, vydávána pro potřeby Internetu (ale nepřímo i pro potřeby mnohem širšího okruhu sítí a služeb). „Vydavatelem“ RFC je IETF (*Internet Engineering Task Force).*

Pro správné pochopení významu dokumentů RFC je potřebné si ještě uvědomit a náležitě zdůraznit, že jejich obsahem nejsou zdaleka jen standardy - tedy popisy řešení, která mají povahu závazných standardů (byť standardů "de facto", a nikoli "de jure", ale přesto velmi důsledně uznávaných a dodržovaných). Ve formě dokumentů RFC jsou vydávány i jiné dokumenty, například návody, doporučení, či vysvětlení, a v poslední době i stanoviska a názory. Do dnešního dne bylo vydáno více než 3500 dokumentů RFC, a početně mezi nimi převažují právě takovéto ne-standardy. Faktických standardů je tedy početně méně.

Obecně se považují RFC za bezkonkurenčně „nejčtivější“ specifikace (doporučuji srovnat zejména s doporučeními ITU-T nebo normami IEEE či ISO).

II.2 Dostupnost dokumentů

RFC jsou veřejně dostupná (http://www.ietf.org/rfc.html), ale zdaleka ne všechna jsou standardy v rámci internetové komunity.

V listopadu 2001 bylo pouze 61 RFC schválenými, plnoprávnými *de facto* normami (*RFC 3000 Internet Official Protocol Standards*) a jsou vyjma čísla RFC také označeny číslem normy (STD #). K 16.4.2003 je celkem 62 takovýchto specifických norem.

Dokumenty RFC v celkovém počtu **3751** (k 12.4.2004) již obsahují statisíce stránek textu. Pro vyhledávání se dá využít tzv. index, který je dostupný na : http://www.ietf.org/iesg/1rfc_index.txt , součástí citace v indexu je i aktuální status dokumentu.

II.3 Číslování dokumentů (RFC number)

Dokumenty RFC jsou číslovány - každý nově vydaný dokument je opatřen svým pořadovým číslem, a pod tímto číslem je také nejsnáze a přitom i jednoznačně identifikovatelný (k jednoznačnému určení stačí např. zápisy jako RFC1234, RFC2003 apod.). Další významnou vlastností dokumentů RFC je skutečnost, že se nikdy nemění - jakmile je konkrétní dokument jednou vydán, pod určitým pořadovým číslem, nemění se ani jeho číslo, ani jeho obsah (ani jeho slovní název). Je-li potřeba provést nějakou změnu v tom, co dokument RFC popisuje, neřeší se to změnou již existujícího dokumentu RFC, ale vydáním nového dokumentu, s novým pořadovým číslem (takovým, jaké je právě "na řadě". Tento nový dokument RFC pak ve svém záhlaví nese poznámku o tom, že "zneplatňuje" předchozí dokument RFC s příslušným číslem (ev. několik takovýchto dokumentů).

II.4 Typy dokumentů

Proposed standards , Draft standards , Internet standards (plné de facto normy)
Experimental, Informational, Prototype, Historic

Standards Track - Proposed Standard, Draft Standard, Internet Standard

První tři skupiny skupiny tvoří vlastně tři stádia, kterými musí projít každý návrh na cestě k definitivní podobě standardu (tedy: Proposed Standard, Draft Standard a Internet Standard). Představují jednu konkrétní trajektorii, určenou pro takové dokumenty, které aspirují na to, aby se staly standardem. Této trajektorii se přitom říká "Standards Track".

Každé řešení, které se má stát standardem, musí být předloženo nejprve ve formě tzv. navrhovaného standardu (Proposed Standard), a musí prokázat svou životaschopnost nejméně na dvou na sobě nezávislých implementacích. Nejdříve po půl roce pak může návrh přejít do stádia "Draft Standard" (předběžný standard), ve kterém se musí zdržet nejméně čtvrt roku, a k postupu do finálního stádia "definitivního standardu" (Internet Standard) musí být nashromážděny dostatečné provozní zkušenosti s příslušným řešením. Během všech tří těchto stádií jsou příslušné dokumenty publikovány jako dokumenty RFC.

Off-Track – Informational, Experimental, Prototype, Historic

Vedle výše popsané trajektorie "Standards Track“ existuje i druhá trajektorie, označovaná "Off-Track", do které patří hned čtyři druhy dokumentů (přičemž termín "trajektorie", resp. anglické "track", zde není až tak na místě, protože většina dokumentů zde "nepostupuje" podobným způsobem, jako je tomu u návrhů standardů). Patří sem čtyři kategorie dokumentů RFC: informational, experimental, protoype a konečně historic.

Informational RFC (informační) označuje dokument, který je zamýšlen jako informativní materiál - tedy takový, který vysvětluje, radí, přináší doplňující informace atd. Dokumentů RFC tohoto typu je početně zdaleka nejvíce.

Experimental RFC (experimentální) – takto označené dokumenty obsahují zajímavé informace o protokolech a technologiích, které nemají zřejmou šanci se masově ujmout, ale je dobré o nich veřejně vědět.

Prototype RFC – jedná se o řešení, která jsou zatím ve stádiu experimentu, ale se záměrem někdy v budoucnu přejít do "standards-track" a stát se standardem.

Historic RFC (historickou) se specifikace stává, jestliže je překonána svým následovníkem a/nebo se úplně přestane v Internetu používat.

II.5 RFC – jiné členění

Standard (STD)

Skutečnost, že dokument RFC se nikdy nemění, přináší mnoho výhod, ale také některé nevýhody. Nikomu se sice nemůže stát, že by měl v ruce neaktuální exemplář konkrétního dokumentu RFC (s konkrétním číslem), ale může se mu stát, že se zabývá určitou problematikou a má v ruce dokument RFC řešící tuto problematiku, který již byl překonán (zneplatněn) novějším dokumentem RFC, který řeší tutéž problematiku. Aby se problémům tohoto typu předešlo, zavedla se časem další klasifikace dokumentů RFC, označovaná nyní jako STD (od: standard). Důvodem pro její specifické pojmenování je fakt, že je omezena jen na dokumenty charakteru platných standardů (Internet Standard), a netýká se tedy všech dokumentů RFC. Pro názornou představu je možné připodobnit dokument RFC k prázdným deskám (rychlovazači), které mají na svém hřbetě pevně nadepsanou určitou konkrétní problematiku - do těchto "desek" se pak vkládají ty dokumenty RFC, které se zabývají příslušnou problematikou a v daném okamžiku nebyly zneplatněny novějšími dokumenty RFC. Dokument STD je tedy vždy totožný s některým dokumentem RFC (nebo s několika dokumenty RFC, které řeší jednotlivé části dané problematiky), ale na rozdíl od dokumentů RFC se dokumenty STD v čase mění (je vyměněn obsah pomyslných desek novým dokumentem RFC). Nikomu se tedy nemůže stát, že by měl v ruce dokument STD, který je překonán jiným dokumentem STD řešícím stejnou problematiku - na druhé straně se ale může stát, že někdo bude mít v ruce již neaktuální verzi dokumentu STD ("desky se starým obsahem").

FYI (For Your Information)

Dalším typem dokumentů RFC (resp. jejich jinak uspořádanou podmnožinou) se staly dokumenty FYI (doslova: pro vaši informaci). Jde o základní informační dokumenty, určené zejména pro začínající uživatele Internetu. Opět je nejlépe si je představit jako pevně nadepsané "desky", do kterých jsou vloženy konkrétní dokumenty RFC.

BCP (Best Current Practices)

Nejnovější "reinkarnací" dokumentů RFC je série dokumentů BCP (Best Current Practices, ve volném překladu: nejvhodnější postupy a praktiky). Jde o specifickou řadu dokumentů, které vyjadřují stanoviska, názory a postoje a doporučené postupy velmi široké Internetové komunity (příkladem může být postoj ke spammingu).

II.6 Přehled vybraných RFC pro PKI

(Internet X.509 Public Key Infrastructure)
http://crypto-world.info/normy/index.htm
RFC 2510 : Certificate Management Protocols
RFC 2511 : Internet X.509 Certificate Request Message Format
RFC 2459 : Certificate and CRL Profile
RFC 2527 : Certificate Policy and Certification Practices Framework
RFC 2528 : Representation of Key Exchange Algorithm (KEA) Keys in Internet X.509 Public Key Infrastructure Certificates
RFC 2559 : Operational Protocols - LDAPv2
RFC 2560 : Online Certificate Status Protocol - OCSP
RFC 2585 : Operational Protocols: FTP and HTTP
RFC 2587 : LDAPv2 Schema
RFC 2797 : Certificate Management Messages over CMS

RFC 2802 : Digital Signatures for the v1.0 Internet Open Trading Protocol (IOTP)
RFC 2807 : XML Signature Requirements
RFC 3039 : Qualified Certificate Profile
RFC 3161 : Time-Stamp Protocol (TSP)
RFC 3279 : Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL)
RFC 3280 : Certificate and Certificate Revocation List (CRL) Profile
RFC 3281 : An Internet Attribute Certificate Profile for Authorization
RFC 3628 : Policy Requirements for Time-Stamping Authorities (TSAs)
RFC 3647 : Certificate Policy and Certification Practices Framework
RFC 3709 : Logotypes in X.509 Certificates
RFC 3739: Qualified Certificates

II.7 Střípky

Dokumenty RFC jsou datovány pouze měsícem a rokem zveřejnění. Výjimkou jsou některá aprílová RFC. V indexu můžete u některých z nich najít datum zveřejnění 1 April. V těchto případech se nejedná o vážně míněné dokumenty RFC, ale jde jedná se o dílka, která vtipným způsobem (obsahem i zpracováním) jsou parodií na skutečná RFC.

