

ČESKÁ TECHNICKÁ NORMA

ICS 35.040 **Duben 2010**

**Informační technologie - Bezpečnostní techniky - Kritéria pro
hodnocení bezpečnosti IT -
Část 3: Komponenty bezpečnostních záruk**

**ČSN
ISO/IEC 15408-3
36 9789**

Information technology - Security techniques - Evaluation criteria for IT security -
Part 3: Security assurance components

Technologies de l'information - Techniques de sécurité - Criteres d'évaluation pour la sécurité TI -
Partie 3: Composants d'assurance de sécurité

Informationstechnik - IT-Sicherheitsverfahren - Evaluationskriterien für IT-Sicherheit -
Teil 3: Anforderungen an die Vertrauenswürdigkeit

Tato norma je českou verzí mezinárodní normy ISO/IEC 15408-3:2008. Překlad byl zajištěn Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví. Má stejný status jako oficiální verze.

This standard is the Czech version of the International Standard ISO/IEC 15408-3:2008. It was translated by Czech Office for Standards, Metrology and Testing. It has the same status as the official version.

Nahrazení předchozích norem

Touto normou se nahrazuje ČSN ISO/IEC 15408-3 (36 9789) z listopadu 2002.

Národní předmluva

Změny proti předchozím normám

Tato norma představuje technickou revizi předchozí normy ČSN ISO/IEC 15408-3 z roku 2002. Vydání ISO/IEC 15408:2005 nebylo do soustavy českých norem zavedeno.

Informace o citovaných normativních dokumentech

ISO/IEC 15408-1 dosud nezavedena

ISO/IEC 15408-2 zavedena v ČSN ISO/IEC 15408-2 (36 9789) Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT - Část 2: Bezpečnostní funkční požadavky

Národní poznámka

Malé písmeno „s“ u anglické zkratky vyjadřuje její množné číslo, například: SFRs, TSFs, apod.

Anglický termín symbol se překládá českým slovem symbol, protože se zde používá ve významu nadřazeného termínu vůči podřazeným termínům: značky, znaky, označení atd., aby se všechny tyto termíny nemusely vypisovat.

Vypracování normy

Zpracovatel: Ing. Vladimír Pračke, IČ 40654419

Technická normalizační komise: TNK 20 Informační technologie

Pracovník Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví: Ing. Petr Wallenfels

