

ČESKÁ TECHNICKÁ NORMA

ICS35.040 **Březen 2010**

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

**ČSN
ISO/IEC 15408-2
36 9789**

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

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

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

Tato norma je českou verzí mezinárodní normy ISO/IEC 15408-2:2008. 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 15408-2:2008. 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 15408-2 (36 9789) z listopadu 2002.

Národní předmluva

Změny proti předchozím normám

Změny v této normě oproti normě původní se týkají vypuštění některých částí původní normy, přidání nových částí a dále formálních úprav, například číslování.

Informace o citovaných normativních dokumentech

ISO/IEC 15408-1 zavedena v ČSN ISO/IEC 15408-1 (36 9789) Informační technologie - Bezpečnostní techniky - Kritéria hodnocení bezpečnosti IT - Část 1: Úvod a všeobecný model

Další informace

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 vlivech.

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
- c. anglický výraz Management jako správa nebo řízení nebo jejich kombinace
- d. anglický výraz Time Stamp jako vyznačení času.
- e. 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. Alena Hönigová, IČ 61470716

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- Kritéria ISO/IEC 15408-2
pro hodnocení bezpečnosti IT - Třetí vydání
Část 2: Bezpečnostní funkční komponenty 2008-08

Obsah

Strana

Předmluva 24

Úvod 25

1 Předmět normy 26

2 Normativní dokumenty 26

3 Termíny a definice, symboly a zkrácené termíny 26

4 Přehled 26

4.1 Organizace této části ISO/IEC 15408 26

5 Paradigma funkčních požadavků 26

6 Bezpečnostní funkční požadavky 29

6.1	Přehled	29
6.1.1	Struktura třídy	29
6.1.2	Struktura rodiny	30
6.1.3	Struktura komponenty	31
6.2	Katalog komponent	33
6.2.1	Zvýraznění změn komponent	33
7	Třída FAU: Bezpečnostní audit	33
7.1	Automatická odezva bezpečnostního auditu (FAU_ARP)	34
7.1.1	Chování rodiny	34
7.1.2	Řazení komponent do úrovní	34
7.1.3	Správa FAU_ARP.1	34
7.1.4	Audit FAU_ARP.1	34
7.1.5	FAU_ARP.1 Bezpečnostní alarmy	34
7.2	Generování dat bezpečnostního auditu (FAU_GEN)	35
7.2.1	Chování rodiny	35
7.2.2	Řazení komponent do úrovní	35
7.2.3	Správa FAU_GEN.1, FAU_GEN.2	35
7.2.4	Audit FAU_GEN.1, FAU_GEN.2	35
7.2.5	FAU_GEN.1 Generování dat auditu	35
7.2.6	FAU_GEN.2 Přidružení identity uživatele	35
7.3	Analýza bezpečnostního auditu (FAU_SAA)	36
7.3.1	Chování rodiny	36
7.3.2	Řazení komponent do úrovní	36
7.3.3	Správa FAU_SAA.1	36
7.3.4	Správa FAU_SAA.2	36
7.3.5	Správa FAU_SAA.3	36
7.3.6	Správa FAU_SAA.4	36

- 7.3.7 Audit FAU_SAA.1, FAU_SAA.2, FAU_SAA.3, FAU_SAA.4 36
- 7.3.8 Správa FAU_SAA.1 Analýza potenciálního narušení 36
- 7.3.9 FAU_SAA.2 Detekce anomálií založená na profilech 37
- 7.3.10 FAU_SAA.3 Heuristika jednoduchého útoku 37
- 7.3.11 FAU_SAA.4 Heuristika komplexního útoku 37
- 7.4 Revize bezpečnostního auditu (FAU_SAR) 38
 - 7.4.1 Chování rodiny 38
 - 7.4.2 Řazení komponent do úrovní 38
 - 7.4.3 Správa FAU_SAR.1 38
 - 7.4.4 Správa FAU_SAR.2, FAU_SAR.3 38
 - 7.4.5 Audit FAU_SAR.1 38
 - 7.4.6 Audit FAU_SAR.2 38
 - 7.4.7 Audit FAU_SAR.3 38
 - 7.4.8 FAU_SAR.1 Revize auditu 38
 - 7.4.9 FAU_SAR.2 Omezená revize auditu 39
 - 7.4.10 FAU_SAR.3 Volitelná revize auditu 39
- 7.5 Výběr událostí bezpečnostního auditu (FAU_SEL) 39
 - 7.5.1 Chování rodiny 39
 - 7.5.2 Řazení komponent do úrovní 39
 - 7.5.3 Správa FAU_SEL.1 39
 - 7.5.4. Audit FAU_SEL.1 39
 - 7.5.5 FAU_SEL.1 Selektivní audit 39
- 7.6 Uchování událostí bezpečnostního auditu (FAU_STG) 40
 - 7.6.1 Chování rodiny 40
 - 7.6.2 Řazení komponent do úrovní 40
 - 7.6.3 Správa FAU_STG.1 40
 - 7.6.4 Správa FAU_STG.2 40
 - 7.6.5 Správa FAU_STG.3 40