3091 Pi Digit Generation Protocol. H. Kennedy. Apr-01-2001. (Format: TXT=10375 bytes) (Status: INFORMATIONAL)

3092 Etymology of "Foo". D. Eastlake 3rd, C. Manros, E. Raymond. April-01-2001. (Format: TXT=29235 bytes) (Status: INFORMATIONAL)

3093 Firewall Enhancement Protocol (FEP). M. Gaynor, S. Bradner. April-01-2001. (Format: TXT=22405 bytes) (Status: INFORMATIONAL

3251 Electricity over IP. B. Rajagopalan. April-01-2002. (Format: TXT=18994 bytes) (Status: INFORMATIONAL)

3252 Binary Lexical Octet Ad-hoc Transport. H. Kennedy. April-01-2002. (Format: TXT=25962 bytes) (Status: INFORMATIONAL)

3514 The Security Flag in the IPv4 Header. S. Bellovin. 1 April 2003. (Format: TXT=11211 bytes) (Status: INFORMATIONAL)

3751 Omniscience Protocol Requirements. S. Bradner. 1 April 2004. (Format: TXT=20771 bytes) (Status: INFORMATIONAL)

III. Standardy PKCS (Public-Key Cryptographic Standards)

Tyto standardy jsou dnes všeobecně známé a použité v celé řadě dnešních kryptografických produktů. Jedná se o de facto normy americké firmy RSA tzv. standardy PKCS (Public-Key Cryptographic Standards)
PKCS

Standardy PKCS jsou vytvářeny v laboratořích firmy RSA Security (dříve RSA) ve spolupráci s řadou vývojářů z celého světa. Poprvé tyto standardy byly publikovány v roce 1991 jako výsledek jednání určité skupiny pracovníků, kteří implementovali technologii kryptografie s veřejným klíčem (June 3 1991 , publikováno na : NIST/OSI Implementors' Workshop, dokument SEC-SIG-91-16.)

V roce 1993 bylo zveřejněno prvních deset standardů ve formální podobě, která je dodnes zachovávána.

Od té doby byly několikráte upravovány a doplňovány. Původní standardy PKCS #2 a PKCS #4 byly včleněny do PKCS #1 a tato čísla nejsou obsazena.

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**

Pro základní seznámení s obsahem doporučuji např. seriál článků Ing.Jaroslava Pinkavy,CSc., které vycházely v e-zinu Crypto-World v roce 2000.
(Kryptografie a normy I.–V., Crypto-World 9/2000 - Crypto-World 1/2001, http://crypto-world.info/)

IV. České technické normy a svět

IV.1 Právní úprava národní technické normalizace

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

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

IV. 1.1 Charakteristika české technické normy

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

IV.1.2 Pojem „harmonizovaná česká technická norma“

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

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

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

IV.1.3 Zabezpečení tvorby norem

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

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

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

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

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

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

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

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

IV.2 Národní normalizační proces

V současné době se národní technická normalizace orientuje spíše na přejímání evropských a mezinárodních norem, než na jejich vlastní tvorbu. Tvorba norem čistě domácího původu představuje pouze 10% ze všech normalizačních prací [1].

IV.2.1 Tvorba norem

Návrh na zpracování normy může podat u Českého normalizačního institutu (ČSNI) kdokoliv.

Navrhovatel může současně navrhnout zpracovatele, kterým může být sám navrhovatel a popřípadě i způsob financování úkolu. ČSNI ve spolupráci s příslušnou technickou normalizační komisí, pokud je zřízena, návrh posoudí a výsledek, v případě potřeby, projedná s navrhovatelem. Pokud návrh předloží orgán státní správy v oblasti své působnosti, ČSNI s ním návrh projedná vždy, vniknou-li nejasnosti nebo odlišná stanoviska. Je-li výsledek posouzení kladný, ČSNI dohodne zpracovatele úkolu.

Zpracovatelé jsou při tvorbě norem povinni postupovat podle zákona 22/1997 Sb. a respektovat platné metodické pokyny pro normalizaci.

Zpracovatel vypracuje návrh normy, který zašle všem účastníkům připomínkového řízení, včetně ČSNI. Po vyřešení všech připomínek a souhlasu s návrhem účastníky připomínkového řízení je konečný návrh postoupen ke schválení ČSNI. ČSNI posoudí, zda návrh byl projednán stanoveným způsobem, zda odpovídá požadavkům zákona č. 22/1997 Sb. a podmínkám dohodnutým ve smlouvě se zpracovatelem. Poté návrh schválí, popřípadě upraví (po formální stránce) nebo vrátí k dopracování nebo zamítne [2].

IV.2.2 Obecné zásady pro stavbu, členění a úpravu českých technických norem (ČSN)

ČSN má
- být úplná v rozsahu stanoveném předmětem normy
- být jednoznačná, přesná a srozumitelná
- brát v úvahu dosažený stav techniky
- umožnit budoucí technický vývoj

Sloh má být co nejjednodušší, co nejvýstižnější a pokud možno co nejstručnější. Termíny se používají normalizované, pokud existují, a ve spisovném tvaru.

ČSN se vydávají v jazyce českém, jejich součástí však může být i identický cizojazyčný text přejímané evropské nebo mezinárodní, popř. zahraniční normy.

Normy ČSN se člení na části, oddíly, kapitoly, články, odstavce a přílohy.

IV.2.3 Přejímání evropských a mezinárodních norem

Všeobecně

Pod pojmem *evropská norma* se rozumí EN, HD, ENV, ETS, I-ETS, popř. další normy a normativní dokumenty vydané evropskými normalizačními organizacemi.

Pod pojmem *mezinárodní norma* se rozumí ISO a IEC, popř. další normy a normativní dokumenty vydané evropskými normalizačními organizacemi.

EN je norma CEN, CENELEC nebo ETSI, která je určena v členských státech k povinnému zavedení jako národní norma a vyžaduje současné zrušení národních norem, které jsou s ní v rozporu.

HD (harmonizační dokument) je norma CEN nebo CENELEC, která se zpracovává v případech, kdy není možné nebo účelné zpracovat EN a je určena v členských státech k povinnému zavedení na národní úrovni alespoň formou zveřejnění čísla HD a názvu při současném zrušení národních norem nebo jejich částí, které jsou s ní v rozporu.

ENV je předběžná norma CEN nebo CENELEC určená k ověření po dobu tří let (s možností jednorázového prodloužení o další dva roky). Národní normy, které jsou s ní v rozporu, mohou být ponechány v platnosti. Takto převzatá norma se označuje ČSN P ENV.

ETS je dřívější označení normy Evropského ústavu pro telekomunikační normy (ETSI), ke které se vážou stejné povinnosti, jako v případě EN. I-ETS je dřívější označení předběžné normy ETSI s obdobnou funkcí jako má ENV.

IV.2.4 Zásady přejímání norem

Převzetím evropské nebo mezinárodní normy do české normalizační soustavy se rozumí udělení statusu české normy přejímané normě tím, že je bez jakýchkoliv změn obsahu, stavby, členění a úpravy schválena jako ČSN. K počátku platnosti této ČSN musí být zrušeny dříve vydané ČSN nebo jejich části, pokud jsou s ní v rozporu.
Zapracování jakékoliv normy nebo normativního dokumentu do ČSN s odchylkami se nepovažuje za převzetí těchto norem (dokumentů). Označení ČSN se zapracovanou normou nebo normativním dokumentem s odchylkami neobsahuje značku ani číslo zapracované normy (dokumentu). Tyto údaje však mohou být spolu s dalšími potřebnými informacemi uvedeny v předmluvě ČSN.

Označení takto převzatých norem znamená, že:
ČSN EN je česká technická norma identická s EN v technickém obsahu a stavbě.
ČSN P ENV je česká předběžná norma identická s ENV v technickém obsahu a stavbě.
ČSN ETS je česká technická norma identická s ETS v technickém obsahu a stavbě.
ČSN P I-ETS je česká předběžná norma identická s I-ETS v technickém obsahu a stavbě.
ČSN ISO je česká technická norma identická s normou ISO v technickém obsahu a stavbě.
ČSN IEC je česká technická norma identická s normou IEC v technickém obsahu a stavbě.
ČSN EN ISO je česká technická norma identická s normou EN ISO v technickém obsahu a stavbě.

Ve zdůvodněných případech lze do české normalizační soustavy přejímat i jiné normy a normativní dokumenty. Pro jejich přejímání platí obdobné zásady jako pro přejímání evropských a mezinárodních norem.

Evropské a mezinárodní normy se do ČSN přejímají následujícími způsoby

1. překladem,
2. převzetím originálu
3. schválením k přímému používání
4. oznámením o schválení k přímému používání ve Věstníku

Způsob převzetí se volí podle účelu a rozsahu využití ČSN a dohodne se s ČSNI.

Z norem vyhlášených ve Věstníku ÚNMZ např. v roce 2001 bylo:

1246 norem evropských a mezinárodních vydáno překladem (včetně původních ČSN);

1191 norem evropských a mezinárodních vyhlášeno k přímému používání (vydána pouze titulní strana nebo jen oznámení ve Věstníku ÚNMZ). Jednou z těchto norem byla v souvislosti s elektronickým podpisem již zmiňovaná norma ČSN ISO 17799.

19 evropských a mezinárodních norem vydáno převzetím originálu (bez překladu, tzn. jen úvodní část ČSN s přiloženým originálem převzaté normy).

K 31. prosinci 2001 tvořilo soustavu ČSN celkem 25 817 platných norem [3].
V roce 2002 bylo schváleno dalších 2123 nových norem a
V roce 2003 bylo schváleno 2381 nových norem.
V současné době tvoří soustavu ČSN celkem více jak **30 000 platných norem**!!!

Následující tabulka pak zobrazuje počet schválených ČSN (bez jejich změn a oprav) podle zdroje od počátku roku 2003 do konce února 2004:

2003	**leden January**	**únor February**	**březen March**	**duben April**	**květen May**	**červen June**	**červenec July**
EN - CEN	62	159	288	419	573	713	872
EN - CLC	35	73	103	123	143	188	229
EN - ETS	42	51	67	85	89	121	162
ISO	5	6	13	24	45	57	71
IEC	6	9	10	10	13	16	17
ISO/IEC	7	11	13	20	21	28	31
ČSN	22	32	45	55	58	66	78
Celkem Total	179	341	539	736	942	1189	1460

2003 2004	**srpen August**	**září September**	**říjen Oktober**	**listopad November**	**prosinec December**	**2004 leden**	**2004 únor**
EN - CEN	966	1069	1170	1296	1372	78	150
EN - CLC	279	323	345	394	430	24	88
EN - ETS	187	189	226	226	234	8	18
ISO	76	82	96	104	126	7	11
IEC	21	23	23	23	23	0	3
ISO/IEC	32	46	53	57	57	5	6
ČSN	86	116	121	125	139	7	18
Celkem Total	1647	1848	2034	2225	**2381**	129	294

IV.2.5 Značka shody s **českou** technickou normou

Značka shody s českou technickou normou je dobrovolná certifikační značka, kterou výrobce prokazuje shodnost vlastností svého výrobku s požadavky české technické normy (ČSN). Výrobce nebo dovozce ji může použít na výrobku jedině tehdy, jestliže byl výrobek přezkoušen některým z Oprávněných zkušebních a certifikačních míst (OZCM) a byl na něj vystaven certifikát.