MEZINÁRODNÍ NORMA

Informační technologie – Bezpečnostní techniky – ISO/IEC 15408-3

Kritéria pro hodnocení bezpečnosti IT – Třetí vydání

Část 3: Komponenty bezpečnostních záruk 2008-08

ICS 35.040

Obsah

Strana

Předmluva 11

Úvod 12

1 Předmět normy 12

2 Citované normativní dokumenty 12

3 Termíny a definice, symboly a zkrácené termíny 12

4 Přehled 12

4.1 Organizace této části ISO/IEC 15408 12

5 Paradigma záruky 13

5.1 Filosofie ISO/IEC 15408 13

5.2 Koncepce záruky 13

5.2.1 Významnost zranitelností 13

5.2.2 Příčiny zranitelností 14

5.2.3 Záruka ISO/IEC 15408 14

5.2.4 Záruka prostřednictvím hodnocení 14

5.3 Stupnice hodnocení záruky podle ISO/IEC 15408 14

6 Komponenty bezpečnostní záruky 14

6.1 Třídy, rodiny a struktura komponent bezpečnostní záruky 14

6.1.1 Struktura třídy záruky 14

6.1.2 Struktura rodiny záruky 16

6.1.3 Struktura komponenty záruky 16

6.1.4 Prvky záruky 18

6.1.5 Taxonomie komponenty 18

6.2 Struktura EAL 18

6.2.1 Název EAL 19

6.2.2 Cíle 19

6.2.3 Poznámky k aplikaci 19

6.2.4 Komponenty záruky 19

6.2.5 Vzájemný vztah mezi zárukami a úrovněmi záruk 19

6.3 Struktura CAP 20

6.3.1 Název CAP 21

6.3.2 Cíle 21

6.3.3 Poznámky k aplikaci 21

6.3.4 Komponenty záruky 21

6.3.5 Vztah mezi zárukami a balíky záruky 22

Strana

7 Úrovně hodnocení záruky 23

7.1 Úrovně hodnocení záruky (EAL) - přehled 23

7.2 Podrobnosti úrovně hodnocení záruky 24

7.3 Úroveň hodnocení záruky 1 (EAL1) - funkčně testováno 24

7.3.1 Cíle 24

7.3.2 Komponenty záruky 24

7.4 Úroveň hodnocení záruky 2 (EAL2) - strukturovaně testováno 25

7.4.1 Cíle 25

7.4.2 Komponenty záruky 25

7.5 Úroveň hodnocení záruky 3 (EAL3) – metodicky testováno a kontrolováno 26

7.5.1 Cíle 26

7.5.2 Komponenty záruky 26

7.6 Úroveň hodnocení záruky 4 (EAL4) – metodicky navrženo, testováno a zhodnoceno 27

7.6.1 Cíle 27

7.6.2 Komponenty záruky 27

7.7 Úroveň hodnocení záruky 5 (EAL5) – poloformálně navrženo a testováno 28

7.7.1 Cíle 28

7.7.2 Komponenty záruky 28

7.8 Úroveň hodnocení záruky 6 (EAL6) – poloformálně ověřený návrh a testováno 29

7.8.1 Cíle 29

7.8.2 Komponenty záruky 30

7.9 Úroveň hodnocení záruky 7 (EAL7) – formálně ověřený návrh a testováno 31

7.9.1 Cíle 31

7.9.2 Komponenty záruky 31

8 Balíky sestavené záruky 32

8.1 Balíky sestavené záruky – přehled 32

8.2 Balíky sestavené záruky – podrobnosti 33

8.3 Úroveň sestavené záruky A (CAP-A) – strukturovaně sestavená 33

8.3.1 Cíle 33

8.3.2 Komponenty záruky 33

8.4 Úroveň sestavené záruky B (CAP-B) – metodicky sestaveno 34

8.4.1 Cíle 34

8.4.2 Komponenty záruky 34

8.5 Úroveň sestavené záruky C (CAP-C) – metodicky sestaveno, testováno a zhodnoceno 35

