

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

Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements

Technologies de l'information - Techniques de sécurité - Critères d'évaluation pour la sécurité TI -
Partie 2: Exigences
fonctionnelles de sécurité

Informationstechnik - IT-Sicherheitsverfahren: Evaluationskriterien für IT-Sicherheit - Teil 2:
Funktionelle
Sicherheitsanforderungen

Tato norma je českou verzí mezinárodní normy ISO/IEC 15408-2:1999. Mezinárodní norma ISO/IEC 15408-2:1999 má status české technické normy.

This standard is the Czech version of the International Standard ISO/IEC 15408-2:1999. The International Standard ISO/IEC 15408-2:1999 has the status of a Czech Standard.

© Český normalizační institut,
2002

Podle zákona č. 22/1997 Sb. smějí být české technické normy rozmnožovány
a rozšiřovány jen se souhlasem Českého normalizačního institutu.

65002

Citované normy

ISO/IEC 15408-1 zavedena v ČSN ISO/IEC 15408-1 (36 9789), Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT - Část 1: Všeobecně

ISO/IEC 15408-3 zavedena v ČSN ISO/IEC 15408-3 (36 9789) Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT - Část 3: Požadavky na záruku bezpečnosti

Národní poznámka

V této normě je použit výraz *signaturní události (signature events)*. Jsou to takové události, které mají určité charakteristické znaky nebo rysy významné pro další postup. V použitém kontextu to znamená, že jejich výskyt izolovaný od zbytku aktivity systému svědčí o rušivých aktivitách.

Pro účely této normy je přeložen

- a) anglický výraz Target of Evaluation (TOE) volně jako Předmět hodnocení;
- b) anglický výraz Security Target (ST) jako Bezpečnostní cíl; jako cíl je přeložen rovněž anglický výraz Objective;
- c) anglický výraz Management jako správa nebo řízení nebo jejich kombinace.

Vypracování normy

Zpracovatel: Ing. Alena Hönigová, IČO 61470716

Technická normalizační komise: TNK 42 Výměna dat

Pracovník Českého normalizačního institutu: Ing. Petr Wallenfels

Strana 3

MEZINÁRODNÍ NORMA

Informační technologie - Bezpečnostní techniky- Kritéria
pro hodnocení bezpečnosti IT - Část 2: Bezpečnostní
funkční požadavky

ISO/IEC 15408-2
První vydání
1999-12-01

ICS 35.040

Obsah

Strana

1 Předmět
normy

1.1	Rozšíření a aktualizace funkčních požadavků.....	10
1.2	Organizace ISO/IEC 15408-2.....	10
1.3	Paradigma funkčních požadavků.....	11
2	Bezpečnostní funkční požadavky.....	16
2.1	Přehled	16
2.1.1	Struktura třídy	16
2.1.2	Struktura rodiny	16
2.1.3	Struktura komponenty	18
2.1.4	Povolené operace funkčních komponent.....	19
2.2	Katalog komponent	20
2.2.1	Zvýraznění změn komponent.....	21
3	Třída FAU: Bezpečnostní audit.....	22
3.1	Automatická odezva bezpečnostního auditu (FAU_ARP).....	23
3.2	Generování dat bezpečnostního auditu (FAU_GEN).....	24
3.3	Analýza bezpečnostního auditu (FAU_SAA).....	25

3.4	Revize bezpečnostního auditu (FAU_SAR).....	28
3.5	Výběr událostí bezpečnostního auditu (FAU_SEL).....	30
3.6	Uchování událostí bezpečnostního auditu (FAU_STG).....	31
4	Třída FCO: Komunikace	33
4.1	Nepopiratelnost původu (FCO_NRO).....	34
4.2	Nepopiratelnost přijetí (FCO_NRR).....	36
5	Třída FCS: Kryptografická podpora.....	38
5.1	Správa kryptografických klíčů (FCS_CKM).....	39
5.2	Kryptografická operace (FCS_COP).....	41
6	Třída FDP: Ochrana uživatelských dat.....	42
6.1	Politika řízení přístupu (FDP_ACC).....	45
6.2	Funkce řízení přístupu (FDP_ACF).....	46
6.3	Autentizace dat (FDP_DAU)..... 47	
6.4	Export mimo oblast řízení TSF (FDP_ETC).....	49
6.5	Politika řízení toku informací (FDP_IFC).....	50
6.6	Funkce řízení toku informací (FDP_IFF).....	51