Existují čtyři verze značky ČSN TEST, které se používají podle toho, zda výrobek odpovídá původní české technické normě nebo české technické normě přejímající normu mezinárodní nebo evropskou:

ČSN TEST, ČSN ISO TEST, ČSN IEC TEST a ČSN EN TEST.

ČSN TEST shodnost s českou technickou normou nebo normami

ČSN ISO TEST shodnost s normou (normami) ČSN ISO

ČSN IEC TEST shodnost s normou (normami) ČSN IEC

ČSN EN TEST shodnost s normou (normami) ČSN EN

[1] ČSNI - NÁRODNÍ NORMALIZAČNÍ ORGANIZACE, Český normalizační institut.
http://www.csni.cz/wwwcsni/csni.htm
[2] TVORBA NOREM, Český normalizační institut.
http://www.csni.cz/wwwcsni/tvorba.htm
[3] Statistické údaje o tvorbě norem, Český normalizační institut.
http://domino.csni.cz/NP/NotesPortalCSNI.nsf/key/tvorba_norem_v_cr~statistika?Open

IV. 3 Mezinárodní vztahy

ČSNI udržuje rozsáhlé styky s mezinárodními a evropskými normalizačními organizacemi a s národními normalizačními organizacemi řady zemí. Jako nástupce dřívějších čs. normalizačních orgánů je řádným členem za Českou republiku v Mezinárodní normalizační organizaci (ISO) a Mezinárodní elektrotechnické komisi (IEC).

Na evropské úrovni je od roku 1997 plnoprávným řádným členem Evropského výboru pro normalizaci (CEN) a Evropského výboru pro elektrotechnickou normalizaci (CENELEC) a to se všemi právy a povinnostmi. Povinností je uskutečnění připomínkového řízení ke všem návrhům norem, obhájení připomínek na jednáních technických komisí a hlasování o konečném znění evropských norem. Další povinností je zavedení evropských norem do národní soustavy norem a to v půlročním termínu.

Přehled vybraných dokumentů CEN můžete nalézt v příloze crypto_p1.pdf k Crypto-Worldu 1/2003.

ČSNI má v Evropském telekomunikačním normalizačním institutu (ETSI) statut pozorovatele. Přehled dokumentů ETSI, které se zabývají elektronickým podpisem viz příloha crypto_p2.pdf k Crypto-Worldu 2/2003.

Mezinárodní normalizační spolupráce se realizuje účastí ČSNI na tvorbě evropských a mezinárodních norem v pracovních orgánech normalizačních organizací. ČSNI dále zabezpečuje některá zasedání technických komisí popř. subkomisí v ČR a má své zástupce v řídících orgánech (Technickém řídícím výboru, Správní radě apod.) CEN/CENELEC.

Elektronická výměna dat s mezinárodními organizacemi a zpracovateli se uskutečňuje klasickými metodami přenosu dat na disketách nebo CD-ROM nebo pomocí satelitního příjmu a stále častěji pomocí Internetu.

IV.3.1 Mezinárodní organizace pro normalizaci (ISO)

ISO je celosvětovou federací 130 národních normalizačních orgánů, je nevládní organizací a byla založena v roce 1947.

Posláním ISO je podporovat rozvoj standardizace ve světě a tím usnadnit mezinárodní obchod a rozvíjení kooperace ve sféře intelektuální vědecké, technologické a ekonomické aktivity. Výsledkem činnosti ISO jsou mezinárodní standardy, které obvykle připravují technické komise ISO.

Členové ISO jsou rozděleni do tří kategorií:

1. „Member body of ISO“

Plnoprávným členem ISO je vždy jen jedna organizace z konkrétního státu, která ho v oblasti standardizace nejvíce reprezentuje. Člen ISO musí informovat potenciální zájemce ve své zemi o mezinárodních normalizačních aktivitách, zastupovat státní zájmy v jednáních ISO vedoucích k ustanovení mezinárodních standardů a platit členské poplatky. Účastní se jednání v technických komisích ISO a má hlasovací právo.

2. „Correspondent member“

Sem spadají organizace zastupující státy, které ještě nemají plně rozvinutou standardizační infrastrukturu. Neúčastní se aktivně jednání, ale jsou o dění v ISO informovány.

3. „Subscriber membership“

Pod tento typ členství byly zařazeny státy s nerozvinutou ekonomikou. Platí nízké členské poplatky, které jim i přesto umožňují udržovat kontakt s mezinárodní standardizací.

ISO je decentralizovaná instituce, tvořená 2 850 technickými komisemi, podkomisemi a pracovními skupinami. Komise tvoří zástupci průmyslu, výzkumných ústavů, spotřebitelů a mezinárodních organizací z celého světa a jako rovnocenní partneři se setkávají na jednáních ISO. Každý člen ISO, který se zajímá o předmět, pro který byla vytvořena technická komise, má právo být v této komisi zastoupen. Práce se zúčastňují také vládní i nevládní neziskové organizace, s nimiž ISO navázala pracovní styk.

Centrální sekretariát ISO se nachází v Ženevě. Stará se o to, aby dohody schválené technickými komisemi byly editovány, vytištěny, předloženy k hlasování členům ISO a vydány. Vydání mezinárodní normy vyžaduje souhlas alespoň 75% z hlasujících členů. Také svolává jednání komisí, datum a místo s nimi předtím konzultuje. Většina tvůrčí práce však probíhá korespondenčně.

Publikace *ISO Memento* poskytuje informace o činnosti každé z technických komisí. Podrobná pravidla pro práci na mezinárodních standardech jsou popsána v *ISO/IEC Directives.* V publikaci *ISO Liaisons* je seznam okolo 500 mezinárodních organizací, které spolupracují s technickými komisemi ISO.

ISO úzce spolupracuje s Mezinárodní elektrotechnickou komisí (IEC) ve všech záležitostech normalizace v elektrotechnice [1] .

IV.3.2 Mezinárodní elektrotechnická komise (IEC)

IEC je celosvětovou mezinárodní organizací zahrnující všechny národní elektrotechnické komitéty (národní komitéty IEC) a byla založena v roce 1906. Cílem IEC je podporovat mezinárodní spolupráci ve všech otázkách, které se týkají normalizace v oblasti elektrotechniky a elektroniky. Za tím účelem, kromě jiných činností, IEC vydává mezinárodní normy. Jejich příprava je svěřena technickým komisím; každý národní komitét IEC, který se zajímá o projednávaný předmět, se může těchto přípravných prací účastnit. Mezinárodní vládní i nevládní organizace, s nimiž IEC navázala pracovní styk, se této přípravy rovněž zúčastňují.

IEC úzce spolupracuje s ISO v souladu s podmínkami dohodnutými mezi těmito dvěma organizacemi, s CENELEC (Evropský výbor pro elektrotechnickou normalizaci a s ETSI (Evropský telekomunikační normalizační institut) [2].

IEC má více než 50 členů. Prvním typem členství je tzv. „*full membership*“ neboli plné členství. Jedná se o národní organizace, které mají možnost se aktivně podílet na práci v IEC a mají volební právo. Druhým typem členství je tzv. *„associate membership“* neboli partnerské členství. V takovém případě mají národní organizace jen statut pozorovatele, to znamená, že se nepodílí aktivně na práci v IEC a nemají právo hlasovat.

Oficiální rozhodnutí nebo dohody IEC týkající se technických otázek připravené technickými komisemi, v nichž jsou zastoupeny všechny zainteresované národní komitéty, vyjadřují v nejvyšší možné míře mezinárodní shodu v názoru na předmět, kterého se týkají. Mají formu doporučení pro používání publikované formou norem, technických zpráv nebo pokynů a v tomto smyslu jsou přijímány národními komitéty. Na podporu mezinárodního sjednocení tyto komitéty mezinárodní normy IEC transparentně v maximálně možné míře do svých národních a regionálních norem. Každý rozdíl mezi normou IEC a odpovídající národní nebo regionální normou se v těchto normách jasně vyznačí. IEC nemá žádný postup týkající se vyznačování schválení a nenese žádnou odpovědnost za prohlášení o shodě předmětu s některou jeho normou. [2]

IV.3.3 Evropský výbor pro normalizaci (CEN)

Posláním CEN je podporovat dobrovolnou technickou harmonizaci v Evropě ve shodě s celosvětovými orgány a jejich partnery v Evropě.

Harmonizace ztenčuje obchodní bariéry, zvyšuje bezpečnost, umožňuje výměnu zboží, systémů a služeb a zvyšuje základní technické porozumění. V Evropě CEN spolupracuje s CENELEC (Evropský výbor pro elektrotechnickou normalizaci) a ETSI (Evropský telekomunikační normalizační institut).

CEN pracuje podle zásad, které mají zajistit následující:

- **otevřenost a průhlednost**

(Všechny zainteresované společnosti se podílejí na práci. Zastoupení je chráněno především národními normalizačními orgány, které mají povinnost posílat vyvážené zprávy politickým orgánům a technickým výborům. Zástupci průmyslu a ostatních oblastí mají své zastoupení v politických výborech. Celý pracovní program je vydán v „*CEN´s Work programme*“.)

- **konsensus**

(Evropské normy jsou vytvořeny na základě svobodného souhlasu mezi všemi zainteresovanými členy.)

- **národní výbor**
(Formální přijetí evropských norem se rozhoduje prostou většinou hlasů ze všech národních členů a pro všechny je zavazující.)