8.5.1 Cíle 35

8.5.2 Komponenty záruky 35

9 Třída APE: Hodnocení profilu ochrany 36

9.1 Zavedení PP (APE_INT) 37

9.1.1 Cíle 37

9.1.2 APE_INT.1 Zavedení PP 37

9.2 Prohlášení o shodě (APE_CCL) 37

9.2.1 Cíle 37

9.2.2 APE_CCL.1 Prohlášení o shodě 37

Strana

9.3 Definice problému bezpečnosti (APE_SPD) 38

9.3.1 Cíle 38

9.3.2 APE_SPD.1 Definice problému bezpečnosti 39

9.4 Bezpečnostní cíle (APE_OBJ) 39

9.4.1 Cíle 39

9.4.2 Řazení komponent do úrovní 39

9.4.3 APE_OBJ.1 Bezpečnostní cíle pro provozní prostředí 39

9.4.4 APE_OBJ.2 Bezpečnostní cíle 40

9.5 Definice rozšířených komponent (APE_ECD) 40

9.5.1 Cíle 40

9.5.2 APE_ECD.1 Definice rozšířených komponent 41

9.6 Požadavky na bezpečnost (APE_REQ) 41

9.6.1 Cíle 41

9.6.2 Řazení komponent do úrovní 41

9.6.3 APE_REQ.1 Uvedené požadavky na bezpečnost 42

9.6.4 APE_REQ.2 Odvozené požadavky na bezpečnost 42

10 Třída ASE: Hodnocení bezpečnostního cíle 43

10.1 Zavedení ST (ASE_INT) 44

10.1.1 Cíle 44

10.1.2 ASE_INT.1 Zavedení ST	44
10.2 Prohlášení o shodě (ASE_CCL)	45
10.2.1 Cíle	45
10.2.2 ASE_CCL.1 Prohlášení o shodě	45
10.3 Definice problému bezpečnosti (ASE_SPD)	46
10.3.1 Cíle	46
10.3.2 ASE_SPD.1 Definice problému bezpečnosti	46
10.4 Bezpečnostní cíle (ASE_OBJ)	47
10.4.1 Cíle	47
10.4.2 Řazení komponent do úrovní	47
10.4.3 ASE_OBJ.1 Bezpečnostní cíle pro provozní prostředí	47
10.4.4 ASE_OBJ.2 Bezpečnostní cíle	47
10.5 Definice rozšířených komponent (ASE_ECD)	48
10.5.1 Cíle	48
10.5.2 ASE_ECD.1 Definice rozšířených komponent	48
10.6 Požadavky na bezpečnost (ASE_REQ)	49
10.6.1 Cíle	49
10.6.2 Řazení komponent do úrovní	49
10.6.3 ASE_REQ.1 Uvedené požadavky na bezpečnost	49
10.6.4 ASE_REQ.2 Odvozené požadavky na bezpečnost	50
10.7 Souhrnná specifikace TOE (ASE_TSS)	51
10.7.1 Cíle	51
10.7.2 Řazení komponent do úrovní	51
10.7.3 ASE_TSS.1 Souhrnná specifikace TOE	51
10.7.4 ASE_TSS.2 Souhrnná specifikace TOE se souhrnným architektonickým návrhem	52
11 Třída ADV: Vývoj	52
11.1 Architektura bezpečnosti (ADV_ARC)	56

11.1.1 Cíle 56

11.1.2 Řazení komponent do úrovně 56

11.1.3 Poznámky k aplikaci 56

11.1.4 ADV_ARC.1 Popis bezpečnostní architektury 57

11.2 Funkční specifikace (ADV_FSP) 57

11.2.1 Cíle 57

11.2.2 Řazení komponent do úrovně 58

11.2.3 Poznámky k aplikaci 58

11.2.4 ADV_FSP.1 Základní funkční specifikace 59

11.2.5 ADV_FSP.2 Bezpečnost vynucující funkční specifikace 60

11.2.6 ADV_FSP.3 Funkční specifikace s úplným shrnutím 61

11.2.7 ADV_FSP.4 Úplná funkční specifikace 62

11.2.8 ADV_FSP.5 Úplná poloformální funkční specifikace s dodatečnými chybovými informacemi 62

11.2.9 ADV_FSP.6 Úplná poloformální funkční specifikace s dodatečnou formální specifikací 63

11.3 Zobrazení implementace (ADV_IMP) 64

11.3.1 Cíle 64

11.3.2 Řazení komponent do úrovně 65

11.3.3 Poznámky k aplikaci 65

11.3.4 ADV_IMP.1 Zobrazení implementace TSF 65

11.3.5 ADV_IMP.2 Úplné mapování zobrazení implementace TSF 66

11.4 Vnitřní struktura TSF (ADV_INT) 66

11.4.1 Cíle 66

11.4.2 Řazení komponent do úrovně 67

11.4.3 Poznámky k aplikaci 67

11.4.4 ADV_INT.1 Správně strukturovaná podmnožina vnitřního uspořádání TSF 67

11.4.5 ADV_INT.2 Správně strukturované vnitřní uspořádání 68

11.4.6 ADV_INT.3 Minimálně složité vnitřní uspořádání 69

11.5	Modelování bezpečnostní politiky (ADV_SPM)	69
11.5.1	Cíle	69
11.5.2	Řazení komponent do úrovně	69
11.5.3	Poznámky k aplikaci	69
11.5.4	ADV_SPM.1 Formální model bezpečnostní politiky TOE	70
11.6	Návrh TOE (ADV_TDS)	71
11.6.1	Cíle	71
11.6.2	Řazení komponent do úrovně	71
11.6.3	Poznámky k aplikaci	71
11.6.4	ADV_TDS.1 Základní návrh	72
11.6.5	ADV_TDS.2 Řešení architektury	73
11.6.6	ADV_TDS.3 Základní modulární návrh	74
11.6.7	ADV_TDS.4 Poloformální modulární projekt	75
11.6.8	ADV_TDS.5 Úplný poloformální modulární projekt	76
11.6.9	ADV_TDS.6 Úplný poloformální modulární projekt s formální prezentací projektu na vysoké úrovni	77
12	Třída AGD: Průvodní dokumentace	78
12.1	Provozní uživatelská příručka (AGD_OPE)	79
12.1.1	Cíle	79
12.1.2	Řazení komponent do úrovně	79
12.1.3	Poznámky k aplikaci	79
12.1.4	AGD_OPE.1 Provozní uživatelská příručka	79
12.2	Přípravné postupy (AGD_PRE)	80
12.2.1	Cíle	80
12.2.2	Řazení komponent do úrovně	80
12.2.3	Poznámky k aplikaci	80
12.2.4	AGD_PRE.1 Přípravné postupy	81