7.6.6	Správa FAU_STG.4	40
7.6.7	Audit FAU_STG.1, FAU_STG.2	40
7.6.8	Audit FAU_STG.3	40
7.6.9	Audit FAU_STG.4	40
7.6.10	FAU_STG.1 Chráněné uchování auditního záznamu	40
7.6.11	FAU_STG.2 Záruky dostupnosti auditních dat	41
7.6.12	FAU_STG.3 Akce v případě možné ztráty auditních dat	41
7.6.13	FAU_STG.4 Zabránění ztrátě auditních dat	41
8	Třída FCO: Komunikace	41
8.1	Nepopiratelnost původu (FCO_NRO)	42
8.1.1	Chování rodiny	42
8.1.2	Řazení komponent do úrovní	42
8.1.3	Správa FCO_NRO.1, FCO_NRO.2	42
8.1.4	Audit FCO_NRO.1	42
8.1.5	Audit FCO_NRO.2	42
8.1.6	FCO_NRO.1 Selektivní průkaz původu	42
8.1.7	FCO_NRO.2 Prosazený průkaz původu	42
8.2	Nepopiratelnost přijetí (FCO_NRR)	43
8.2.1	Chování rodiny	43
8.2.2	Řazení komponent do úrovní	43
8.2.3	Správa FCO_NRR.1, FCO_NRR.2	43
8.2.4	Audit FCO_NRR.1	43
8.2.5	Audit FCO_NRR.2	43
8.2.6	FCO_NRR.1 Selektivní průkaz přijetí	43
8.2.7	FCO_NRR.2 Prosazený průkaz přijetí	44
9	Třída FCS: Kryptografická podpora	44
9.1	Správa kryptografických klíčů (FCS_CKM)	45

- 9.1.1** Chování rodiny 45
- 9.1.2** Řazení komponent do úrovní 45
- 9.1.3** Správa FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4 45
- 9.1.4** Audit FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4 45
- 9.1.5** FCS_CKM.1 Generování kryptografických klíčů 45
- 9.1.6** FCS_CKM.2 Distribuce kryptografických klíčů 45
- 9.1.7** FCS_CKM.3 Přístup ke kryptografickým klíčům 46
- 9.1.8** FCS_CKM.4 Zničení kryptografických klíčů 46
- 9.2** Kryptografická operace (FCS_COP) 46
 - 9.2.1** Chování rodiny 46
 - 9.2.2** Řazení komponent do úrovní 46
 - 9.2.3** Správa FCS_COP.1 46
 - 9.2.4** Audit FCS_COP.1 46
 - 9.2.5** FCS_COP.1 Kryptografické operace 47
- 10** Třída FDP: Ochrana uživatelských dat 47
 - 10.1** Politika řízení přístupu (FDP_ACC) 49
 - 10.1.1** Chování rodiny 49
 - 10.1.2** Řazení komponent do úrovní 49
 - 10.1.3** Správa FDP_ACC.1, FDP_ACC.2 49
 - 10.1.4** Audit FDP_ACC.1, FDP_ACC.2 49
 - 10.1.5** FDP_ACC.1 Řízení přístupu k podmnožině 49
 - 10.1.6** FDP_ACC.2 Úplné řízení přístupu 49
 - 10.2** Funkce řízení přístupu (FDP_ACF) 49
 - 10.2.1** Chování rodiny 49
 - 10.2.2** Řazení komponent do úrovní 50
 - 10.2.3** Správa FDP_ACF.1 50
 - 10.2.4** Audit FDP_ACF.1 50
 - 10.2.5** FDP_ACF.1 Řízení přístupu založené na bezpečnostních attributech 50

- 10.3 Autentizace dat (FDP_DAU) 50**
 - 10.3.1 Chování rodiny 50**
 - 10.3.2 Řazení komponent do úrovní 51**
 - 10.3.3 Správa FDP_DAU.1, FDP_DAU.2 51**
 - 10.3.4 Audit FDP_DAU.1 51**
 - 10.3.5 Audit FDP_DAU.2 51**
 - 10.3.6 FDP_DAU.1.Základní autentizace dat 51**
 - 10.3.7 FDP_DAU.2.Autentizace dat s identitou ručitele 51**
- 10.4 Export mimo oblast řízení TOE (FDP_ETC) 52**
 - 10.4.1 Chování rodiny 52**
 - 10.4.2 Řazení komponent do úrovní 52**
 - 10.4.3 Správa FDP_ETC.1 52**
 - 10.4.4 Správa FDP_ETC.2 52**
 - 10.4.5 Audit FDP_ETC.1, FDP_ETC.2 52**
 - 10.4.6 FDP_ETC.1 Export uživatelských dat bez bezpečnostních atributů 52**
 - 10.4.7 FDP_ETC.2 Export uživatelských dat s bezpečnostními atributy 52**
- 10.5 Politika řízení toku informací (FDP_IFC) 53**
 - 10.5.1 Chování rodiny 53**
 - 10.5.2 Řazení komponent do úrovní 53**
 - 10.5.3 Správa FDP_IFC.1, FDP_IFC.2 53**
 - 10.5.4 Audit FDP_IFC.1, FDP_IFC.2 53**
 - 10.5.5 FDP_IFC.1 Řízení toku informací podmnožiny 53**
 - 10.5.6 FDP_IFC.1.2 Úplné řízení toku informací 53**
- 10.6 Funkce řízení toku informací (FDP_IFF) 54**
 - 10.6.1 Chování rodiny 54**
 - 10.6.2 Řazení komponent do úrovní 54**
 - 10.6.3 Správa FDP_IFF.1, FDP_IFF.2 54**