- **technická soudržnost na národní a evropské úrovni**
(Normy tvoří soubor, který zajišťuje vlastní kontinuitu pro dobro uživatelů, a to jak na evropské úrovni, tak na národních úrovních a to díky závaznosti zavádění evropských standardů a stahování problematických národních norem.)

- **správná integrace mezinárodní práce**
(Normalizace je drahá a časově náročná.)

Tvorbu norem provádí technické komise a subkomise. Koordinaci technických činností zajišťuje Technical Board CEN. Ročně se vypracuje v CEN zhruba 1000 evropských norem. Důležitá rozhodnutí jsou předkládána Generálnímu shromáždění, které se schází 1x ročně. Generální shromáždění má veřejnou část, na kterou jsou pozváni zástupci jiných mezinárodních a regionálních organizací a kde jsou projednávány obecné otázky evropské normalizace a uzavřenou část, kde jsou přítomni pouze zástupci národních normalizačních organizací řádných členů a přidružených členů CEN.

V září roku 1999 se poprvé konalo generální zasedání CEN i v Praze.

Členy CEN jsou národní normalizační organizace zemí Evropské unie a Evropského sdružení volného obchodu.

CEN lze dělit na následující členy:

- řádné národní

Své zastoupení v CEN mají státy: Rakousko (ON), Belgie (IBN/BIN), Česká republika (ČSNI), Dánsko (DS), Finsko (SFS), Francie (AFNOR), Německo (DIN), Řecko (ELOT), Island (STRÍ), Irsko (NSAI), Itálie (UNI), Lucembursko (SEE), Nizozemí (NEN), Norsko (NSF), Portugalsko (IPQ), Španělsko (AENOR), Švédsko (SIS), Švýcarsko (SNV), Velká Británie (BSI)

- **spolupracující členy (asociace)**

ANEC (European Association for the co-operation of consumer representation in standardization)
CEFIC (European Chemical Industry Council)
EUCOMED (European Confederation of Medical Devices Associations)
FIEC (European Construction Industry Federation)
NORMAPME (European Office of Crafts, Trades and Small and Medium-sized Enterprises for standardization)
TUTB (European Trade Union Technical Bureau for Health and Safety)

- poradní členy (evropské instituce)
EC (The European Commission - Evropská komise)
EFTA Secretariat (European Free Trade Association - Evropská asociace volného obchodu)

- přidružené (afiliované) členy

Tito členové se mohou stát řádnými členy po splnění všech podmínek stanovených CEN, mimo jiné musí zavést 80% evropských norem do svých národních technických norem.

Na přijetí do CEN čekají státy se zastoupením: Albánie (DPS); Bulharsko (SASM); Chorvatsko (DZNM); Kypr (CYS); Estonsko (ESK); Maďarsko (MSZT); Lotyšsko (LVS); Litva (LST); Malta (MSA); Polsko (PKN); Rumunsko (ASRO); Slovensko (SUTN); Slovinsko (SMIS) a Turecko (TSE).

IV.3.4 Evropský výbor pro elektrotechnickou normalizaci (CENELEC)

CENELEC byl ustanoven roku 1973 jako nevýdělečně činná organizace v rámci belgického práva. Oficiálně byl uznán jako evropská normalizační organizace Evropskou komisí nařízením 83/189 EEC.

Jeho členové spolupracují v zájmu evropské harmonizace od konce padesátých let, vyvíjející se po boku Evropského hospodářského společenství. CENELEC má 40 000 technických odborníků v 19 zemích Evropského společenství a EFTA (Evropské sdružení volného obchodu) pro vydávání norem pro evropský trh [3] .

Literatura:

[1] http://www.iso.ch/infoe/intro.htm
[2] Metodické pokyny pro normalizaci MPN 1: 1999 : stavba, členění a úprava českých technických norem. 1. vyd. Praha : Český normalizační institut, 1999.
[3] http://www.cenelec.org/Info/about.htm

V. Přehled norem v oblasti bezpečnosti informačních technologií (normy vyvíjené ISO/IEC JTC1 SC27 a ISO TC 68) zavedených do soustavy českých norem

V.1 Normy z oblasti bezpečnosti informačních technologií

Do 70tých let bylo používání bezpečnostních, zejména kryptografických technik určených na ochranu informací omezeno na specifické oblasti aplikace. S rozšířením osobních počítačů a počítačových sítí, s nástupem Internetu a prováděním obchodních i dalších činností on-line se tento stav dramaticky změnil. Prudce vzrostla rovněž možná rizika spojená s využíváním těchto progresivních technologií. Proto se začal zejména v posledních letech klást důraz na jejich bezpečnost, tj. na zajištění zejména integrity, důvěrnosti a dostupnosti dat zpracovávaných prostřednictvím těchto technologií. Je zřejmé, že normalizované bezpečnostní techniky (autentizace entit, integrita dat, nepopiratelnost, důvěrnost dat) se stávají povinnými požadavky pro elektronický obchod, zdravotní péči a řadu dalších aplikačních oblastí. Bezpečnost IT se tak stala s ohledem na svůj průřezový charakter významnou částí normalizačních aktivit v celém světě.

Mezinárodní organizace pro normalizaci ISO (International Organisation for Standardisation) vyvíjí normy týkající se bezpečnosti informačních technologií v několika svých komisích a subkomisích. Nejdůležitější jsou vyvíjené pod ISO/IEC JTC1 SC 27 (Informační technologie – Bezpečnostní techniky) a TC 68 (Bankovnictví a související finanční služby).

V oblasti spolupráce s ostatními normalizačními komisemi ISO je cílem zajistit vývoj společných norem, vyhnout se možnému. překrývání a duplicitám ve vyvíjených normách a sdílet expertizy. SC 27 úzce spolupracuje v oblasti bezpečnostních norem s TC 68; za tímto účelem byla zřízena společná koordinační komise. Další spolupráce s ITU-T SG 7/Q20 je zaměřena zejména na vydávání společných norem. Spolupráce s CCIMB (Common Criteria Interpretation Managerial Board) umožňuje národním úřadům, které nejsou členy CCEB (Common Criteria Editorial Board) a CCIMB revidovat, připomínkovat a přispívat k vyvíjeným projektům (např. Common Criteria).

Vzhledem k tomu, že vývoj bezpečnostních norem je velmi náročnou záležitostí nezpracovávají se původní české normy. Vzhledem k úkolům na úseku harmonizace norem a právních dokumentů jsou běžně mezinárodní bezpečnostní normy ISO národními normalizačními orgány přejímány a vydávány jako národní normy. ČSNI plní v této oblasti významnou roli– mezinárodní bezpečnostní normy mající charakter průřezových norem (vyvíjené ISO/IEC JTC1 SC 27) jsou průběžně sledovány, přejímány a vydávány a aktualizovány jako české technické normy již řadu let. ČSNI rovněž zajišťuje mezinárodní spolupráci v této oblasti.

České technické normy přejímané z ISO/IEC JTC1 SC 27 pokrývají problematiku bezpečnosti informačních technologií na průřezové úrovni, jsou tedy všeobecně využitelné. Zajišťují normalizaci generických metod a technik pro bezpečnost informačních technologií. To zahrnuje:

- identifikaci generických požadavků (včetně požadavků na metodologii) pro bezpečnostní služby systémů IT

- vývoj bezpečnostních technik a mechanismů (včetně registračních postupů a vztahů mezi bezpečnostními komponentami)
- vývoj bezpečnostních směrnic (např. interpretační dokumenty)
- vývoj dokumentace a norem určených k podpoře managementu (např. terminologie a kritéria pro hodnocení bezpečnosti, problematika analýzy rizik).

České technické normy přejímané z ISO/IEC JTC1 SC 27 pokrývají normalizaci kryptografických algoritmů pro zajištění služeb integrity, autentizace a nepopiratelnosti. Zahrnují rovněž normalizaci kryptografických algoritmů pro zajištění služeb důvěrnosti a to v souladu s mezinárodně akceptovanými zásadami.

V.2 Přehled ČSN z oblasti bezpečnosti informačních technologií

ČSN ISO/IEC	2382-1	Informační technologie - Slovník - Část 1: Základní termíny
ČSN ISO/IEC	2382-8	Informační technologie - Slovník - Část 8: Bezpečnost
ČSN ISO/IEC	2382-14	Informační technologie - Slovník - Část 14: Spolehlivost
ČSN ISO/IEC	10116	Informační technologie - Bezpečnostní techniky - Módy činnosti pro n-bitovou blokovou šifru
ČSN ISO/IEC	10118-1	Informační technologie - Bezpečnostní techniky - Hašovací funkce - Část 1: Všeobecně
ČSN ISO/IEC	10118-2	Informační technologie - Bezpečnostní techniky - Hašovací funkce - Část 2: Hašovací funkce používající n-bitovou blokovou šifru
ČSN ISO/IEC	10118-3	Informační technologie - Bezpečnostní techniky - Hash funkce - Část 3: Dedikované hash funkce
ČSN ISO/IEC	10118-4	Informační technologie - Bezpečnostní techniky - Hašovací funkce - Část 4: Hašovací funkce používající modulární aritmetiku
ČSN ISO	10126-1	Bankovnictví - Postupy pro šifrování zpráv (bankovní služby pro velkou klientelu) - Část 1: Obecné zásady
ČSN ISO	10126-2	Bankovnictví - Postupy pro šifrování zpráv (bankovní služby pro velkou klientelu). Část 2: Algoritmus DEA
ČSN ISO	10202-1	Identifikační karty. Karty pro finanční transakce. Bezpečnostní architektura systémů finančních transakcí využívajících karty s integrovanými obvody. Část 1: Životní cyklus karty
ČSN ISO	11131	Bankovnictví - Autentizace přihlášením
ČSN ISO	11166-1	Bankovnictví - Správa klíčů prostřednictvím asymetrických algoritmů - Část 1: Zásady, postupy a formáty
ČSN ISO	11166-2	Bankovnictví - Správa klíčů pomocí asymetrických algoritmů - Část 2: Schválené algoritmy používající kryptosystém RSA
ČSN EN ISO	11568-1	Bankovnictví - Správa klíčů (bankovní služby pro drobnou klientelu) - Část 1: Úvod do správy klíčů
ČSN EN ISO	11568-2	Bankovnictví - Správa klíčů (bankovní služby pro drobnou klientelu) - Část 2: Techniky správy klíčů pro symetrickou šifru
ČSN EN ISO	11568-3	Bankovnictví - Správa klíčů (bankovní služby pro drobnou klientelu) - Část 3: Životní cyklus klíče pro symetrickou šifru
ČSN ISO/IEC	11770-1	Informační technologie - Bezpečnostní techniky - Správa klíčů - Část 1: Struktura
ČSN ISO/IEC	11770-2	Informační technologie - Bezpečnostní techniky - Správa klíčů -

