Aplikovaná kryptografie a Společná kritéria

Luděk Novák

lnovak@gity.cz

GiTy, a.s.
Mariánské náměstí 1
Brno / Česko

Abstrakt

Společná kritéria jsou celosvětově uznávaným standardem, který slouží k přesnému vyjádření bezpečnostních charakteristik v průmyslu informačních technologií. Jednou z možností realizace bezpečnostních mechanismů je aplikování kryptografických technik. Tento příspěvek se snaží přiblížit možnosti Společných kritérií, objasňuje základní rysy profilů bezpečnosti a upozorňuje na způsoby využití aplikované kryptografie u několika konkrétních profilů bezpečnosti.

Klíčová slova: Společná kritéria, katalog kryptografických funkcí, profily bezpečnosti.

1 Úvod

Společná kritéria se jako norma ISO/IEC 15408:1999 stávají celosvětovým standardem pro formulování bezpečnostních požadavků u informačních technologií. Tato kritéria obsahují i požadavky na bezpečnostní funkce, které se opírají o schopnosti aplikované kryptografie.

Tento příspěvek se snaží objasnit postavení kryptografie v celém komplexu Společných kritérií. Nejprve je pozornost věnována postavení kryptografických funkcí v katalogu bezpečnostních funkcí. V dalších částech jsou pak demonstrovány praktické příklady použití katalogu kryptografických funkcí na existujících profilech bezpečnosti. Současně jsou rozebrány tři možnosti zavedení kryptografických požadavků do popisu bezpečnostních technologií.

2 Společná kritéria

Společná kritéria[1] (pro hodnocení bezpečnosti informačních technologií) [1] jsou výsledkem snah o vytvoření normy pro hodnocení bezpečnosti informačních technologií, která by byla uznána širokou mezinárodní komunitou. Mezi základní cíle normy patří především zformování jednotných celosvětových bezpečnostních kritérií, která dovolí vzájemné uznávání výsledků hodnocení na celém světě. V širších souvislostech má tato norma přispět k rozšíření nabídky kvalitních bezpečnostních produktů.

Celou normu ISO/IEC 15408:1999 tvoří tři dokumenty. První definuje globální koncepci a principy hodnocení bezpečnosti informačních technologií. Také je zde popsána konstrukce základních používaných struktur a vysvětlena používaná terminologie. Druhý dokument obsahuje katalog požadavků na bezpečnostní funkce. V tomto dokumentu je vysvětleno obecné chápání **předmětu hodnocení**[2]. Další části obsahují obšírné vymezení požadavků všech jedenácti funkčních tříd, ze kterých jedna je přímo věnována kryptografii. Poslední, třetí dokument obsahuje katalog požadavků na bezpečnostní záruky, které jsou

[1] Označení Společná kritéria (Common Criteria – CC) je vžité jméno normy ISO/IEC 15408, jejíž oficiální název zní **Kritéria hodnocení bezpečnosti informačních technologií** (Evaluation Criteria for Information Technology Security).

[2] Předmět hodnocení (Target of Evaluation – TOE) je část produktu nebo informačního systému, která je subjektem hodnocení bezpečnosti.

tvořeny deseti třídami. V dokumentu je též objasněn účel a obsah sedmi účelových sad, které míru záruk pojímají jako ucelený soubor požadavků.

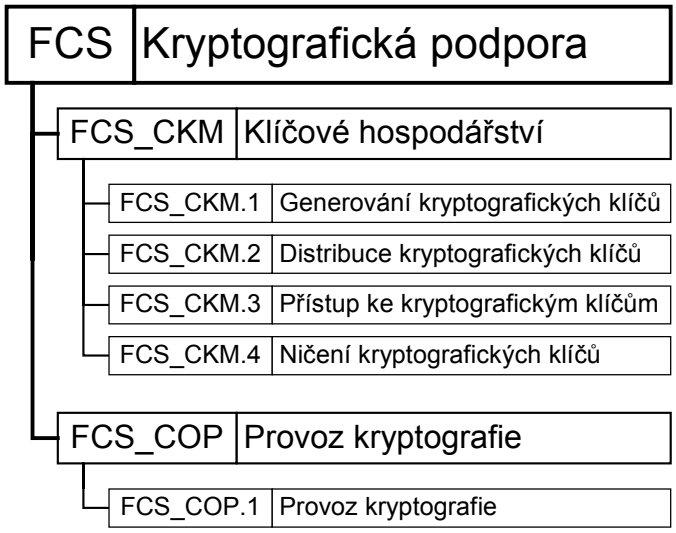
2.1 Katalog kryptografických požadavků

Společná kritéria soustředí požadavky kryptografické funkce do třídy **FCS: Kryptografická podpora** (Cryptographic Support). Tato třída obsahuje dvě rodiny, ze kterých první nazvaná **FCS_CKM: Klíčové hospodářství** (Cryptographic Key Management) zahrnuje bezpečností požadavky spojené s životním cyklem kryptografických klíčů a obsahuje následující komponenty:

- **FCS_CKM.1: Generování kryptografických klíčů** (Cryptographic Key Generation) – zpřesňuje délku generovaných klíčů, použité algoritmy a vazby na mezinárodní, státní či oborové normativy;
- **FCS_CKM.2: Distribuce kryptografických klíčů** (Cryptographic Key Distribution) – stanoví metody a pravidla šíření klíčů;
- **FCS_CKM.3: Přístup ke kryptografickým klíčům** (Cryptographic Key Access) – specifikuje použité typy přístupů, pravidla a způsoby zálohování, archivace a obnovení klíčů;
- **FCS_CKM.4: Ničení kryptografických klíčů** (Cryptographic Key Destruction) – upřesňuje metody a postupy destrukce klíčů včetně vazeb na příslušné standardy.

Druhá rodina **FCS_COP: Provoz kryptografie** (Cryptographic Operation) pak vyjadřuje provozní požadavky spojené s využitím kryptografických nástrojů a obsahuje pouze jednu komponentu:

- **FCS_COP.1: Provoz kryptografie** (Cryptographic Operation) – při popisu TOE musí komponenta upřesnit způsoby aplikace a módy kryptografických operací, použité kryptografické algoritmy, přípustné délky klíčů a vazby na specializované standardy.