6.7	Import z oblasti mimo řízení TSF (FDP_ITC).....	55
6.8	Přenos uvnitř TOE (FDP_IPT).....	57
6.9	Ochrana zbytkových informací (FDP_RIP).....	59
6.10	Návrat zpracování (FDP_ROL).....	60
6.11	Integrita uchovávaných dat (FDP_SDI).....	61
6.12	Ochrana důvěrnosti uživatelských dat při přenosu mezi TSF (FDP_UCT).....	63
6.13	Ochrana integrity uživatelských dat při přenosu mezi TSF (FDP_UIT).....	64
7	Třída FIA: Identifikace a autentizace.....	66
7.1	Selhání autentizace (FIA_AFL).....	67
7.2	Definice uživatelských atributů (FIA_ATD).....	68
7.3	Specifikace tajných informací (FIA_SOS).....	69
7.4	Autentizace uživatele (FIA_UAU).....	70
7.5	Identifikace uživatele (FIA_UID).....	73
7.6	Svázání uživatele se subjektem (FIA_USB).....	74
8	Třída FMT: Správa bezpečnosti.....	75
8.1	Správa funkcí v TSF (FMT_MOF).....	77
8.2	Správa bezpečnostních atributů (FMT_MSA).....	78
8.3	Správa dat TSF	

(FMT_MTD).....	80
8.4 Revokace (FMT_REV).....	82
8.5 Vypršení platnosti bezpečnostních atributů (FMT_SAE).....	83
8.6 Role Správy bezpečnosti (FMT_SMR).....	84
9 Třída FPR: Soukromí.....	86
9.1 Anonymita (FPR_ANO).....	87
9.2 Pseudonymita (FPR_PSE).....	88
9.3 Nespojitelnost (FPR_UNL).....	90
9.4 Nepozorovatelnost (FPR_UNO).....	91
10 Třída FPT: Ochrana TSF.....	93
10.1 Test základního abstraktního stroje (FPT_AMT).....	96
10.2 Bezpečné selhání (FPT_FLS).....	97
10.3 Dostupnost exportovaných dat TSF (FPT_ITA).....	98
10.4 Důvěrnost exportovaných dat TSF (FPT_ITC).....	99
10.5 Integrita exportovaných dat TSF (FPT_ITI).....	100
10.6 Přenos dat TSF uvnitř TOE (FPT_ITT).....	102

10.7 Fyzická ochrana TSF (FPT_PHP).....	104
10.8 Důvěryhodná obnova (FPT_RCV).....	106
10.9 Detekce opakovaného přenosu (FPT_RPL).....	108
10.10 Zprostředkování odkazu (FPT_RVM).....	109
10.11 Oddělení domény (FPT_SEP).....	110
10.12 Protokol synchronizace stavu (FPT_SSP).....	112
10.13 Vyznačení času (FPT_STM).....	113
10.14 Konzistence dat TSF mezi TSF (FPT_TDC).....	114
10.15 Konzistence replikace dat TSF uvnitř TOE (FPT_TRC).....	115

10.16 Samotestování (self test) TSF (FPT_TST).....	116
11 Třída FRU: Využití zdrojů.....	117
11.1 Tolerance k chybě (FRU_FLT).....	118
11.2 Priorita služeb (FRU_PRS).....	119
11.3 Alokace zdrojů (FRU_RSA).....	120
12 Třída FTA: přístup k TOE.....	121

12.1	Limitování rozsahu volitelných atributů (FTA_LSA).....	122
12.2	Limitování vícenásobných souběžných relací (FTA_MCS).....	123
12.3	Uzamknutí relace (FTA_SSL).....	124
12.4	Upozornění při přístupu k TOE (FTA_TAB).....	126
12.5	Historie přístupu k TOE (FTA_TAH).....	127
12.6	Ustavení relace TOE (FTA_TSE).....	128
13	Třída FTP: Důvěryhodná cesta/kanály.....	129
13.1	Důvěryhodný kanál mezi TSF (FTP_ITC).....	130
13.2	Důvěryhodná cesta (FTP_TRP).....	131
Příloha A (informativní) Aplikační poznámky týkající se bezpečnostních funkčních požadavků..... 132		
A.1	Struktura poznámek	132
A.2	Tabulka závislostí	135
Příloha B (informativní) Funkční třídy, rodiny a komponenty..... 142		
Příloha C (informativní) Bezpečnostní audit (FAU)..... 143		
C.1	Automatická odezva bezpečnostního auditu (FAU_ARP).....	145
C.2	Generování dat bezpečnostního auditu (FAU_GEN).....	146
C.3	Analýza bezpečnostního auditu (FAU_SAA).....	148