		Část 2: Mechanismy používající symetrické techniky
ČSN ISO/IEC	11770-3	Informační technologie - Bezpečnostní techniky - Správa klíčů - Část 3: Mechanismy používající asymetrické techniky
ČSN ISO/IEC TR	13335-1	Informační technologie - Směrnice pro řízení bezpečnosti IT - Část 1: Pojetí a modely bezpečnosti IT
ČSN ISO/IEC TR	13335-2	Informační technologie - Směrnice pro řízení bezpečnosti IT - Část 2: Řízení a plánování bezpečnosti IT
ČSN ISO/IEC TR	13335-3	Informační technologie - Směrnice pro řízení bezpečnosti IT - Část 3: Techniky pro řízení bezpečnosti IT
ČSN ISO/IEC TR	13335-4	Informační technologie - Směrnice pro řízení bezpečnosti IT - Část 4: Výběr ochranných opatření
ČSN ISO/IEC	13888-1	Informační technologie - Bezpečnostní techniky - Nepopiratelnost - Část 1: Všeobecně
ČSN ISO/IEC	13888-2	Informační technologie - Bezpečnostní techniky - Nepopiratelnost - Část 2: Mechanismy používající symetrické techniky
ČSN ISO/IEC	13888-3	Informační technologie - Bezpečnostní techniky - Nepopiratelnost - Část 3: Mechanismy používající asymetrické techniky
ČSN ISO/IEC	14888-1	Informační technologie - Bezpečnostní techniky - Digitální podpisy s dodatkem - Část 1: Všeobecně
ČSN ISO/IEC	14888-2	Informační technologie - Bezpečnostní techniky - Digitální podpisy s dodatkem - Část 2: Mechanismy založené na identitě
ČSN ISO/IEC	14888-3	Informační technologie - Bezpečnostní techniky - Digitální podpisy s dodatkem - Část 3: Mechanismy založené na certifikátu
ČSN ISO/IEC	15408-1	Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT - Část 1: Úvod a všeobecný model
ČSN ISO/IEC	15408-2	Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT - Část 2: Bezpečnostní funkční požadavky
ČSN ISO/IEC	15408-3	Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT - Část 3: Požadavky na záruky bezpečnosti
ČSN ISO/IEC	17799	Informační technologie - Soubor postupů pro řízení informační bezpečnosti
ČSN ISO	6166	Cenné papíry a příbuzné finanční nástroje - Mezinárodní systém identifikačního číslování cenných papírů (ISIN)
ČSN ISO	7775	Bankovnictví - Cenné papíry - Schéma pro typy zpráv
ČSN ISO	8372	Zpracování informací - Módy činnosti pro algoritmus 64-bitové blokové šifry
ČSN ISO	8730	Bankovnictví - Požadavky na autentizaci zprávy (bankovní služby pro velkou klientelu)
ČSN ISO	8731-1	Bankovnictví - Schválené algoritmy pro autentizaci zprávy - Část 1: DEA
ČSN ISO	8731-2	Bankovnictví - Schválené algoritmy pro autentizaci zprávy - Část 2: Algoritmus autentikátora zprávy
ČSN ISO	8732	Bankovnictví - Správa klíčů (bankovní služby pro velkou klientelu)
ČSN ISO	8908	Bankovnictví a souvisící finanční služby - Slovník a datové

		prvky
ČSN ISO	9564-1	Bankovnictví - Řízení a bezpečnost osobních identifikačních čísel. Část 1: Principy a techniky ochrany PIN
ČSN ISO	9564-2	Bankovnictví - Řízení a bezpečnost osobních identifikačních čísel. Část 2: Schválené algoritmy pro šifrování PIN
ČSN ISO	9735-5	Elektronická výměna dat pro správu, obchod a dopravu (EDIFACT) - Pravidla syntaxe aplikační úrovně (Číslo verze syntaxe: 4) - Část 5: Pravidla bezpečnosti pro dávkovou EDI (autentičnost, integrita a nepopření původu)
ČSN ISO	9735-6	Elektronická výměna dat pro správu, obchod a dopravu (EDIFACT) - Pravidla syntaxe aplikační úrovně (Číslo verze syntaxe: 4) - Část 6: Bezpečnostní autentizace a potvrzení (Zpráva AUTACK)
ČSN ISO/IEC	9796-2	Informační technologie - Bezpečnostní techniky - Schémata digitálního podpisu umožňující obnovu zprávy - Část 2: Mechanismy využívající hash funkci
ČSN ISO/IEC	9796-3	Informační technologie - Bezpečnostní techniky - Schémata digitálních podpisů umožňující obnovu zprávy - Část 3: Mechanismy založené na diskrétních logaritmech
ČSN ISO/IEC	9797	Informační technologie - Bezpečnostní techniky - Mechanismus integrity dat používající kryptografickou kontrolní funkci s využitím algoritmu blokové šifry
ČSN ISO/IEC	9797-1	Informační technologie - Bezpečnostní techniky - Kódy pro autentizaci zprávy (MAC) - Část 1: Mechanismy používající blokovou šifru
ČSN ISO/IEC	9798-1	Informační technologie - Bezpečnostní techniky - Mechanismy autentizace entit - 1. část: Obecný model
ČSN ISO/IEC	9798-2	Informační technologie - Bezpečnostní techniky - Autentizace entit - Část 2: Mechanismy používající symetrické šifrovací algoritmy
ČSN ISO/IEC	9798-3	Informační technologie - Bezpečnostní techniky - Mechanismy autentizace entit - Část 3: Autentizace entit používající algoritmus s veřejným klíčem
ČSN ISO/IEC	9798-4	Informační technologie - Bezpečnostní techniky - Autentizace entit - Část 4: Mechanismy používající kryptografickou kontrolní funkci
ČSN ISO/IEC	9798-5	Informační technologie - Bezpečnostní techniky - Autentizace entit - Část 5: Mechanismy používající techniku nulových znalostí
ČSN ISO	9807	Bankovnictví - Požadavky na autentizaci zpráv (bankovní služby pro drobnou klientelu)
ČSN ISO/IEC	9979	Informační technologie - Bezpečnostní techniky - Postupy pro registraci kryptografických algoritmů

Použitá literatura

Ing. Petr Wallenfels : Přehled norem v oblasti bezpečnosti informačních technologií (normy vyvíjené ISO/IEC JTC1 SC27 a ISO TC 68) zavedených do soustavy českých norem, zveřejněno v e-zinu Crypto-World 3/2003, http://crypto-world.info

VI. Přehled mezinárodních a národních normalizačních institucí

VI.1 Mezinárodní standardizační instituty

ISO - International Organization for Standardization http://www.iso.ch/
IEC - International Electrotechnical Commission http://www.iec.ch/
ITU - International Telecommunication Union http://www.itu.ch/
WSSN - World Standards Services Network http://www.wssn.net/

VI.2 Regionální standardizační instituty

CEN - European Committee for Standardization http://www.cenorm.be/
CENELEC - European Committee for Electrotechnical Standardization
http://www.cenelec.org/
COPANT - Pan American Standards Commission http://www.copant.org/
ETSI - European Telecommunications Standards Organisation
http://www.etsi.org/

VI.3 Národní standardizační instituty

Argentina - Instituto Argentino de Normalización (IRAM) http://www.iram.com.ar/
Austrálie - Standards Australia (SAA) http://www.standards.com.au/
Dánsko - DS - Denmark http://www.ds.dk/
Finsko - SFS - Finnish Standards Association http://www.sfs.fi/
Francie - AFNOR -Association française de normalisation http://www.afnor.fr/
Holandsko - NNI - Nederlands Normalisatie-Instituut http://www.nni.nl/
Itálie - UNI - Ente Nazionale Italiano di Unificazione http://www.unicei.it/
Island - STRI - Iceland http://tobbi.iti.is/STRI/
Japonsko - JISC - Japanese Industrial Standards Committee
http://www.hike.te.chiba-u.ac.jp/ikeda/JIS/index.html
Kanada - Standards Council of Canada (SCC) http://www.scc.ca/
Maďarsko - MSZT - Magyar Szabványügyi Testület http://www.mszt.hu/
Malajsie - DSM - Department of Standards Malaysia http://www.dsm.gov.my/
Norsko - NSF - Norges Standardiseringsforbund http://www.standard.no/
Nový Zéland - SNZ - Standards New Zealand http://www.standards.co.nz/
Rakousko - ON - Österreichisches Normungsinstitut http://www.on-norm.at/
Rusko - GOST - Státní normy http://www.gost.ru/sls/gost.nsf/
Řecko - ELOT -Hellenic Organization for Standardization http://www.elot.gr/
Slovensko - Úrad pre normalizáciu metrológiu a skúšobníctvo
http://www.normoff.gov.sk/unms_sr/index.html
- Slovenský Ústav Technickej Normalizácie http://www.sutn.gov.sk/
Slovinsko - SMIS - Standards and Metrology Institute http://www.usm.mzt.si/
Spolková republika Německo - DIN - Deutsches Institut für Normung
http://www.din.de/
Španělsko - AENOR - Asociación Espanola de Normalización y Certificación
http://www.aenor.es/
Švédsko - SIS - Standardiseringen i Sverige http://www.sis.se/

Švýcarsko - SNV - Schweizerische Normen-Vereinigung http://www.snv.ch/
Thajsko - TISI - Thai Industrial Standards Institute http://www.tisi.go.th/
USA - ANSI - American National Standards Institute http://www.ansi.org/
IEEE - Institute of Electrotechnics and Electronics Engineers
http://www.ieee.org/portal/index.jsp
UL - Underwriters Laboratories, Inc http://www.ul.com/
Velká Británie - BSI - British Standards Institution http://www.bsi.org.uk/

VII. Přehled některých základních kritérií hodnocení bezpečnosti IT

VII.1 Úvod

Kritéria pro hodnocení bezpečnosti IT (dále jen "kritéria") slouží především jako **měřítko používané k hodnocení informačních technologií s ohledem na jejich bezpečnost, na konkrétní aplikace služeb a na opatření k zajištění bezpečnosti**. Vládní kritéria většinou určují hlavní směr vývoje i pro kritéria bankovní, komerční atd. -- obvykle však jsou vládní kritéria používána i nevládními organizacemi. Vlastní vládní kritéria používaná pro hodnocení kryptografických zařízení řada zemí nezveřejňuje.