Obrázek 1 Rozdělení třídy kryptografických požadavků

Všechny zformulované požadavky jsou velice povrchní a široce se odkazují na zapracování vhodných mezinárodních, národních či oborových norem. Důvodem je ponechání prostoru pro speciální odborné normy (např. FIPS140 apod.), které jsou více zohledňují kryptografická specifika. Z tohoto důvodu se CC omezují na základní styčné body, na základě kterých je možné vydefinovat rozhraní, kde na jedné straně máme řekněme obecnější aplikovanou kryptografii (např. hardwarový šifrovací modul, popis symetrického algoritmu) a druhou stranu tvoří správné začlenění kryptografických funkcí do komplexnější bezpečnostní technologie (např. VPN brány, PKI infrastruktury).

Tato forma velmi volné vazby Společných kritérií a kryptografických norem oba odborné směry přímo nesvazuje a dovoluje jejich relativně nezávislý rozvoj. Zásadní výhoda pak spočívá ve skutečnosti, že Společná kritéria ani jejich praktické použití nemusí být nezbytně spojeno s konkrétní vymezením

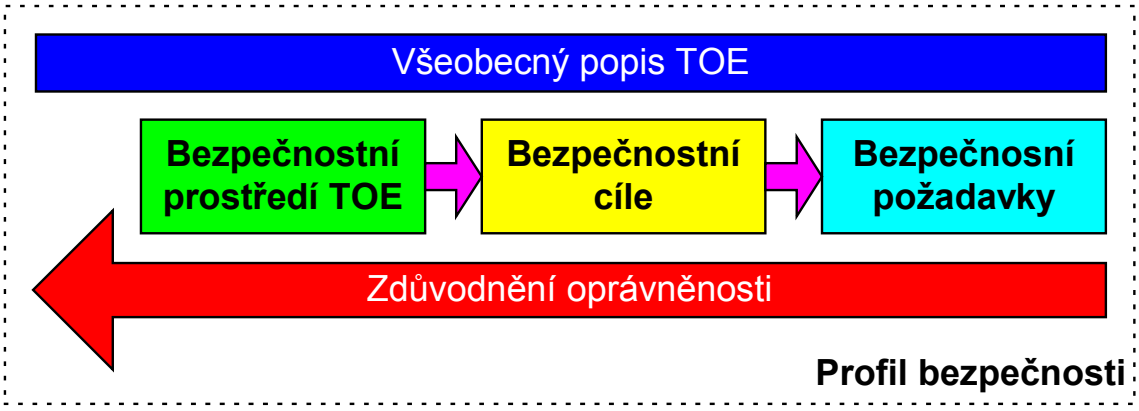
kryptografických parametrů. A proto mohou být tyto parametry vyjádřeny odkazy na příslušné normativy, které se dokonce mohou odlišovat podle toho, kde bude TOE využito (např. nasazení TOE v armádním prostředí znamená využití specifického katalogu algoritmů apod.).

2.2 Profily bezpečnosti

Oba katalogy požadavků jsou velmi komplexní a jejich přímé použití je prakticky nemožné. Proto Společná kritéria definují **profil bezpečnosti** (Protection Profile – PP) jako implementačně nezávislou množinu bezpečnostních požadavků určité skupiny předmětů hodnocení, které pokrývají přesně vymezené potřeby uživatele [1], [2].

Cílem profilu bezpečnosti je přesné, jednoznačné a konzistentní vymezení bezpečnostních požadavků, které jsou společné pro určitou množinu TOE. Obsah profilu je rozdělen do pěti následujících informačních celků (viz obrázek 2):

1. **Všeobecný popis TOE** – obsahuje informace, které daný profil identifikující (např. jméno PP, verze PP ap.) a které vysvětlují obecné vlastností TOE. Nepovinným popisem je upřesnění hranic TOE a základních podmínek správného použití.
2. **Bezpečnostní prostředí TOE** – má jasně a jednoznačně vymezit povahu a rozsah bezpečnostních potřeb TOE. Charakteristika prostředí je dána předpoklady použití TOE, popisem existujících hrozeb a vymezením bezpečnostních zásad organizace, kterým má TOE vyhovovat.
3. **Bezpečnostní cíle** – vyjadřují záměr jak uspokojit bezpečnostní potřeby TOE. Části potřeb čelí přímo bezpečnostní funkce TOE. Zbylá část je uspokojena vlastnostmi prostředí, ve kterém má být TOE používáno.
4. **Bezpečnostní požadavky** – jsou klíčový blokem celého profilu. Zde jsou za pomoci obou katalogů normy ISO/IEC 15408:1999 vymezeny vlastnosti všech bezpečnostních funkcí TOE a upřesněna míru záruk za jejich správné fungování.
5. **Zdůvodnění oprávněnosti** – dokládá úplnost a bezrozpornost návrhu profilu. V první části musí být doložena oprávněnost bezpečnostních cílů (tj. vazby mezi celky 2 a 3). Ve druhé pak oprávněnost bezpečnostních požadavků (tj. vazby mezi celky 3 a 4).

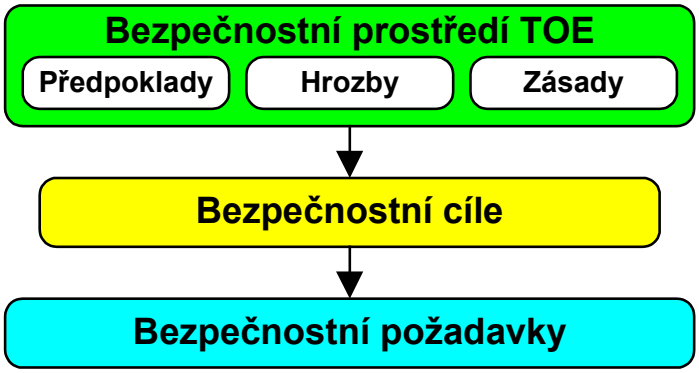


Obrázek 2 Základní informační celky PP

Systematické uspořádání profilu bezpečnosti přináší srozumitelné vyjádření bezpečnostní potřeb uživatele, ve kterém je plynule zvyšována podrobnost popisu. Ta začíná u obecného popisu TOE a končí u zdůvodnění vnitřních vazeb, které osvětlují existenci všech potřeb, cílů i požadavků.