C.4	Revize bezpečnostního auditu (FAU_SAR).....	152
C.5	Výběr událostí bezpečnostního auditu (FAU_SEL).....	154
C.6	Uchování událostí bezpečnostního auditu (FAU_STG).....	155
Příloha D	(informativní) Komunikace (FCO).....	157
D.1	Nepopiratelnost původu (FCO_NRO).....	158
D.2	Nepopiratelnost přijetí (FCO_NRR).....	160
Příloha E	(informativní) Kryptografická podpora (FCS).....	162
E.1	Správa kryptografických klíčů (FCS_CKM).....	163
E.2	Kryptografická operace (FCS_COP).....	164
Příloha F	(informativní) Ochrana uživatelských dat (FDP).....	166
F.1	Politika řízení přístupu (FDP_ACC).....	170
F.2	Funkce řízení přístupu (FDP_ACF).....	172
F.3	Autentizace dat (FDP_DAU).....	174
F.4	Export mimo oblast řízení TSF (FDP_ETC).....	175
F.5	Politika řízení toku informací (FDP_IFC).....	176
F.6	Funkce řízení toku informací (FDP_IFT).....	178
F.7	Import z oblasti mimo řízení TSF (FDP_ITC).....	182
F.8	Přenos uvnitř TOE (FDP_ITT).....	184

F.9 Ochrana zbytkových informací (FDP_RIP).....	187
---	-----

Strana 6

Strana

F.10 Návrat zpracování (Rollback) (FDP_ROL).....	189
--	-----

F.11 Integrita uchovávaných dat (FDP_SDI).....	191
--	-----

F.12 Ochrana důvěrnosti uživatelských dat při přenosu mezi TSF (FDP_UCT).....	192
---	-----

F.13 Ochrana integrity uživatelských dat při přenosu mezi TSF (FDP_UIT).....	193
--	-----

Příloha G (informativní) Identifikace a autentizace (FIA).....	195
--	-----

G.1 Selhání autentizace (FIA_AFL).....	197
--	-----

G.2 Definice uživatelských atributů (FIA_ATD).....	198
--	-----

G.3 Specifikace tajných informací (FIA_SOS).....	199
--	-----

G.4 Autentizace uživatele (FIA_UAU).....	200
--	-----

G.5 Identifikace uživatele (FIA_UID).....	203
---	-----

G.6 Svázání uživatele se subjektem (FIA_USB).....	204
---	-----

Příloha H (informativní) Správa bezpečnosti (FMT).....	205
--	-----

H.1 Správa funkcí v TSF (FMT_MOF).....	207
--	-----

H.2 Správa bezpečnostních atributů (FMT_MSA).....	208
---	-----

H.3 Správa dat TSF (FMT_MTD).....	210
---	-----

H.4	Revokace (FMT_REV)	212
H.5	Vypršení platnosti bezpečnostních atributů (FMT_SAE)	213
H.6	Role Správy bezpečnosti (FMT_SMR)	214
Příloha I	(informativní) Soukromí (FPR)	215
I.1	Anonymita (FPR_ANO)	217
I.2	Pseudonymita (FPR_PSE)	217
I.3	Nespojitelnost (FPR_UNL)	222
I.4	Nepozorovatelnost (FPR_UNO)	223
Příloha J	(informativní) Ochrana TSF (FPT)	226
J.1	Test základního abstraktního stroje (FPT_AMT)	230
J.2	Bezpečné selhání (FPT_FLS)	231
J.3	Dostupnost exportovaných dat TSF (FPT_ITA)	232
J.4	Důvěrnost exportovaných dat TSF (FPT_ITC)	233
J.5	Integrita exportovaných dat TSF (FPT_ITI)	234
J.6	Přenos dat TSF uvnitř TOE (FPT_ITT)	236
J.7	Fyzická ochrana TSF (FPT_PHP)	237
J.8	Důvěryhodná obnova	