Hodnocené objekty se často dělí na *produkty* (nemají specifikováno provozní prostředí a tedy ani hrozby) a na *systémy* (větší spojité celky s rysem -- kde je při hodnocení známa i konfigurace a provozní prostředí).

Při hodnocení *je* od výrobce (žadatele o hodnocení) *vyžadována podrobná specifikace, dokumentace a popis postupu při vývoji*, které by u jiné než komerčně nezávislé agentury byly vystaveny většímu riziku ohrožení úniku informací, jež jsou pro výrobce často životně důležité. Hodnocení je prováděno hodnotitelem na základě žádosti (a za prostředky) výrobce, který také specifikuje, na jaké úrovni má být produkt či systém hodnocen. Podle specifikace požadavků v kritériích musí výrobce hodnotiteli poskytnout potřebnou dokumentaci, podporu odborníků atd.

Hodnocení probíhá v určitém prostředí a konfiguraci, proto je také nutno tyto údaje uvádět při prezentování výsledků hodnocení a akreditace (např. u databázových systémů uvést platformu a operační systém, se kterými bylo hodnocení prováděno, verze všech produktů atd.).

VII.2 Trusted Computer System Evaluation Criteria (TCSEC)
"Oranžová kniha"

Koncem 60. let si odpovědní činitelé amerických vládních agentur začali uvědomovat potřebu jednotného měřítka pro hodnocení produktů s ohledem na jejich služby při ochraně informací. Hodnocení produktů pro jednotlivé úřady bylo jak časově, tak i finančně náročné a perspektiva jednoho zhodnocení a akreditace, která by byla platná pro daný produkt na celém území USA, byla snad nejjednodušším řešením. Daná akreditace šetří čas a vládní prostředky, protože bez ní by bylo nutno provádět hodnocení vždy znovu při každém nákupu. Druhým pozitivním aspektem je pak možnost srovnání a snazší specifikace potřeb jednotlivých úřadů.
Výsledek dlouholeté práce ministerstva obrany, standardizačních orgánů a také vládě blízkých firem se dostavil v podobě kritérií pro hodnocení důvěryhodných výpočetních systémů. Tato kritéria byla vydána v roce 1985 jako standard ministerstva obrany. Oranžový přebal charakterizoval tuto publikaci, která je pod názvem "Orange Book" známa po celém světě.

Trusted Computer System Evaluation Criteria (TCSEC) jsou ovlivněna dobou vzniku a slouží především pro potřeby víceuživatelských monolitických počítačů. Databázové systémy, sítě, menší části systémů atd. byly pak s postupem času zohledněny "interpretacemi" TCSEC -- jako např. Trusted Database Interpretation, Trusted Network Interpretation atd. I jejich barvy přebalů pak daly podnět k názvům jako "Red Book" atd.

Čtyři skupiny TCSEC (A, B, C, D) odpovídají vždy jednomu kvalitativně odlišnému stupni bezpečnosti a jsou dále děleny do tříd (D, C1, C2, B1, B2, B3, A1). Každá ze tříd

pokrývá a popisuje čtyři aspekty hodnocení - bezpečnostní směrnice, zodpovědnost, zabezpečení a dokumentaci.
Jednotlivé požadavky pro dané třídy se postupně zpodrobňují a tvoří hierarchii s třídou D jako prvkem nejnižším a s třídou A1 jako prvkem nejvyšším. Praktického užití se dostává především skupinám B a hlavně C, neboť třída D zahrnuje prostě produkty, které byly podrobeny hodnocení s užitím TCSEC, ale které nedosáhly žádné z vyšších tříd, a třída A1 stanovuje požadavky, které jsou pro většinu produktů z finančních důvodů nerealizovatelné.

TCSEC a „duhová série“:
http://csrc.ncsl.nist.gov/secpubs/rainbow/
Seznam produktů skutečně vyhodnocených dle TCSEC:
http://www.radium.ncsc.mil/tpep/epl/

VII.3 Information Technology Security Evaluation Criteria (ITSEC)

Hodnocení bezpečnosti podle IT ITSEC (Information Technology Security Evaluation Criteria) bylo vytvořeno v roce 1990. Harmonizovaná verze národních kritérií přijatých ve Francii, Německu, Anglii a Nizozemí, byla předložena v září 1990 v Bruselu k připomínkám a diskusi, které se zúčastnily i USA. Po úpravách byla vydána Úřadem pro oficiální publikace Evropského společenství v červnu 1991 (materiál byl označen jako prozatímní materiál k dvouletému ověření). Schválena jako doporučení byla v dubnu 1995.

Třídy funkčnosti ITSEC

Kritéria ITSEC specifikují sedm tříd míry zaručitelnosti bezpečnosti E0 až E6 reprezentujících vzrůstající úrovně důvěry a dále v příloze definuje dalších deset tříd bezpečnostní funkčnosti F-xx. Třídy míry zaručitelnosti kladou požadavky na:
- proces vývoje IS
- prostředí vývoje IS
- provozní dokumentace IS
- provozní prostředí IS.

Pět tříd funkčnosti F-C1, F-C2, F-B1, F-B2 a F-B3 odpovídá stejnojmenným třídám kritérií TCSEC. Zbylých pět tříd funkčnosti je orientováno aplikačně. Na rozdíl od TCSEC, která vznikala pro vojenské prostředí a orientovala se zejména na důvěrnost informace je TCSEC koncipován mnohem obecněji a pokrývá částečně i požadavky integrity a dostupnosti informace. Oproti TCSEC definuje ITSEC navíc způsob dokumentace hodnoceného předmětu, způsob definování bezpečnostního cíle a způsob provádění hodnocení.

Míru zaručitelnosti bezpečnosti je v kritériích ITSEC definováno sedm tříd zaručitelnosti bezpečnosti E0 až E6 a nepředpokládá se, že by uživatelé kritérií definice těchto tříd měnili nebo si definovali své vlastní třídy.

Pět tříd funkčnosti F-C1, F-C2, F-B1, F-B2 a F-B3 odpovídá stejnojmenným třídám kritérií TCSEC. Zbylých pět tříd funkčnosti (F-IN, F-AV, F-DI, F-DC a F-DX) nemá hierarchickou strukturu. Tyto třídy funkčnosti jsou třídy se zvýšenými bezpečnostními požadavky v některé oblasti bezpečnosti - například F-IN je třída se zvýšenými požadavky v oblasti integrity, F-AV je třída se zvýšenými požadavky v oblasti dostupnosti atd.

Výše uvedené třídy funkčnosti jsou, na rozdíl od tříd míry zaručitelnosti bezpečnosti, pouze příklady. Nejsou závazné a mají sloužit pro usnadnění práce uživatelům kritérií ITSEC.
První možností je, že uživatel přímo použije některou ze tříd funkčnosti, uvedenou v kritériích ITSEC. V tomto případě si zpravidla vybere některou ze tříd, které jsou hierarchické a odpovídají třídám kritérií TCSEC.

Druhou možností je, že uživatel kritérií použije vhodné kombinace některých ze tříd funkčnosti, uvedených v kritériích ITSEC. Tato možnost dává uživateli kritérií větší možnosti a dovoluje mu vytvořit třídu funkčnosti, která lépe odpovídá jeho požadavkům.

Třetí možností je, že uživatel kritérií použije některou, již vytvořenou třídu funkčnosti, která není součástí kritérií ITSEC, ale je vytvořena v souladu s těmito kritérii a nejlépe vyhovuje požadavkům uživatele.

Konečně poslední, čtvrtou, možností je případ, kdy si uživatel kritérií vytvoří sám vlastní třídu funkčnosti, která je v souladu s požadavky kritérií ITSEC. Tento případ nastane zejména v okamžiku, kdy je hodnocený předmět natolik specifický, že jsou všechny výše uvedené cesty neschůdné. Vzhledem k pracnosti tohoto způsobu stojí však vždy za úvahu, zda skutečně nelze využít některý ze tří výše uvedených případů.

Specifikace funkcí prosazujících bezpečnost podle ITSEC
Jedná se o tato ***generická záhlaví:***
Identifikace a autentizace
Řízení přístupu
Účtovatelnost
Audit
Opakované užití
Přesnost
Spolehlivost a dostupnost služeb
Výměna dat

ITSEC:
http://www.itsec.gov.uk/docs/formal.htm#ITSEC
Další dokumenty k ITSEC, seznam vyhodnocených produktů apod.:
http://www.itsec.gov.uk/
http://www.itsec.gov.uk/products/locate.htm

VII.4 Canadian Trusted Computer Product Evaluation Criteria (CTPEC)

Kanadská kritéria pro hodnocení bezpečnosti informačních systémů CTCPEC (Canadian Trusted Computer Product Evaluation Criteria) se pokusila vytvořit prakticky použitelnější kategorizaci bezpečnostních funkcí. Bezpečnostní funkce jsou v CTCPEC nazývány bezpečnostními službami. Tyto bezpečnostní funkce jsou rozděleny do čtyř kategorií, na bezpečnostní funkce zajišťující důvěrnost, integritu, dostupnost a účtovatelnost. V rámci každé bezpečnostní funkce je definováno několik úrovní. Úroveň bezpečnostní funkce je definovaný a měřitelný požadavek na granularitu nebo sílu bezpečnostní funkce vzhledem k určité množině hrozeb. Bezpečnostní funkce s vyšší úrovní poskytují účinnější ochranu proti hrozbám. To však neznamená, že následující úroveň musí nutně zahrnovat vše, co bylo požadováno v předcházejících úrovních. Úrovně jsou vzestupně číslovány číselně počínaje od nuly, která představuje nejnižší úroveň ochrany. Například bezpečnostní funkce identifikace a autentizace, která má zkratku WA, obsahuje úrovně WA-0, WA-1, WA-2 a WA-3.