Východiskem kvalitního zformování bezpečnosti je jasné a jednoznačné vymezení povahy a rozsahu bezpečnostních potřeb, kterém má TOE čelit. Cílem popisu prostředí je snaha přesně vymezit bezpečnostní aspekty prostředí. Charakteristika prostředí je složena popisu předpokladů, hrozeb a bezpečnostních zásad organizace. Popis bezpečnostního prostředí je i základem pro následné aplikování kryptografických požadavků, které tudíž mohou být zavedeny za pomoci (viz obrázek 3):

- **bezpečnostních zásad organizace** – je asi nejjednodušší cestou (blíže viz profily popisované v kapitolách 3.2 a 4.1.1);
- **předpokladů** – není příliš často používaným postupem (blíže viz profily popisované v kapitolách 3.1 a 4.1.2);
- **hrozeb** – je vzhledem k vyšší složitosti vazeb poměrně náročné a pro uživatele profilu není příliš přehledné (blíže viz profily popisované v kapitole 4.3);



Obrázek 3 Tři formy popisu bezpečnostního prostředí

Jak už bylo uvedeno profil bezpečnosti je určen k vyjádření zobecněných bezpečnostních požadavků (např. pro daný okruh nástrojů či zařízení). V případě vývoje reálných zařízení je nutné popis profilu bezpečnosti dále upřesňovat. V těchto případech mluvíme o **specifikaci bezpečnosti** (Security Target – ST) jako cílové kombinací bezpečnostních komponent, která již nevyjadřuje obecný pohled na bezpečnostní problematiku, ale vždy je těsně spojena s konkrétním systémem či produktem.

V případě kryptografických požadavků to znamená, že tvůrce specifikace bezpečnosti musí konkretizovat všechny zobecněné požadavky profilů. Jinými slovy to znamená, že tvůrce specifikace musí doplnit konkrétní použité kryptografické funkce, algoritmy i délky klíčů. To je nezbytné zvláště v případech, kdy profily obdobné informace neobsahují.

2.3 Obecný popis bezpečnosti kryptografických modulů

Na normu ISO/IEC 15408:1999 úzce navazuje pracovní dokument ISO/IEC PDTR 15446, který upřesňuje postupy tvorby profilů a specifikací bezpečnosti. Zvláštnosti spojené s nasazením kryptografických modulů soustředí příloha C, která obsahuje doporučení zohledňující zvláštnosti spojené s formováním PP či ST zahrnující aspekty kryptografických modulů. Základem zmiňované přílohy je výčet všeobecných hrozeb a bezpečnostních zásad, které jsou s kryptografickými moduly spojeny a které by se nějak měly do návrhu řešení promítnout. Příklady základních hrozeb, cílů a jejich zdůvodnění je uveden v příloze tohoto příspěvku.

3 Evropské profily bezpečnosti

Vytváření profilů bezpečnosti není úplně jednoduchou záležitostí a reálné výsledky má pouze některé státní či komerční organizace, které disponují dostatečnými odbornými kapacitami. Díky tomu většina obdobných aktivit pochází pouze ze dvou hlavních teritorií – evropského a amerického.

Evropské aktivity spojené s formováním profilů lze vnímat jako poměrně roztříštěné a méně koordinované. Činorodé jsou různé komerční organizace, které svoje činnosti úzce váží na vládní organizace Velké Británie, Francie a Německa. Připraveno a certifikováno bylo již několik profilů, které například řeší bezpečnost čipových karet, systémů řízení báze dat nebo mobilních kódů. Jednotlivé aktivity se většinou soustředí na jednotlivé typy či druhy bezpečnostních technologií, avšak projekty nejsou ve větší měře koordinovány.

Jedním z prvních evropských orgánů, které započali s certifikací profilů bezpečnosti, byl úřad CESG ve Velké Británii. Jeho aktivity se soustředily především na problematiku operačních systémů a systémů řízení bází dat. V nedávné době byly aktivity rozšířeny i o bezpečnost mobilních kódů. Jediným profilem, který obšírněji aplikuje kryptografické funkce, je poslední certifikovaný profil označený **Postage Meter Approval Protection Profile** upřesňující fungování „registračních pokladen“ poštovních služeb.

Z pohledu kryptografie jsou zajímavější aktivity francouzské SCSSI, které od roku 1998 certifikovala již několik různých profilů popisujících bezpečnost čipových karet. Jedním s posledních je **Smart Card Security User Group Smart Card Protection Profile**, který byl certifikován v září roku 2001 a kterému se budeme věnovat podrobněji.

S drobným příspěvkem přišlo i německé BSI, které doposud certifikovalo dva profily. Jedním z nich je profil s názvem **Smartcard IC Platform Protection Profil** certifikovaný v červenci 2001, které se soustředí na vyjádření bezpečnosti technického vybavení čipových karet včetně zabudovaného programového vybavení a který vyžaduje záruky EAL4.

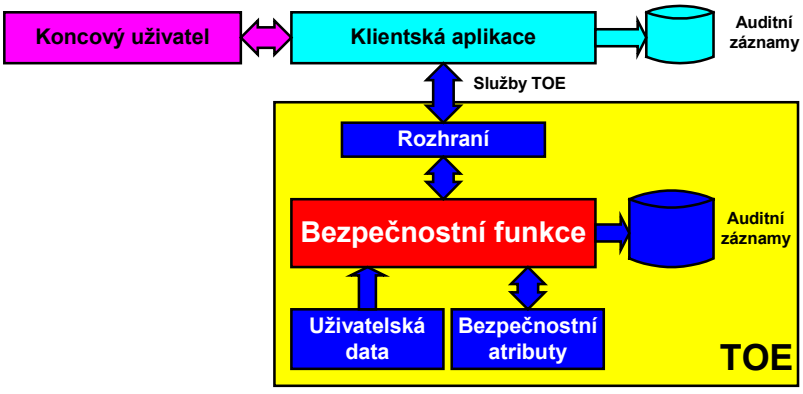
Novým evropským subjektem, který začal pracovat na tvorbě profilů bezpečnosti je iniciativa EESSI, které připravuje návrh profilu s názvem **Cryptographic Module for CSP Signing Operations – Protection Profile**. Tento profil je velmi důležitý, protože je úzce spojen s tvorbou evropských zásad a pravidel pro využívání elektronického podpisu a podrobněji se mu bude věnovat následující kapitola.