13	Třída ALC: Podpora životního cyklu	81
13.1	Schopnosti CM (ALC_CMC)	82
13.1.1	Cíle	82
13.1.2	Rozdělení komponent do úrovní	88
13.1.3	Poznámky k aplikaci	82
13.1.4	ALC_CMC.1 Označení TOE	83
13.1.5	ALC_CMC.2 Použití CM systému	83
13.1.6	ALC_CMC.3 Kontroly autorizace	84
13.1.7	ALC_CMC.4 Podpora produkce, procedury převzetí a automatizace	85
13.1.8	ALC_CMC.5 Zdokonalená podpora	87
13.2	Předmět CM (ALC_CMS)	89
13.2.2	Rozdělení komponent do úrovní	89
13.2.5	ALC_CMS.2 Části TOE CM Pokrytí	90
13.2.6	ALC_CMS.3 Zobrazení implementace pokrytí CM	90
13.2.7	ALC_CMS.4 Otázka sledování CM pokrytí	91
13.2.8	ALC_CMS.5 Vývojové nástroje pro CM pokrytí	92
13.3	Dodání (ALC_DEL)	93
13.3.1	Cíle	93
13.4	Bezpečnost vývoje (ALC_DVS)	94
13.4.1	Cíle	94
13.4.2	Rozdělení komponent do úrovní	94
13.4.3	Poznámky k aplikaci	94
13.4.5	ALC_DVS.2Dostatečnost bezpečnostních opatření	94
13.5	Náprava závad (ALC_FLR)	95
13.5.1	Cíle	95
13.5.2	Rozdělení komponent do úrovní	95
13.5.3	Poznámky k aplikaci	95
13.5.4	ALC_FLR.1 Základní nápravy závad	96

13.5.5	ALC_FLR.2	Procedury pro ohlašování závad	96
13.5.6	ALC_FLR.3	Systematická náprava závad	97
13.6		Definice životního cyklu (ALC_LCD)	99
13.6.1		Cíle	99
13.6.2		Rozdělení komponent do úrovní	99
13.6.3		Poznámky k aplikaci	99
13.6.4	ALC_LCD.1.1D	Vývojovým pracovníkem definovaný model životního cyklu	99
13.6.5	ALC_LCD.2	Měřitelný model životního cyklu	100
13.7		Nástroje a techniky (ALC_TAT)	100
13.7.1		Cíle	102
13.7.2		Rozdělení komponent do úrovní	101
13.7.3		Poznámky k aplikaci	101
13.7.5	ALC_TAT.2	Shoda s implementačními normami	101
13.7.6	ALC_TAT.3	Shoda s implementačními normami – všechny části	102
14		Třída ATE: Testy	103
14.1		Pokrytí (ATE-COV)	103
14.1.1		Cíle	103
14.1.2		Rozdělení komponent do úrovní	103
14.1.3		Poznámky k aplikaci	104
14.1.4	ATE_COV.1	Důkaz pokrytí	104
14.1.5	ATE_COV2	Analýza pokrytí	104
14.1.6	ATE_COV.3	Důsledná analýza pokrytí	105
14.2		Hloubka (ATE_DPT)	105
14.2.1		Cíle	105
14.2.2		Rozdělení komponent do úrovní	106
14.2.3		Poznámky k aplikaci	106
14.2.4	ATE_DPT.1	Testování: základní návrh	106