Bezpečnostní funkce zajišťující důvěrnost
Bezpečnostní funkce v této kategorii jsou určeny proti hrozbám, které mohou zapříčinit odhalení informace neoprávněným subjektům (neoprávněné prozrazení informace). Jedná se o následující bezpečnostní funkce:

- *Skryté kanály* (obsahuje čtyři úrovně CC-0 až CC-3)
- *Nepovinné řízení důvěrnosti* (CD-0 až CD-4)
- *Povinné řízení důvěrnosti* (CM-0 až CM-4)
- *Opětné použití objektů* (CR-0 až CR-1)

Bezpečnostní funkce zajišťující integritu
Bezpečnostní funkce zajišťující dostupnost
Bezpečnostní funkce zajišťující účtovatelnost

CTCPEC:
ftp://ftp.cse.dnd.ca/pub/criteria/CTCPEC/

VII.5 Common Criteria

V roce 1998 byla po dvou letech intenzivní práce podepsaná následujícími pěti státy : **CSE** (Canada), **SCSSI** (France), **BSI** (Germany), **NLNCSA** (Netherlands), **CESG** (UK), **NIST** (USA) a **NSA** (USA) smlouva „**Common Criteria Recognition Arrangement"**

Hlavní body této smlouvy jsou:
- to ensure that evaluations of IT products and protection profiles are performed to high and consistent standards and are seen to contribute significantly to confidence in the security of those products and profiles;
- to increase the availability of evaluated, security-enhanced IT products and
- protection profiles for national use;
- to eliminate duplicate evaluations of IT products and protection profiles; and
- to continuously improve the efficiency and cost-effectiveness of security evaluations and the certification/validation process for IT products and protection profiles.

V květnu 2000 byla skupina uznávající CC výrazným způsobem rozšířena. Čtyřicetistránkovou smlouvu o uznávání certifikátů, které stvrzují hodnocení produktů v oblasti bezpečnostních technologií (***Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security***) podepsali zástupci z 13 států. Později přistoupili k této smlouvě ještě zástupci dvou dalších států – Izrael a Rakousko. Aktuální přehled všech signatářů smlouvy Australia and New Zealand, Austria, Canada, Finland, France, Germany, Greece, Israel, Italy, Netherlands, Norway, Spain, Sweden, United Kingdom, United States)

Common Criteria Documentation
Oficiální dokumentace. Z této verze vychází norma ISO 15408 a obsahově je s ní totožná.
Common Criteria for Information Technology, Security Evaluation , Part 1, Introduction and general model, August 1999, Version 2.1, CCIMB-99-031, 61 stran
(Part 1, Introduction and general model, is the introduction to the CC. It defines general concepts and principles of IT security evaluation and presents a general model of evaluation. Part 1 also presents constructs for expressing IT security objectives, for selecting and defining

IT security requirements, and for writing high-level specifications for products and systems. In addition, the usefulness of each part of the CC is described in terms of each of the target audiences).

Common Criteria for Information Technology, Security Evaluation , Part 2, Security functional requirements, August 1999, Version 2.1, CCIMB-99-032, 362 stran
(Part 2, Security functional requirements, establishes a set of security functional components as a standard way of expressing the security functional requirements for Targets of Evaluation (TOEs). Part 2 catalogues the set of functional components, families, and classes.)

Common Criteria for Information Technology, Security Evaluation , Part 3, Security assurance requirements, August 1999, Version 2.1, CCIMB-99-033, 216 stran
(Part 3, Security assurance requirements, establishes a set of assurance components as a standard way of expressing the assurance requirements for TOEs. Part 3 catalogues the set of assurance components, families, and classes. Part 3 also defines evaluation criteria for Protection Profiles (PPs) and Security Targets (STs) and presents evaluation assurance levels that define the predefined CC scale for rating assurance for TOEs, which is called the Evaluation Assurance Levels (EALs)).

Společná kritéria (CC):
http://www.tno.nl/instit/fel/refs/cc.html, resp.
http://www.cse.dnd.ca/cse/english/cc.html.

VII.6 Kritéria pro hodnocení bezpečnosti IT - ISO/IEC 15408

Norma ISO 15408 vychází z CC viz. kapitola 4. Tato norma je dostupná jako norma ČSN ISO.

Charakteristiky úrovní zaručitelnosti bezpečnosti podle ISO/IEC 15408

Norma zavádí sedm *úrovní zaručitelnosti bezpečnosti*, *EAL* (Evaluation Assurance Level). Jsou uspořádané hierarchicky, každá úroveň musí splňovat jednak požadavky zaručitelnosti všech nižších úrovní a navíc požadavky definované na dané úrovni zaručitelnosti nově. Pro konkrétní aplikační prostředí se mohou jednotlivé úrovně zaručitelnosti bezpečnosti volitelně zesilovat.

Pro informaci zde uvedeme požadavky na EAL 1.

EAL1, funkčně testovaný produkt nebo systém IT

Cíle EAL1

- Úroveň EAL1 je použitelná tam, kde se požaduje správný (bezchybný) provoz, ale hrozby nejsou posuzovány jako závažné. Je vhodná tehdy, když se požaduje získání nezávisle vyslovené záruky podporující tvrzení, že byla vynaložena patřičná snaha o ochranu např. personalistik a podobných informací.
- Úroveň EAL1 se odvozuje z hodnocení produktu nebo systému IT dostupného zákazníkovi. Hodnocení zahrnuje nezávislé testování, zda jsou splněny specifikace a

zkoumání poskytnuté dokumentace s návody. Hodnocení na této úrovni by mohlo být úspěšně proveditelné bez spoluúčasti a bez pomoci vývojáře a mohlo by si vyžádat vynaložení minimálních nákladů.

- Při hodnocení produktu nebo systému IT úrovně EAL1 se poskytují důkazy, že jeho funkčnost je konzistentní s dokumentací a že poskytuje použitelnou ochranu proti identifikovaným hrozbám.

Záruky EAL1

- Úroveň EAL1 je základní úrovní zaručitelnosti bezpečnosti danou výsledky analýzy bezpečnostních funkcí pomocí specifikací funkcí a rozhraní a dokumentace s návody prováděnou s cílem porozumět bezpečnostnímu chování.
- Analýza se podporuje nezávislým testováním bezpečnostních funkcí.
- Ve srovnání s nehodnocenými produkty nebo systémy IT úroveň EAL1 představuje významně vyšší zaručitelnost bezpečnosti.
- Hodnocení na úrovni EAL1 se týká identifikace (čísla verze) produktu nebo systému IT, procedur instalace, generování a spuštění provozu, neformální specifikace funkcí, dokumentace správce a uživatele a provádí se nezávislé testování bezpečnostních funkcí.

V další části se budeme zabývat bezpečnostními funkcemi, definovanými v druhém díle mezinárodním standardu ISO/IEC 15408 ("Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT - Část 2: Bezpečnostní funkční požadavky" [ISO/IEC 15408-2].

Bezpečnostní funkční komponenty, definované ve druhé části ISO/IEC 15408, jsou základem pro funkční požadavky bezpečnosti produktu nebo systému IT, vyjádřené v profilu ochrany (PP – Protection Profile) a v bezpečnostním cíli (ST – Secure Target). Tyto požadavky popisují požadované bezpečnostní chování, očekávané od bezpečného produktu nebo systému IT a musí splňovat bezpečnostní plán, uvedený v PP nebo ST. Tyto požadavky popisují bezpečnostní vlastnosti, které mohou uživatelé pozorovat při jejich přímé interakci s produktem nebo systémem IT (tj. při jeho vstupních a výstupních operacích) a nebo pozorováním odezvy produktu nebo systému IT na podnět.

Bezpečnostní funkční komponenty vyjadřují bezpečnostní požadavky, jejichž cílem je zabránit hrozbám v předpokládaném provozním prostředí produktu nebo systému IT a/nebo pokrýt všechny identifikované bezpečnostní politiky organizace nebo jiné předpoklady.

Dokument ISO/IEC 15408 je určen pro spotřebitele, vývojáře a hodnotitele bezpečných systémů a produktů IT. Tyto skupiny mohou využít ISO/IEC 15408-2 následujícím způsobem:

- Zákazníci použijí ISO/IEC 15408-2 pří výběru komponent pro vyjádření svých funkčních požadavků, které splní bezpečnostní plán, vyjádřený PP nebo ST. Kapitola 4.3 dokumentu ISO/IEC 15408-1 poskytuje podrobnější informace o vztahu mezi bezpečnostní plánem a bezpečnostními požadavky

- Vývojáři, kteří reagují na skutečné nebo předpokládané bezpečnostní požadavky spotřebitelů při vývoji produktu nebo systému IT, mohou v této části ISO/IEC 15408 nalézt standardizované metody pro porozumění požadavků zákazníků. Mohou také využít obsah této části ISO/IEC 15408 jako základ pro definici bezpečnostních funkcí a mechanismů, které splňují tyto požadavky.

- Hodnotitelé využijí funkční požadavky, definované v této části ISO/IEC 15408 při ověřování, zda funkční požadavky, vyjádřené v PP nebo ST splňují bezpečnostní plány a zda byly vzaty v úvahu všechny vzájemné závislosti a bylo ukázáno, že jsou splněny. Hodnotitelé by si také měli vzít tuto část ISO/IEC 15408 na pomoc při rozhodování, zda daný produkt nebo systém IT splňuje dané požadavky.