3.1 Evropský profil pro elektronický podpis

Přelom století evropský informační průmysl spojil s intenzivními aktivity, které jsou spojené s využíváním elektronického podpisu. Jako součást úsilí se na jaře roku 2001 objevila snaha o zformulování profilu **Cryptographic Module for CSP Signing Operations – Protection Profile** (CMCSO PP), jehož poslední pracovní verze 0.18 byla zveřejněna v listopadu 2001. Tento profil je přímo odvozován od evropských direktiv spojených s elektronickým podpisem a s vydáváním kvalifikovaných certifikátů.

Předmětem hodnocení profilu je kryptografický modul, který je jádrem důvěryhodného systému pro poskytování služeb elektronického podpisu. TOE tudíž zahrnuje bezpečnost služeb spojených s generováním dat pro vytváření elektronických podpisů a s vytvářením zaručených elektronických podpisů. Primární oblastí použití je vytváření zaručených elektronických podpisů, nicméně tento profil je možné aplikovat i na příbuzné činnosti např. při tvorbě časových razítek.

Obsahem profilu jsou požadavky na technické a programové vybavení kryptografického modulu. Potřebné parametry kryptografických algoritmů nejsou v profilu obsaženy přímo a jsou dány jen odkazem na příslušný dokument. Profil se opírá o záruky EAL4+ (rozšířený zejména o náročnější analýzu zranitelnosti) a všechny použité bezpečnostní mechanismy musí vykazovat minimální odolnost na vysoké úrovni. Aplikování profilu počítá se třemi nezávislými bezpečnostními rolemi, za které jsou považovány role: uživatel, správce a auditor. Vnitřní uspřádání a vnější vazby TOE jsou zachyceny na obrázku 4.



Obrázek 4 Vnitřní struktura TOE

Pohledem na tento obrázek zjistíme, že reálný uživatel používá klientskou aplikaci, které pak dále komunikuje s rozhraním TOE v zastoupení uživatele. Díky tomu je aplikace odpovědná za předávání korektních dat a stává se tak nedílnou součástí prostředí, ve kterém je TOE používáno. Tato bezpečnostní potřeba se prolíná celým profilem.

Základem pro její úspěšné naplnění je předpoklad A.Human_Interface, který se pokouší o řešení problému spojeného s odlišnostmi v technickém a lidském vnímán a říká, že bezpečnost TOE se opírá o spolehlivé fungování klientských aplikací. Profil předpokládá, že digitální údaje jsou klientskými aplikacemi zobrazeny správně a že jsou předávány skrze důvěrný kanál. Tento předpoklad, v obecné rovině zajisté správný, přenáší zásadní problém spojený s elektronickým podpisem na bedra aplikačního programového vybavení, které tudíž nutně musí vykazovat shodné bezpečnostní kvality.

Použití předpokladu vede k formulaci dvou bezpečnostních cílů O.ENV_Application a O.ENV_Human_Interface, které jsou spojeny s bezpečností klientské aplikace. Oba cíle jsou ošetřeny požadavky, které musí klientská aplikace obsahovat (např. nezbytnost používání důvěryhodné cesty). Bohužel skutečné aplikační systémy, které požadovaný komplex služeb obsahují, se prakticky nevyskytují. A navíc ani nejsou obecně zformulovány náležité bezpečnostní požadavky například formou příslušného profilu, takže je vývoj takových aplikací poměrně obtížný.

Nicméně je nutné konstatovat, že autoři si tento problému uvědomují a nad rámec běžné praxe profil obsahuje množství přesně zformulovaných požadavků, které nejsou spojeny s bezpečností TOE. Tyto požadavky upřesňují bezpečnostní vlastnosti prostředí, ve kterém má být TOE nasazeno. Otázkou však zůstává, jak klientské aplikace vytvářet a jak je formálně hodnotit tak, aby mohl byl náležitě zkompletován celý systém pro vytváření elektronických podpisů.

3.2 Profil bezpečnosti čipových karet

Sdružení uživatelů čipových karet je hlavním tvůrcem profilu **Smart Card Security User Group Smart Card Protection Profile – SCSUG SCPP**, jehož poslední verze 3.0 byla v září 2001 certifikována francouzskými úřady. Východiskem nejsou pouze předchozí verze tohoto profilu (tvorba byla zahájena ke konci 90. let), ale též další aktivity často spojené s evropskými výrobci obdobných technologií. Profil je postaven na míře záruk EAL4+ (posíleny jsou požadavky na modularitu a na střední míru odolnosti).

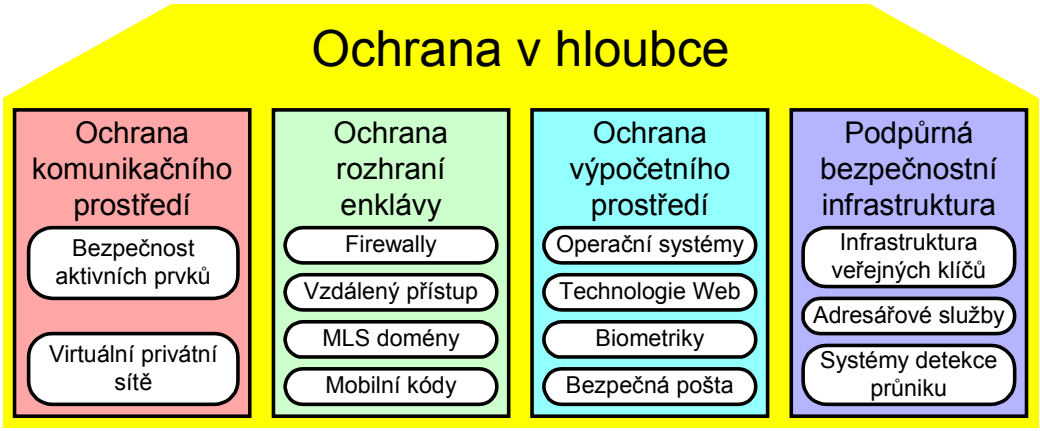
Bezpečnostní funkce TOE obsahují především: kryptografické operace, nástroje pro řízení přístupu, prostor pro bezpečné uložení klíčů a schopnosti auditu. Kryptografické požadavky jsou ošetřeny organizační zásadou P.Crypt_Std, která vyžaduje použití mechanismů v souladu příslušnými standardy bez bližšího upřesnění. To dává velký prostor výrobců, kteří mohou použít standard, který je pro jejich potřeby ideální (mezinárodní, národní, oborový apod.). Toto volné vymezení může být jednoduchým způsobem zpřesněno (blíže popis profilu v kapitole 4.1.1).