(FPT_RCV).....	239
J.9 Detekce opakovaného přenosu	
(FPT_RPL).....	242
J.10 Zprostředkování odkazů	
(FPT_RVM).....	243
J.11 Oddělení domény	
(FPT_SEP).....	244
J.12 Protokol synchronizace stavu	
(FPT_SSP).....	246
J.13 Vyznačení času	
(FPT_STM).....	247
J.14 Konzistence dat TSF mezi TSF	
(FPT_TDC).....	248
J.15 Konzistence replikace dat TSF uvnitř TOE	
(FPT_TRC).....	249
J.16 Samotestování TSF	
(FPT_TST).....	250
Příloha K (informativní) Využití zdrojů	
(FRU).....	251
K.1 Tolerance k chybě	
(FRU_FLT).....	252

Strana 7

Strana

K.2 Priorita služby	
(FRU_PRS).....	253
K.3 Alokace zdrojů	
(FRU_RSA).....	254
Příloha L (informativní) Přístup k TOE	
(FTA).....	256
L.1 Limitování rozsahu volitelných atributů	
(FTA_LSA).....	258
L.2 Limitování vícenásobných souběžných relací	

(FTA_MCS).....	259
L.3 Uzamknutí relace	
(FTA_SSL).....	260
L.4 Upozornění při přístupu k TOE	
(FTA_TAB).....	262
L.5 Historie přístupu k TOE	
(FTA_TAH).....	263
L.6 Ustavení relace s TOE	
(FTA_TSE).....	264
Příloha M (informativní) Důvěryhodná cesta/kanály	
(FTP).....	265
M.1 Důvěryhodný kanál mezi TSF	
(FTP_ITC).....	266
M.2 Důvěryhodná cesta	
(FTP_TRP).....	267

Seznam obrázků

Obrázek 1.1 - Paradigma bezpečnostních funkčních požadavků (monolitický TOE)

Obrázek 1.2 - Diagram bezpečnostních funkcí v distribuovaném TOE

Obrázek 1.3 - Vztah mezi uživatelskými daty a daty TSF

Obrázek 1.4 - Vztah mezi „autentizačními daty“ a „tajnými informacemi“

Obrázek 2.1 - Struktura funkční třídy

Obrázek 2.2 - Struktura funkční rodiny

Obrázek 2.3 - Struktura funkční komponenty

Obrázek 2.4 - Vzorový diagram dekompozice třídy

Obrázek 3.1 - Dekompozice třídy Bezpečnostní audit

Obrázek 4.1 - Dekompozice třídy Komunikace

Obrázek 5.1 - Dekompozice třídy Kryptografická podpora

Obrázek 6.1 - Dekompozice třídy Ochrana uživatelských dat

Obrázek 6.2 - Dekompozice třídy Ochrana uživatelských dat (pokrač.)

Obrázek 7.1 - Dekompozice třídy Identifikace a autentizace

Obrázek 8.1 - Dekompozice třídy Správa bezpečnosti

Obrázek 9.1 - Dekompozice třídy Soukromí

Obrázek 10.1 - Dekompozice třídy Ochrana TSF

Obrázek 10.2 - Dekompozice třídy Ochrana TSF (pokrač.)

Obrázek 11.1 - Dekompozice třídy Využití zdrojů

Obrázek 12.1 - Dekompozice třídy Přístup k TOE

Obrázek 13.1 - Dekompozice třídy Důvěryhodná cesta/kanály

Obrázek A.1 - Struktura funkční třídy

Obrázek A.2 - Struktura funkční rodiny pro aplikační poznámky

Obrázek A.3 - Struktura funkční komponenty

Obrázek C.1 - Dekompozice třídy Bezpečnostní audit

Obrázek D.1 - Dekompozice třídy Komunikace

Obrázek E.1 - Dekompozice třídy Kryptografická podpora

Obrázek F.1 - Dekompozice třídy Ochrana uživatelských dat

Obrázek F.2 - Dekompozice třídy Ochrana uživatelských dat (pokrač.)

Obrázek G.1 - Dekompozice třídy Identifikace a autentizace

Obrázek H.1 - Dekompozice třídy Správa bezpečnosti

Obrázek I.1 - Dekompozice třídy Soukromí

Obrázek J.1 - Dekompozice třídy Ochrana TSF

Obrázek J.2 - Dekompozice třídy Ochrana TSF (pokrač.)

Obrázek K.1 - Dekompozice třídy Využití zdrojů

Obrázek L.1 - Dekompozice třídy Přístup k TOE

Obrázek M.1 - Dekompozice třídy Důvěryhodná cesta/kanály

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 mezinárodní organizace, vládní i nevládní, s nimiž ISO a IEC navázalo pracovní styk.

