Přehled některých základních kritérií hodnocení

Úvodní informace

Obsah :

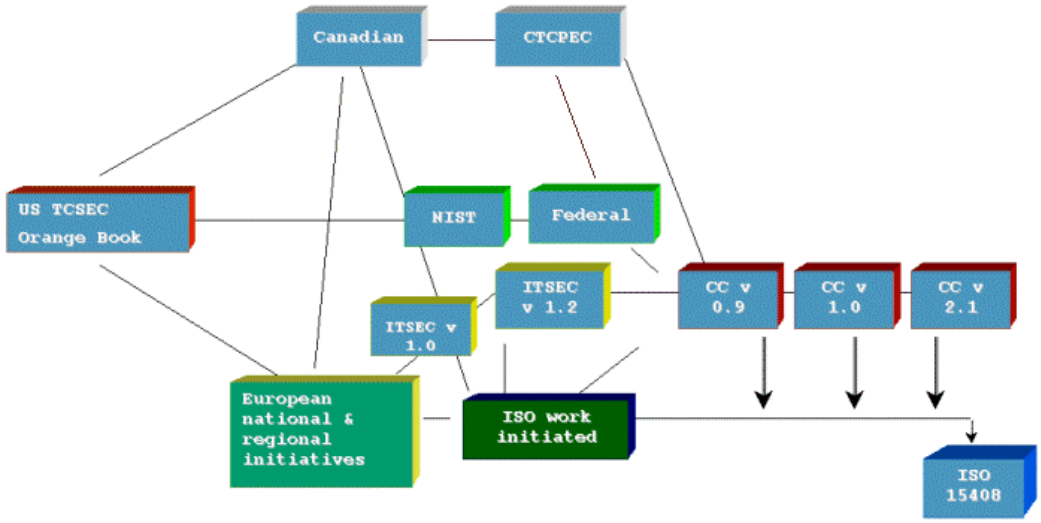
1. Úvod

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.).



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/

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

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/

V. 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.

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.

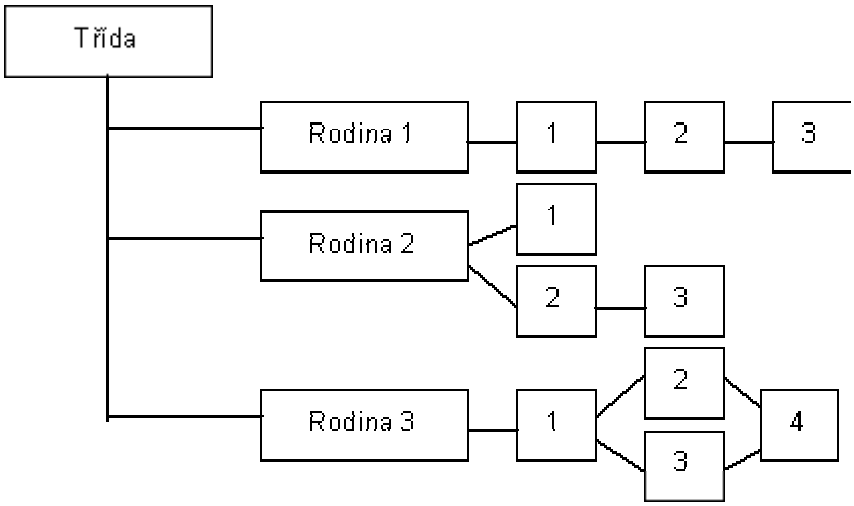
Organizace dokumentu ISO/IEC 15408-2

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.

Model funkčních požadavků

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

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 zabezepečení – (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/