4 Americký systém profilů

Počátky tvorby profilů bezpečnosti jsou i na americkém kontinentu spojeny s méně koncepčními přístupy. Ke konci devadesátých let bylo certifikováno několik profilů (např. pro firewally či jako náhrady za třídy C2 a B1 kritérií TCSEC). Současně s tím vznikaly i nové profily více spojené s komerčním prostředím. Avšak na přelomu století dochází ke sjednocení víceméně rozptýleného úsilí NSA, NIST a dalších amerických tvůrců do komplexní program, který je nazýván „**Strategie ochrany v hloubce**“ (Defense in Depth Strategy).

Koncepce je zastřešena dvěma orgány, které vznikly sdružením více rozličných americké subjektů. Prvním orgánem je Inforamtion Assurance Technical Framework Forum – IATFF sdružující vládní i komerční organizace, jejichž společným úkolem je rozvoj celé strategie v souladu s bezpečnostními potřebami a podle skutečných možností amerického informačního průmyslu. Profily bezpečnosti jsou jedním ze základů budované strategie, protože jsou využívány jako společný komunikační nástroj určený pro popis

bezpečnostních vlastností informačních technologií. Jak je patrné z obrázku 5, pojetí strategie je ucelené a počet připravených profilů bezpečnosti se dnes blíží ke třem desítkám.



Obrázek 5 Profily bezpečnosti a Strategie ochrany v hloubce

Druhým orgánem je partnerská dohoda nazvaná National Information Assurance Partnership – NIAP, kterou uzavřely NSA a NIST. Základním úkolem NIAP, který zůstává plně pod vládní kontrolou, je udržení potřebné nezávislosti hodnocení a certifikace bezpečnosti IT. NIAP je odpovědný např. za výběr hodnotících laboratoří. Součástí úkolů NIAP je i certifikace a validace profilů bezpečnosti. Takových je v současné době asi jedna desítka.

Zásadní výhodou přístupu USA je komplexní a ucelené pojetí bezpečnosti a jasné rozdělení odpovědnosti zainteresovaných orgánů. Připravované profily pokrývají nejen specializované bezpečnostní nástroje ale i bezpečné fungování běžných technologií (např. operačních systémů). Jednotné zastřešení navíc usnadňuje společné nasazení a kombinování více rozdílných profilů.

4.1 Profily pro PKI

Důležitou skupinu amerických profilů, které jsou úzce spojeny s aplikovanou kryptografií, shromažďuje dokument **Certificate Issuing and Management Components (CIMC) Family of Protection Profiles**, jehož verze 1.0 byla certifikována v NIAP na konci října 2001.

Celé uskupení tvoří čtyři profily, které spojuje stejná funkční charakteristika TOE. Tu tvoří infrastruktura veřejných klíčů, jejíž jádrem jsou technologie pro vydávání a správu certifikátů např. certifikační či registrační autority a další funkční moduly PKI infrastruktury. Funkcí, které provádí komponenty pro vydávání a správu certifikátů (CIMC), jsou profilem rozděleny do třech následujících kategorií:

- bezpečnostní funkce spojené s fungováním PKI – tyto funkce musí být prováděny přímo uvnitř TOE;
- kryptografické funkce – jsou realizovány speciálními moduly v souladu s FIPS 140-1;
- ostatní bezpečnostní funkce – jsou většinou funkce, které zajišťuje operační systém (např. identifikace a autentizace uživatelů) a které tudíž většinou leží mimo TOE[3].

Všechny čtyři profily se odličují různou bezpečnostní úrovní (Security Level – SL), která vyjadřuje schopnost odolávat různému stupni hrozeb a rozsah zranitelných míst, jež společně určující míru celkového únosného rizika. Množiny předpokladů, hrozeb, organizačních zásad, cílů, požadavků i zdůvodnění spojených s každou úrovní jsou vyjádřeny samostatným profilem. Tyto profily jsou hierarchicky uspořádány od nejnižší úrovně SL1 až po nejnáročnější SL4.

[3] Tyto funkce mohou být v případě potřeby realizovány uvnitř TOE, nicméně profil je chápe jako požadavky na prostředí TOE.

První bezpečnostní úroveň SL1 vyjadřuje nejnižší míru bezpečnosti a je určena pouze pro prostředí, kde lze bezpečnostní riziko považovat za nízké. SL1 vyžaduje existenci dvou nezávislých rolí, kde první je odpovědná za správu účtů, generování klíčů, nastavení auditu. Druhá pak odpovídá za vydávání a správu certifikátů. Navržený systém musí odpovídat míře záruk EAL1+ (posíleno je testování funkčnosti). Z hlediska kryptografie je nutné, aby použité mechanismy byly v souladu s normou FIPS 140-1 Level 1.

Úroveň SL2 je určena pro prostředí, kde jsou bezpečnostní rizika považována za méně významná. Nad rámec SL1 jsou rozšířeny požadavky auditu včetně vyšší úrovně jejich ochrany. Spolu s tím jsou zpřísněny záruky na úroveň EAL–CSPP[4] a kryptografické funkce musí odpovídat FIPS 140-1 Level 2.

Další úroveň SL3 je připravena pro prostředí, které vykazuje střední míru rizika. Tomu odpovídají další požadavky spojené s udržením integrity, vyšší fyzickou ochranou TOE. Současně profil počítá se třemi rolemi. První má na starosti správu účtů a generování klíčů, druhá odpovídá za vydávání a rušení certifikátů a poslední má v péči auditní záznamy. Záruky SL3 vychází z úrovně EAL3+ (vyšší nároky na podrobný popis návrhu). Klíčové kryptografické moduly tohoto profilu musí odpovídat FIPS 140-1 Level 3.

Největší nároky jsou spojeny s SL4, které ještě není komerčně dostupná, avšak její příchod lze očekávat v blízké budoucnosti. Úroveň pokrývá prostředí, kde lze bezpečnostní rizika považovat za významná včetně výskytu nepřátelských jedinců. Bezpečnost je posílena především nutností udržení integrity auditních záznamů pomocí nezávislých časových razítek. Počet rolí je rozšířen na čtyři tím, že přibývá samostatná osoba odpovědná za zálohování. Taktéž záruky musí být velmi vysoké, což je vyjádřeno úrovní EAL4+ (zapojení i specializovaných metod vývoje). Důležité kryptografické moduly pak musí odpovídat nejvyšším požadavků FIPS 140-1 Level 4.