Mezinárodní normy jsou navrhovány v souladu s pravidly uvedenými v části 3 směrnice ISO/IEC.

ISO a IEC ustavily v oblasti informačních technologií společnou technickou komisi, ISO/IEC JTC 1. Návrhy mezinárodních norem, přijaté společnou technickou komisí, se rozesílají národním orgánům k hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75 % hlasujících národních orgánů.

Mezinárodní norma ISO/IEC 15408-2 byla připravena společnou technickou komisí ISO/IEC JTC 1, *Informační technologie*, ve spolupráci s organizacemi sponzorujícími projekt Common Criteria. Identický text ISO/IEC 15408-2 je zveřejněn organizacemi sponzorujícími projekt Common Criteria pod názvem *Společná kritéria pro hodnocení bezpečnosti informačních technologií*. V příloze A ISO/IEC 15408-1 jsou uvedeny další informace o projektu Common Criteria a kontaktní informace o sponzorech projektu.

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 požadavky
- Část 3: Požadavky na záruku bezpečnosti.

Přílohy A až M této části ISO/IEC 15408 jsou pouze informativní.

Na základě žádosti byla do všech částí ISO/IEC 15408 umístěna tato PRÁVNÍ POZNÁMKA:

Sedm vládních organizací (společně nazývaných „Organizace sponzorující projekt Common Criteria“), které jsou uvedené v příloze A ISO/IEC 15408-1, přidělují tímto jako společní držitelé autorských práv dokumentu Společná kritéria pro hodnocení bezpečnosti informačních technologií, část 1 až 3 (nazývaných „CC“) organizaci ISO/IEC neexkluzivní licenci k používání CC při vývoji mezinárodní normy ISO/IEC 15408. Organizace sponzorující projekt Common Criteria si však ponechávají právo používat, kopírovat, šířit nebo pozměňovat CC, jak uznají za vhodné.

1 Předmět normy

Bezpečnostní funkční komponenty definované v této části ISO/IEC 15408 jsou základem pro IT bezpečnostní funkční požadavky vyjádřené v Profilu ochrany (PP) nebo v Bezpečnostním cíli (ST). Tyto požadavky popisují žádoucí bezpečnostní chování očekávané Předmětem hodnocení (TOE) a jsou určeny ke splnění bezpečnostních cílů uvedených v PP nebo ST. Tyto požadavky popisují bezpečnostní vlastnosti, které uživatel může detekovat přímou interakcí s TOE (například vstupy, výstupy) nebo odezvou TOE na podnět.

Bezpečnostní funkční komponenty vyjadřují bezpečnostní požadavky, jejichž cílem je čelit hrozbám v

předpokládaném provozním prostředí TOE a/nebo pokrýt jakékoliv identifikované organizační bezpečnostní politiky a předpoklady.

Tato část ISO/IEC 15408 je určena spotřebitelům, vývojářům a hodnotitelům bezpečných systémů a produktů IT. Kapitola 3 ISO/IEC 15408-1 poskytuje další informace o cílových adresátech ISO/IEC 15408 a o použití norem skupinami, které zahrnují tyto adresáty. Tyto skupiny mohou použít tuto část ISO/IEC 15408 následovně.

- Spotřebitelé, kteří používají při výběru komponent ISO/IEC 15408-2, aby vyjádřili funkční požadavky k uspokojení bezpečnostních cílů vyjádřených v PP nebo ST. ISO/IEC 15408-1 ve 4.3 poskytuje podrobnější informace o vztahu mezi bezpečnostními cíli a bezpečnostními požadavky.
- Vývojáři, kteří odpovídají na aktuální nebo registrované bezpečnostní požadavky při konstruování TOE, mohou nalézt v této části ISO/IEC 15408 normalizovanou metodu k pochopení těchto požadavků. Mohou také použít obsah této části ISO/IEC 15408 jako základ pro další definování bezpečnostních funkcí a mechanismů TOE, které odpovídají těmto požadavkům.
- Hodnotitelé, kteří používají funkční požadavky definované v této části ISO/IEC 15408 při ověřování, zda funkční požadavky TOE vyjádřené v PP nebo ST splňují cíle bezpečnosti IT a zda jsou objasněny a ukázány všechny závislosti, aby mohly být splněny. Hodnotitelé by také měli použít tuto část ISO/IEC 15408 jako pomoc při určení, zda daný TOE uspokojuje stanovené požadavky.

-- Vynechaný text --