14.2.5	ATE_DPT.2 Testování: moduly vynucení bezpečnosti	106
14.2.6	ATE_DPT.3 Testování: modulární návrh	107
14.2.7	ATE_DPT.4 Testování: zobrazení implementace	108
14.3	Funkční testy (ATE_FUN)	108
14.3.1	Cíle	108
14.3.2	Rozdělení komponent do úrovní.	108
14.3.4	ATE_FUN.1 Funkční testování	109
14.3.5	ATE_FUN.2 Uspořádané funkční testování	109
14.4	Nezávislé testování (ATE_IND)	110
14.4.1	Cíle	110
14.4.2	Rozdělení komponent do úrovní	110
14.4.3	Poznámky k aplikaci	110
14.4.5	ATE_IND.2 Nezávislé testování - vzorek	112
14.4.6	ATE_IND.3 Nezávislé testování - kompletní	113
15	Třída AVA: Posouzení zranitelnosti	113
15.1	Poznámky k aplikaci	114
15.2	Analýza zranitelností (AVA_VAN)	114
15.2.1	Cíle	114
15.2.2	Rozdělení komponent do úrovní	114
15.2.3	AVA_VAN.1 Přehled zranitelností	114
15.2.4	AVA_VAN.2 Analýza zranitelnosti	115
15.2.5	AVA_VAN.3 Cílená analýza zranitelnosti	116
15.2.6	AVA_VAN.4 Systematická analýza zranitelnosti	116
15.2.7	AVA_VAN.5 Rozšířená systematická analýza zranitelnosti	117
16	Třída ACO: Sestavení	118
16.1	Logický základ sestavení (ACO_COR)	120
16.1.1	Cíle	120
16.1.2	Rozdělení komponent do úrovní	120

16.1.3 ACO_COR.1 Logický základ sestavení 121

Strana

16.2 Důkaz vývoje (ACO_DEV) 121

16.2.1 Cíle 121

16.2.2 Rozdělení komponent do úrovní 121

16.2.3 Poznámky k aplikaci 121

16.2.4 ACO_DEV.1 Funkční popis 122

16.2.5 ACO_DEV.2 Základní průkazná fakta návrhu 122

16.2.6 ACO_DEV.3 Podrobná průkazná fakta návrhu 123

16.3 Spolehlivost závislé komponenty (ACO_REL) 124

16.3.1 Cíle 124

16.3.3 Poznámky k aplikaci 124

16.3.4 ACO_REL.1 Základní informace o spolehlivosti 124

16.3.5 ACO_REL.2 Informace o spolehlivosti 124

16.4 Testování sestaveného TOE (ACO_CTT) 125

16.4.1 Cíle 125

16.4.2 Rozdělení komponent do úrovní 125

16.4.3 Poznámky k aplikaci 125

16.4.4 ACO_CTT.1 Testování rozhraní 126

16.4.5 ACO_CTT.2 Přesné testování rozhraní 127

16.5 Analýza zranitelnosti sestavení 128

16.5.1 Cíle 128

16.5.2 Rozdělení komponent do úrovní 128

16.5.3 Poznámky k aplikaci 128

16.5.4 ACO_VUL.1 Revize zranitelnosti sestavení 128

16.5.6 ACO_VUL.3 Rozšířená-základní analýza zranitelností sestavení 129

Příloha A (informativní) Vývoj (ADV) 131

A.1 ADV_ARC: Doplnující materiál k bezpečnostní architektuře 131

A.1.1	Vlastnosti bezpečnostní architektury	131
A.1.2	Popis bezpečnostní architektury	131
A.2	ADV_FSP: Doplnující materiál pro TSFIs	133
A.2.1	Určování TSFI	133
A.3	ADV_INT: Doplnkový materiál pro vnitřní části TSF	137
A.3.1	Struktura procedurálního software	137
A.3.1.1	Provázanost	138
A.3.1.2	Propojení	138
A.4	ADV_TDS: Subsystémy a moduly	139
A.5	Doplnkový materiál pro formální metody	142
Příloha B	(informativní) Sestavení (ACO)	144
B.1	Nezbytnost hodnocení sestaveného TOE	144
B.2	Provádění hodnocení bezpečnostního cíle pro sestavené TOE	145
B.3	Interakce mezi sestavenými entitami IT	145
Příloha C	(informativní) Křížové odkazy závislostí komponent záruky	150
Příloha D	(informativní) Křížové odkazy PP a komponenty záruky	154
Příloha E	(informativní) Křížové odkazy EAL a komponent záruky	155
Příloha F	(informativní) Křížové odkazy CAP a komponent záruky	156