Na rozdíl od obdobného evropského profilu, je tato rodina profilů orientována čistě na technickou rovinu. To se projevuje již tím, že se nezmiňuje o elektronickém podpisu, ale pracuje pouze s termíny vydávání a správa certifikátů.

Zajímavým přístupem je účelné spojení více obdobných profilů do jediného dokumentu, kde jsou většinou nejdříve objasněna společná východiska. Za těmi pak následuje upřesnění či rozšíření, které je již platné pouze pro některý ze čtyř profilů. Tento přístup dovoluje snadné porovnání rozdílů v bezpečnostní náročnosti jednotlivých profilů. Díky otevřenému popisu profilů je pak možné optimalizovat formy konkrétního nasazení podle skutečných potřeb (např. cílené přenesením části hrozeb z vyššího profilu do nižšího).

Dalším zajímavým momentem je skutečnost, že katalog Společných kritérií je v profilech intenzivně rozšiřován právě v souvislosti se specifickými potřebami, které jsou spojeny se systémem klíčového hospodářství u PKI. Výsledním projevem je několik nových rodin požadavků, které úzce propojují jednotlivé profily bezpečnosti s normou FIPS 140-1. Nové požadavky upřesňují například formy ochrany důvěrnosti a integrity uživatelských klíčů, způsoby bezpečného uložení a ničení klíčů, pravidla pro export klíčů, zásady pro správu certifikátů a údržby CRL a obdobné požadavky, které jsou specifické pro PKI

1.1.1 Profil pro bezpečné uložení PKI klíčů

Dalším zajímavým materiálem je profil **Department of Defense Public Key Infrastructure Token Protection Profile**. Východiskem jeho poslední verze 2.00, která pochází z března 2001, byl profil SCSUG SCPP pro čipové karty ve starší verzi 2.0. Zmiňovaný profil upřesňuje požadavky na uživatelské tokeny, které slouží pro bezpečné uložení šifrovacích klíčů uživatele. Profil definuje požadavky na technické i programové vybavení a je určen pro podporu symetrických i asymetrických krypto-systémů.

V tomto profilu se zásada P.Key_Length odkazuje na směrnici, která upřesňuje použití certifikátů X.509 v prostředí amerického ministerstva obrany. Na jejím základě jsou v profilu stanoveny konkrétní délky klíčů a to dokonce pro více algoritmů (např. pro RSA 2048 bitů, pro DSA 1024 bitů resp. pro eliptický systém 384 bitů). Na základě této organizační zásady je stanoven cíl O.Crypt, který je dále rozpracován při formulaci požadavků třídy FCS.

[4] Míra záruk EAL–CSPP byla připravena pro kvalitní komerční produkty a odpovídá zárukám EAL3, u kterých byly vypuštěny požadavky na popisného vyjádření návrhu na vysoké úrovni abstrakce.

Vazba na resortní předpis dovoluje velmi konkrétní formulaci požadavků včetně různých úrovní FIPS 140-1 pro odlišné moduly systému (Level 2 pro uživatele a Level 3 pro certifikační a registrační autority). Vysoká konkrétnost profilu se odráží i v příloze E, kde je uveden seznam schválených kryptografických algoritmů a požadované délky klíčů.

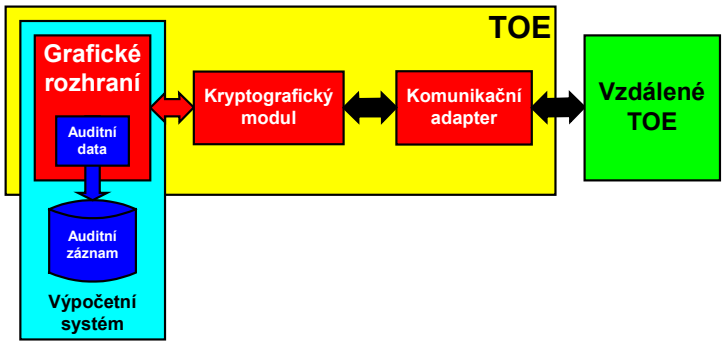
1.1.2 Profil bezpečnosti adresářových služeb

Profil **Directory for US Department of Defense Class 4 PKI Protection Profile** ve verzi 0.2 z listopadu 2000 je formuluje bezpečnostní požadavky spojené s adresářovými službami a s možnostmi vzájemného propojení více systémů, které jsou na infrastruktuře PKI závislé. Profil popisuje bezpečnostní nároky na bázi adresářových informací (Directory Information Base – DIB), které obsahuje údaje o všech prvcích řízeného komunikačního systému. Krom toho profil obsahuje i požadavky na bezpečné sdílení uložených údajů a na systém správy a řízení adresářových služeb. Míra záruk je dána úrovní EAL3.

Zvláštností profilu je, že kryptografické požadavky jsou zavedeny použitím předpokladu A.Crypto. Ten předpokládá nasazení pouze kryptografických modulů, které odpovídají FIPS 140-1 Level 3. Daný předpoklad se pak přímo odráží v cíli O.CryptoFunction, který je následně pokryt náležitými požadavky třídy FCS. Použitý předpokladu nebývá příliš obvyklé, nicméně je též jednou z možností zapracování požadavků kladených na aplikování kryptografie.

4.2 Profily pro vzdálený přístup

Profil s názvem **Cryptographic Communications System Protection Profile** formuluje bezpečnostní požadavky na vysoce spolehlivé in-line šifrátory, které dovolují bezpečné připojení vzdálených uživatelů do lokálních sítí či samostatných domén prostřednictvím běžných telekomunikačních sítí. Profil se vyznačuje extrémně vysokými požadavky na záruky, protože výrobce musí respektovat míru záruk EAL5+.



Obrázek 6 Uspořádání TOE profilu a jeho vazby

Uspořádání TOE počítá s existencí třech základních prvků, kterými jsou kryptografický modul, komunikační adapter a grafické rozhraní. Kryptografický modul je jádrem celého systému a provádí vlastní šifrování všech přenosů. Nicméně podrobnější kryptografické požadavky nejsou v profilu uváděny a musí být stanoveny až ve specifikaci bezpečnosti konkrétního produktu.