Organizace dokumentu ISO/IEC 15408-2

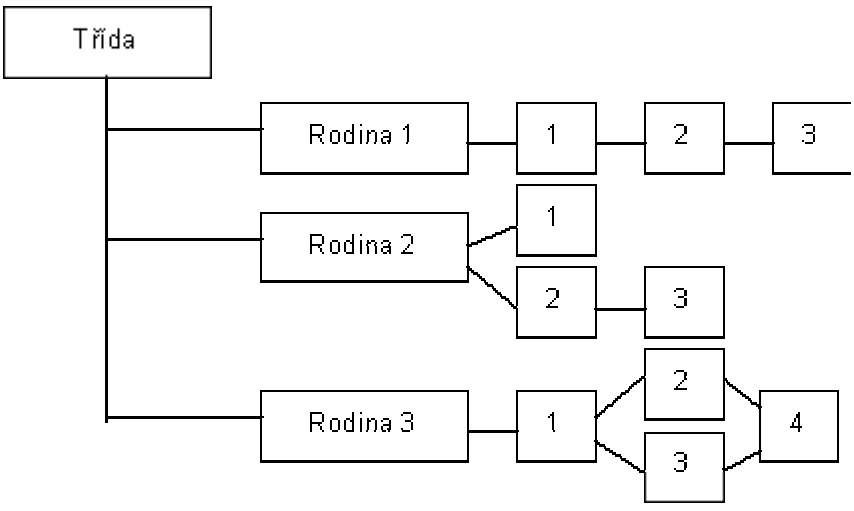
Kapitola 1 obsahuje úvodní materiál k ISO/IEC 15408-2. Kapitola 2 uvádí katalog funkčních komponent ISO/IEC 15408-2 a kapitoly 3 až 13 popisují jednotlivé funkční třídy. Příloha A poskytuje dodatečné informace, které by mohly zajímat potenciální uživatele funkčních komponent, včetně úplné tabulky křížových referencí závislostí jednotlivých komponent. Přílohy B až M obsahují aplikační informace k jednotlivým funkčním třídám.

Katalog komponent funkčních požadavků

Seskupení komponent funkčních požadavků v ISO/IEC 15408-2 neodpovídá žádné formální taxonomii. Bezpečnostní funkce jsou rozděleny do kategorií, které se nazývají třídy (např. třída Bezpečnostní audit nebo třída Komunikace). Každá třída se skládá z rodin, které odpovídají například bezpečnostním funkcím v kritériích CTPEC. Konečně každá rodina se skládá z komponent, které plní požadavky rodiny s různou mírou ochrany. Na rozdíl od kritérií CTPEC nemusí být jednotlivé komponenty nutně hierarchické (viz dále).

Katalog funkčních požadavků obsahuje třídy rodin a komponent, které jsou pouhým seskupením podle podobné funkce nebo podobného účelu a komponenty v rámci třídy jsou uvedeny v abecedním pořadí.

Na začátku každé třídy je uveden v dokumentu ISO/IEC 15408-2 informativní diagram, který ukazuje strukturu této třídy, rodiny v této třídě a komponenty v každé rodině.



Obr. Ukázka rozdělení třídy na rodiny a komponent

Katalog obsahuje následující třídy:

Třída FAU: Bezpečnostní audit

Třída FCO: Komunikace

Tato třída obsahuje dvě rodiny, které se zabývají bezpečným zjištěním identity protistrany, která se účastní výměny (přenosu) dat. Tyto rodiny se vztahují k zajištění identity původce přenášené informace (důkaz původu) a k zajištění identity příjemce přenášené informace (důkaz přijetí). Tyto rodiny zajišťují, že ani původce nemůže popřít odeslání

zprávy, ani příjemce nemůže popřít její přijetí. Třída bezpečnostních funkcí Komunikace obsahuje tyto rodiny komponent:

- FCO-NRO Nepopiratelnost původu
- FCO-NRR Nepopiratelnost přijetí

Třída FCS: Kryptografická podpora

Bezpečnostní funkcionalita hodnoceného předmětu (TOE : Target of Evoluation) může zahrnovat i kryptografické funkce, které pomohou splnit některé bezpečnostní plány vyšší úrovně. Tyto plány zahrnují (mimo jiné): identifikaci a autentizaci, nepopiratelnost, důvěryhodnou cestu, důvěryhodný kanál a oddělení dat. Tato třída se použije, pokud TOE obsahuje kryptografické funkce, jejichž implementace může být pomocí hardware, firmware a/nebo software.

Třída FCS se skládá ze dvou rodin: FCS-CKM Správa kryptografických klíčů a FCS-COP Kryptografické operace. Rodina FCS-CKM se zabývá aspekty správy kryptografických klíčů, zatímco rodina FCS-COP se zabývá jejich provozním použitím.

- FCS-CKM Správa kryptografických klíčů
- FCS-COP Kryptografické operace

Třída FDP: Ochrana uživatelských dat
Třída FIA: Identifikace a autentizace
Třída FMT: Správa bezpečnosti
Třída FPR: Soukromí
Třída FPT: Ochrana bezpečnostní funkcionality
Třída FRU: Využití zdrojů
Třída FTA: Přihlášení do TOE
Třída FTP: Důvěryhodné cesty/kanály

VII.7 Federal Information Processing Standard (FIPS 140-1 a FIPS 140-2)

FIPS 140-1: Security Requirements for Cryptographic Modules, January 4, 1994.
FIPS 140-2: Security Requirements for Cryptographic Modules, May 25, 2001. Change Notices 2, 3 and 4: 12/03/2002

Tyto standrady vydal *National Institute for Standards and Technology* (NIST), který je vládním standardizačním orgánem (nástupce NBS - National Bureau of Standards , který byl založen již 1901 !). NIST vydává standardy pro federální vládu USA (http://www.nist.gov/).

Související standardy tzv. kryptografické standardy:
FIPS 197: Advanced Encryption Standard (AES). FIPS 197 specifies the AES algorithm.
FIPS 46-3 and FIPS 81: Data Encryption Standard (DES) and DES Modes of Operation. FIPS 46-3 specifies the DES and Triple DES algorithms.
FIPS 186-2 and FIPS 180-1: Digital Signature Standard (DSS) and Secure Hash Standard (SHS), which specify the DSA, RSA, ECDSA, and SHA-1 algorithms

Na začátku července 2001 bylo NIST (National Institute of Standards and Technology – USA) oznámeno schválení nové verze známé normy FIPS-140 (datum vydání uvedené v samotném dokumentu je 25. květen 2001). Tato podoba normy nahrazuje předchozí verzi FIPS PUB 140-1 z ledna 1994. Základní informace o normě lze nalézt na adrese [1] ,

samotnou normu pak na adrese [2] . Draft FIPS-140-2 byl zveřejněn již v roce 1995 a byl tak podroben rozsáhlé diskusi.

Nesporně zajímavým dokumentem je [3] , které přináší podrobné srovnání obou verzí FIPS 140, tj. verze FIPS 140-1 a FIPS 140-2.

Bezpečnostní požadavky v normě obsažené jsou rozděleny do 11 oblastí a hodnoceny dle čtyř úrovní bezpečnosti (s postupně narůstajícími nároky). To platí pro obě verze normy. Jak však lze vidět z následující tabulky, pozměnil se obsah těchto oblasti:

FIPS 140-1	FIPS 140-2
4.1 Cryptographic Modules	4.1 Cryptographic Module Specification*
4.2 Cryptographic Module Interfaces	4.2 Cryptographic Module Ports and Interfaces
4.3 Roles and Services	4.3 Roles, Services, and Authentication*
4.4 Finite State Machine Model	4.4 Finite State Model
4.5 Physical Security	4.5 Physical Security*
4.6 Software Security	4.6 Operational Environment*
4.7 Operating System Security	4.7 Cryptographic Key Management
4.8 Cryptographic Key Management	4.8 EMI/EMC
4.9 Cryptographic Algorithms	4.9 Self-Tests*
4.10 EMI/EMC	4.10 Design Assurance*
4.11 Self-Tests	4.11 Mitigation of Other Attacks*

Přitom odstavce označené hvězdičkou byly zcela přepracovány, nebo doznaly význačných změn.

Změny vychází v převážné většině z nezbytnosti reagovat na existenci nových technologií či nových bezpečnostních požadavků (např. autentizace v paragrafu 4.3 atd). V odstavci 4.6 dochází k významné změně v odkazu na hodnocení bezpečnosti informačních systémů. Zatímco dříve se norma odkazovala na TCSEC, odkazuje se FIPS 140-2 již na Common Criteria. Odstavec 4.11 je vlastně nový (došlo k přesunu jiných odstavců) a jeho význam spočívá v tom, že metodika zde umožňuje reagovat na řadu kryptografických útoků, které se objevily teprve v poslední době (jako jsou analýza spotřeby proudu, časová analýza, analýza vynucených chyb atd.).

NIST a CES (obdobná kanadská instituce) dále připravili příručku (FIPS 140-2 Implementation Guidance) pro výrobce kryptografických modulů a testovací laboratoře. Rovněž tak je připravována nová verze dokumentu FIPS 140-2 Derived Test Requirements.

Od **26.5.2002** přijímají všechny testovací laboratoře jen validační zprávy, které testují proti FIPS 140-2.

Dále však ještě dobíhají testování podle FIPS PUB 140-1. To znamená, že pokud byla přijata žádost před 26.5.2002, probíhá testování ještě podle této žádosti a hodnotí se proti FIPS 140-1.

Agentury / zákazníci si i po 25. květnu 2002 mohou stále kupovat a používat potvrzené produkty podle FIPS 140-1.

V současné době všechny laboratoře CMT již jsou připraveny testovat kryptografické moduly podle FIPS 140-2

Podle tohoto standardu jsou hodnoceny kryptografické moduly a zařízení. Hodnocené prostředky se dělí do 4 odlišných tříd úrovně zabezpečení – (Level 1 až Level 4).
Nejnižší požadavky jsou kladeny na úroveň zabezpečení 1.

Odkazy:

[1] http://csrc.nist.gov/cryptval/140-2.htm
[2] http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
[3] http://csrc.nist.gov/publications/nistpubs/800-29/sp800-29.pdf
[4] http://csrc.nist.gov/cryptval/140-1/1401val.htm
[5] http://www.nist.gov/public_affairs/general2.htm
[6] http://csrc.nist.gov/cryptval/