Odmítnutí odpovědnosti za manipulaci s PDF souborem

Tento soubor PDF může obsahovat vložené typy písma. V souladu s licenční politikou Adobe lze tento soubor tisknout nebo prohlížet, ale nesmí být editován, pokud nejsou typy písma, které jsou vloženy, používány na základě licence a instalovány v počítači, na němž se editace provádí. Při stažení tohoto souboru přejímají jeho uživatelé odpovědnost za to, že nebude porušena licenční politika Adobe. Ústřední sekretariát ISO nepřijímá za její porušení žádnou odpovědnost. Adobe je obchodní značka „Adobe Systems Incorporated“.

Podrobnosti o softwarových produktech použitých k vytvoření tohoto souboru PDF lze najít ve Všeobecných informacích, které se vztahují k souboru; parametry, pomocí kterých byl PDF soubor vytvořen, byly optimalizovány pro tisk. Soubor byl zpracován s maximální péčí tak, aby ho členské organizace ISO mohly používat. V málo pravděpodobném případě, například když vznikne problém, který se týká souboru, informujte o tom Ústřední sekretariát ISO na níže uvedené adrese.



DOKUMENT CHRÁNĚNÝ COPYRIGHTEM

© ISO/IEC 2008

Veškerá práva vyhrazena. Pokud není specifikováno jinak, nesmí být žádná část této publikace reprodukována nebo používána v jakémkoliv formě nebo jakýmkoliv způsobem, elektronickým nebo mechanickým, včetně fotokopíí a mikrofilmů, bez písemného svolení buď od organizace ISO na níže uvedené adrese nebo od členské organizace ISO v zemi žadatele.

ISO copyright office

Case postale 56 · CH-1211 Geneva 20

Tel. + 41 22 749 01 11

Fax + 41 22 749 09 47

Předmluva

ISO (Mezinárodní organizace pro normalizaci) a IEC (Mezinárodní elektrotechnická komise) tvoří specializovaný systém světové normalizace. Národní orgány, které jsou členy ISO a IEC, se podílejí na vývoji mezinárodních norem prostřednictvím technických komisí, zřízených příslušnou organizací a zabývajících se určitou oblastí technické činnosti. Technické komise ISO a IEC spolupracují v oblastech společných zájmů. Práce se zúčastňují i další mezinárodní organizace, vládní i nevládní, s nimiž ISO a IEC navázalo pracovní styk. ISO a IEC ustavily v oblasti informačních technologií společnou technickou komisi, ISO/IEC JTC 1.

Mezinárodní normy jsou navrhovány v souladu s pravidly uvedenými v části 2 Směrnic ISO/IEC.

Hlavním úkolem společné technické komise je příprava mezinárodních norem. Návrhy mezinárodních norem, přijaté společnou technickou komisí, se rozesílají národním orgánům k hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75 % z hlasujících národních orgánů.

Pozornost je nutno věnovat možnosti, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO a IEC nelze považovat za odpovědné za identifikování některých nebo všech takových patentových práv.

ISO/IEC 15408-3 byla připravena společnou technickou komisí ISO/IEC JTC 1, *Informační technologie*, subkomise SC27, *Bezpečnostní techniky IT*. Identický text ISO/IEC 15408-3 je zveřejněn organizacemi sponzorujícími projekt „Common Criteria“ pod názvem *Společná kritéria pro hodnocení bezpečnosti informačních technologií*. Veřejný XML zdroj obou publikací lze nalézt na <http://www.oc.ccn.cni.es/xml>.

Třetí vydání zrušuje a nahrazuje druhé vydání (ISO/IEC 15408-3:2005), které prošlo technickou revizí.