Další prvky TOE je komunikační adapter, který zajišťuje připojení systému do datové sítě, a grafické rozhraní, které je určeno pro bezpečnou komunikaci s uživateli, pomocí které je kryptografický modul nastavován. Modul grafické rozhraní je též odpovědný za řízení přístupu běžných uživatelů a za generování auditních záznamů. Ty jsou ale ukládány mimo TOE na systém, kde je TOE implementováno. Celá struktura je vidět na obrázku 6.

Tento profil je odvozen od dvou dalších profilů, které specifikují nároky na bezpečnost vzdáleného přístupu prostřednictvím telekomunikačních sítě. Oba profily jsou velmi podobné a odlišnosti jsou dány pouze vyšší mírou záruk u profilu HARA PP. Z kryptografického hlediska se oba profily liší nasazením dvou různých algoritmů.

Jméno profilu	Označení	Verze PP	CC	EAL	Datum
Cryptographic Communications System (CCS) Protection Profile	CCS PP	1.06	2.1	EAL5+	listopad 2000
U.S. DoD Remote Access Protection Profile for High Assurance Environments	HARA PP	1.0	2.1	EAL5	červen 2000
U.S. DoD Remote Access Protection Profile for SBU-High Environments		0.9	2.1	EAL2+	květen 2000

4.3 Profily pro VPN

Profily bezpečnosti pro **virtuální privátní sítě** (Virtual Private Network – VPN) definují požadavky na bezpečné propojení, které sdílí společné páteřní spoje. Profily dovolují použití bezpečného propojení na úrovni site–to–site, LAN–to–LAN, host–to–host, resp. jakékoli jejich kombinace. Profily současně rozlišují dva typy uživatelů, kterými jsou místní a vzdálení uživatelé VPN.

Součástí profilů je popis několika bezpečnostních hrozeb (např. T.MASQUERADE_BYPASS, T.MASQUERADE_HIJACK, T.CRYPTOANALYTIC), kterým TOE čelí několika bezpečnostními cíli (např. O.CONFIDENTIALITY). Cíle jsou následně pokryty požadavky na zavedení kryptografických funkcí, které jsou velmi konkrétně vymezeny (předepsány jsou algoritmy i délky klíčů). Díky tomu jsou kryptografické požadavky vázány přímo na hrozby, které v prostředí působí.

Nicméně nejnovější profil pro VPN se snaží použití hrozeb jako základního východiska omezit, a proto jsou vcelku jednoznačné požadavky silněji podloženy taktéž několika organizačními zásadami (např. P.CRYPTO, P.INTEGRITY).

Jméno profilu	Označení	Verze PP	CC	EAL	Datum
U.S. DoD Virtual Private Network (VPN) Boundary Gateway Protection Profile for Basic Robustness Environments		0.6	2.1	EAL2	září 2001
A Goal Virtual Private Network Protection Profile For Protecting Sensitive Information		2.0	2.0	EAL3+	červenec 2000
Virtual Private Network Protection Profile For Protecting Sensitive Information		1.0	2.0	EAL3+	únor 2000

4.4 Další profily bezpečnosti

Součástí amerického konceptu je řada dalších profilů bezpečnosti, které též obsahují požadavky spojené s aplikováním kryptografických technik. Formulace požadavků bývá velmi odlišná a většinou je podřízena praktickým potřebám konkrétního profilu. Například **profilu bezpečnosti pro elektronickou poštu** vyžaduje realizaci v souladu se standardem S/MIME verze 3. Naproti tomu **profil bezpečnosti mobilních kódů** si nárokuje standard X.509 verze 3 s délkou RSA/DSA klíče 512 bitů a vyšší. Novější profily se pak většinou přesnějšímu vymezení kryptografických požadavků vyhýbají a prostor je tak přenechán výrobců, kteří musí tyto záležitosti zpřesnit při tvorbě specifikace bezpečnosti.

5 Závěr

Společná kritéria jsou složitým souborem požadavků na bezpečnostní funkce, který samozřejmě zahrnuje i kryptografické funkce. Použití rozsáhlého katalogu usnadňují profily bezpečnosti, které se snaží zobecnit bezpečnostní rysy typických případů nasazení. Díky tomu se právě profily stávají cenným zdrojem, který zpřístupňuje Společná kritéria širší odborné veřejnosti. Rozšíření obecného povědomí o užitečnosti Společných kritérií je cílem i tohoto příspěvku.

6 Literatura

[1] Information technology – Security techniques – Evaluation criteria for IT security, ISO/IEC 15408:1999, ISO/IEC 1999.

[2] Information technology – Security techniques – Guide for the production of protection profiles and security targets, ISO/IEC PDTR 15446:2000, ISO/IEC 2000.

[3] Information Assurance Technical Framework, release 3.0, IATF Forum, NSA 2000.

6.1 WWW odkazy

http://www.commoncriteria.org/
http://www.iatf.net/protection_profiles/profiles.cfm
http://csrc.nist.gov/cc/pp/pplist.htm
http://www.radium.ncsc.mil/tpep/library/protection_profiles/index.html
http://www.itsec.gov.uk/docs/protect.htm
http://www.scssi.gouv.fr/fr/confiance/pp.html
http://www.bsi.de/cc/pplist.htm

6.2 Použité zkratky

BSI	Bundesamt für Sicherheit in der Informationstechnik
CC	Common Criteria
CEN/ISSS	European Committee for Standardization, Information Society Standardization System
CESG	Communications-Electronics Security Group
CRL	Certificate Revocation List
EESSI	European Electronic Signature Standardisation Initiative
FIPS	Federal Information Processing Standard
IATF	Information Assurance Technical Framework
IATFF	Information Assurance Technical Framework Forum
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
PKI	Public Key Infrastructure
PP	Protection Profile
SCSSI	Service Central de la Sécurité des Systèmes d'Information
ST	Security Target
TCSEC	Trusted Computer System Evaluation Criteria
TOE	Target of Evaluation

7 Přílohy

7.1 Přehled úrovní záruk

EAL1	**funkčně testováno** (Functionally Tested) – je nejnižší úrovní záruk a jejím cílem je poskytnutí jisté míry důvěry bez složitějšího rozboru bezpečnostních rizik. Záruky se opírají o upřesnění funkční specifikace, vymezení rozhraní a zpracování bezpečnostní dokumentace.	**Komerční metody vývoje**
EAL2	**strukturovaně testováno** (Structurally Tested) – nad rámec AEL1 zpřísňuje požadavky především na nezávislé testování. Vývoj je zároveň nutné rozšířit o neformální popis architektury a ošetření běžně známých útoků.	
EAL3	**metodicky testováno a kontrolováno** (Methodically Tested and Checked) – dovoluje svědomitým tvůrcům uplatnit maximální záruky, které vycházejí z osvědčených přístupů k vývojovému procesu bez podstatného navýšení náročnosti. Na rozdíl od nižších tříd EAL3 požaduje ucelenější testování bezpečnostních funkcí a mechanismů a uplatňuje postupy, které vytváří základní předpoklady k tomu, aby nedocházelo ke kompromitaci TOE během vývoje. Tato úroveň je doporučena pro střední úroveň nezávisle ověřené bezpečnosti.	
EAL4	**metodicky navrženo, testováno a kontrolováno** (Methodically Designed, Tested and Checked) – je založena na velmi kvalitních praktikách vývoje, které jsou vysoce spolehlivé, ale nevyžadují rozsáhlejší zapojení specifických znalostí či zdrojů. Tímto se AEL4 stává nejnáročnější úrovní, která ještě zůstává komerčně únosná. Toho je docíleno hlubším popisem návrhu a doložením odolnosti proti útokům s omezenými zdroji.	
EAL5	**poloformálně navrženo a testováno** (Semiformally Designed and Tested) – je první úrovní, která vyžaduje zapojení specializovaných metod vývoje. Záruky se opírají o existenci formálního modelu, který je doplněn poloformálním vyjádřením celkového návrhu. Tato úroveň vyžaduje strukturovaný návrh a základní analýzu skrytých kanálů. Produkty tak odolávají útokům, při kterých jsou použity zdroje střední výkonnosti.	**Specializované metody vývoje**
EAL6	**poloformálně ověřený návrh a testováno** (Semiformally Verified Design and Tested) – vychází z modulárního a vrstveného návrhu a výsledný produkt musí být vysoce odolný vůči útokům. Celý vývoj musí probíhat v přísně řízeném prostředí.	
EAL7	**formálně ověřený návrh a testováno** (Formally Verified Design and Tested) – je nejnáročnější a vychází z plně formálního návrhu. Současně dochází i k cílenému snížení složitosti návrhu. To znamená, že vývoj je spojen s neúměrně vysokými náklady a praktické použití této úrovně je velmi omezené.	

7.2 Typické hrozby spojené s kryptografickými aktivy

Označení	**Hrozba**
T.EMI	Kryptograficky důležitá aktiva TOE mohou být prozrazena neautorizovaným osobám či uživatelům formou elektromagnetického vyzařování.
T.IMPERSON	Útočník může předstírat identitu oprávněného uživatele TOE.
T.ERROR	Oprávněný uživatel či neautorizovaná osoba mohou do TOE zavléci chybu, která povede k prozrazení důležitých aktiv.
T.MODIFY	Integrity informací může být poškozena neautorizovanou modifikací nebo zničením informací.
T.ATTACK	Neodhalené kompromitování kryptografických aktiv muže být způsobeno tím, že se útočník pokusí provést činnosti, pro které nebyl autorizován.
T.ABUSE	Neodhalené kompromitování kryptografických aktiv muže být způsobeno tím, že autorizovaný uživatel TOE provede činnosti, pro které byl autorizován.
T.MAL	Kryptografická aktiva mohou být modifikována nebo prozrazena díky selhání TOE.
T.PHYSICAL	Bezpečnostně důležité části TOE mohou být cílem fyzického útoku, který poškodí jejich bezpečnost.

7.3 Příklady bezpečnostních cílů TOE

Označení	Bezpečnostní cíl
O.I&A	Před vlastním použitím musí TOE každého uživatele identifikovat a deklarovaná identita musí autentizována.
O.DAC	TOE musí poskytovat nástroje na řízení a omezení přístupu k objektům a zdrojům, za které TOE odpovídá. Nástroje musí být schopny prosadit příslušná bezpečnostní pravidla.
O.PHP	TOE se musí samo chránit před neautorizovanými fyzickými útoky, modifikací či zneužitím.
O.INTEGRITY	TOE musí obsahovat nástroje, které odhalí ztrátu integrity.
O.FAILSAFE	V případě výskytu chyby musí být bezpečný stav TOE zachován.
O.ADMIN	TOE musí obsahovat funkce, které dovolí jeho efektivní správu, kterou provádí pouze autorizovaní správci.
O.EMI	Musí existovat procesní a fyzická opatření, které omezí možnosti neautorizovaného prozrazení způsobené elektromagnetickým vyzařováním.
O.PHYSICAL	Kritické části TOE musí být chráněny před fyzickými útoky, které by mohly ohrozit jejich bezpečnost.

7.4 Příklad zdůvodnění oprávněnosti cílů

Hrozba	Cíle	Zdůvodnění oprávněnosti
T.EMI	O.EMI	Vhodná opatření mohou snížit riziko prozrazení kryptograficky důležitých aktiv způsobené vyzařováním.
T.IMPERSON	O.I&A	Identifikace a autentizace uživatelů snižuje riziko spojené s předstíráním identity.
T.ERROR	O.FAILSAFE	Požadavek na zachování bezpečného stavu snižuje pravděpodobnost prozrazení nebo modifikace důležitých kryptografických aktiv v důsledku chyby.
T.MODIFY	O.INTEGRITY	Schopnost odhalení ztráty integrity snižuje šance úspěšné změny aktiva.
	O.ADMIN	Správná konfigurace a administrace snižuje riziko neoprávněné modifikace.
T.ATTACK	O.I&A	Identifikace a autentizace snižuje možnost neautorizovaného přístupu.
	O.DAC	Řízení přístupu v souladu se zásadami snižuje riziko provedení nežádoucích činností.
T.ABUSE	O.DAC	Řízení přístupu v souladu se zásadami snižuje riziko provedení nežádoucích činností.
T.MAL	O.INTEGRITY	Schopnost odhalení ztráty integrity zvyšuje pravděpodobnost zjištění závady.
	O.FAILSAFE	Požadavek na zachování bezpečného stavu snižuje pravděpodobnost prozrazení nebo modifikace důležitých kryptografických aktiv v důsledku selhání.
T.PHYSICAL	O.PHP	Ochrana před fyzickým útokem snižuje riziko fyzického útoku.
	O.PHYSICAL	Omezení fyzického přístupu na autorizované osoby snižuje riziko fyzického útoku.