ISO/IEC 15408 se skládá z následujících částí se společným názvem *Informační technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti IT*:

- Část 1: Úvod a všeobecný model
- Část 2: Bezpečnostní funkční komponenty
- Část 3: Komponenty bezpečnostních záruk

Právní poznámka

Dále uvedené vládní organizace přispěly k vyvinutí této verze Společných kritérií pro hodnocení bezpečnosti informačních technologií. Jako společní držitelé autorských práv k dokumentu Společná kritéria pro hodnocení bezpečnosti informačních technologií, verze 3.1, části 1 až 3 (nazývané CC 3.1), tímto poskytují nevýhradní oprávnění pro ISO/IEC k používání CC 3.1 při pokračujícím vývoji/údržbě mezinárodní normy ISO/IEC 15408. Tyto vládní organizace si však ponechávají právo používat, kopírovat, šířit, překládat nebo pozměňovat CC 3.1 jak uznají za vhodné.

Government Communications Security Bureau
respectively;

Kanada Communications Security Establishment;

Francie Direction Centrale de la Sécurité des Systemes d'Information;

Německo Bundesamt für Sicherheit in der Informationstechnik;

Japonsko Information Technology Promotion Agency;

Nizozemsko Netherlands National Communications Security Agency;

Španělsko Ministerio de Administraciones Públicas and Centro Criptológico
Nacional;

Spojené království Communications-Electronic Security Group;

USA The National Security Agency and the National Institute of Standards
and Technology.

Úvod

Komponenty bezpečnostních záruk, jak jsou definovány v této části ISO/IEC 15408, jsou základem pro požadavky na bezpečnostní záruky vyjádřené v profilu ochrany (Protection Profile, PP) nebo v bezpečnostním cíli (Security Target, ST).

Tyto požadavky ustanovují standardní způsob vyjádření požadavků záruky pro předměty hodnocení (Target of evaluation, TOE). Tato část ISO/IEC 15408 katalogizuje sadu součástí záruky, rodu záruky a tříd záruky. Tato část ISO/IEC 15408 rovněž definuje kritéria hodnocení pro PP a ST a představuje úrovně záruk hodnocení, které vymezují předem definovanou stupnici ISO/IEC 15408 hodnocení záruk pro TOE, která se nazývá úrovně hodnocení záruky (Evaluation Assurance Levels, EAL).

Uživatelé této části ISO/IEC 15408 jsou spotřebitelé, vývojoví pracovníci a hodnotitelé bezpečných IT produktů. ISO/IEC 15408-1 poskytuje dodatečné informace týkající se cílových uživatelů ISO/IEC 15408 a používání ISO/IEC 15408 skupinami, které zahrnují cílové uživatele. Tyto skupiny mohou používat tuto část ISO/IEC 15408 následovně:

- a. Zákazníci, kteří používají tuto část ISO/IEC 15408 při výběru komponent pro vyjádření požadavků záruky, které splní bezpečnostní cíle vyjádřené v PP nebo ST, stanovujících požadované úrovně bezpečnostních záruk TOE.
- b. Vývojoví pracovníci, kteří reagují na aktuální nebo vnímané požadavky zákazníků na bezpečnost při vytváření TOE, se odkazují na tuto část ISO/IEC 15408 při interpretaci specifikací požadavků záruky a při určování přístupů k zárukám TOE.
- c. Hodnotitelé, kteří používají požadavky záruky definované v této části ISO/IEC 15408 jako závazný výrok kritérií pro hodnocení při určování záruky TOE a při hodnocení PP a ST.

1 Předmět normy

Tato část ISO/IEC 15408 definuje požadavky normy na záruku. Obsahuje úrovně hodnocení záruky (Evaluation Assurance Levels, EALs), které definují měřítko pro posouzení záruky TOE komponenty, sestavené balíky záruk (composed assurance packages, CAPs), které definují měřítko pro posouzení záruky sestavených TOE, jednotlivé komponenty záruky, z kterých se skládají úrovně záruky a balíky, a kritéria pro hodnocení PP a ST.

Konec náhledu - text dále pokračuje v placené verzi ČSN.