- 10.6.4** Správa FDP_IFF.3, FDP_IFF.4, FDP_IFF.5 54
- 10.6.5** Správa FDP_IFF.6 54
- 10.6.6** Audit FDP_IFF.1, FDP_IFF.2, FDP_IFF.5 54
- 10.6.7** Audit FDP_IFF.3, FDP_IFF.4, FDP_IFF.6 55
- 10.6.8** FDP_IFF.1 Jednoduché bezpečnostní atributy 55
- 10.6.9** FDP_IFF.2 Hierarchické bezpečnostní atributy 55
- 10.6.10** FDP_IFF.3 Limitované nelegální toky informací 56
- 10.6.11** FDP_IFF.4 Částečná eliminace nelegálních toků informací 56
- 10.6.12** FDP_IFF.5 Žádné nelegální toky informací 56
- 10.6.13** FDP_IFF.6 Monitorování nelegálních toků informací 56
- 10.7** Import z oblasti mimo řízení TOE (FDP_ITC) 57
 - 10.7.1** Chování rodiny 57
 - 10.7.2** Řazení komponent do úrovní 57
 - 10.7.3** Správa FDP_ITC.1, FDP_ITC.2 57
 - 10.7.4** Audit FDP_ITC.1, FDP_ITC.2 57
 - 10.7.5** FDP_ITC.1 Import uživatelských dat bez bezpečnostních atributů 57
 - 10.7.6** FDP_ITC.2 Import uživatelských dat s bezpečnostními atributy 58
- 10.8** Přenos uvnitř TOE (FDP_ITT) 58
 - 10.8.1** Chování rodiny 58
 - 10.8.2** Řazení komponent do úrovní 58
 - 10.8.3** Správa FDP_ITT.1, FDP_ITT.2 58
 - 10.8.4** Správa FDP_ITT.3, FDP_ITT.4 59
 - 10.8.5** Audit FDP_ITT.1, FDP_ITT.2 59
 - 10.8.6** Audit FDP_ITT.3, FDP_ITT.4 59
 - 10.8.7** FDP_ITT.1 Základní ochrana vnitřního přenosu 59
 - 10.8.8** FDP_ITT.2 Oddělení přenosu pomocí atributů 59
 - 10.8.9** FDP_ITT.3 Monitorování integrity 59

- 10.8.10** FDP_ITT.4 Monitorování integrity založené na attributech 60
- 10.9** Ochrana zbytkových informací (FDP_RIP) 60
 - 10.9.1** Chování rodiny 60
 - 10.9.2** Řazení komponent do úrovní 60
 - 10.9.3** Správa FDP_RIP.1, FDP_RIP.2 60
 - 10.9.4** Audit FDP_RIP.1, FDP_RIP.2 60
 - 10.9.5** FDP_RIP.1 Ochrana podmnožiny zbytkových informací 60
 - 10.9.6** FDP_RIP.2 Úplná ochrana zbytkových informací 61
- 10.10** Návrat zpracování (FDP_ROL) 61
 - 10.10.1** Chování rodiny 61
 - 10.10.2** Zařazení komponent do úrovní 61
 - 10.10.3** Správa FDP_ROL.1, FDP_ROL.2 61
 - 10.10.4** Audit FDP_ROL.1, FDP_ROL.2 61
 - 10.10.5** FDP_ROL.1 Základní návrat zpracování 61
 - 10.10.6** FDP_ROL.2 Opakované zpracování 61
- 10.11** Integrita uchovávaných dat (FDP_SDI) 62
 - 10.11.1** Chování rodiny 62
 - 10.11.2** Zařazení komponent do úrovní 62
 - 10.11.3** Správa FDP_SDI.1 62
 - 10.11.4** Správa FDP_SDI.2 62
 - 10.11.5** Audit FDP_SDI.1 62
 - 10.11.6** Audit FDP_SDI.2 62
 - 10.11.7** FDP_SDI.1 Monitorování integrity uložených dat 62
 - 10.11.8** FDP_SDI.2 Monitorování integrity uložených dat a následná akce 63
- 10.12** Ochrana důvěrnosti uživatelských dat při přenosu mezi TSF (FDP_UCT) 63
 - 10.12.1** Chování rodiny 63
 - 10.12.2** Řazení komponent do úrovní 63
 - 10.12.3** Správa FDP_UCT.1 63

- 10.12.4** Audit FDP_UCT.1 63
- 10.12.5** FDP_UCT.1 Důvěrnost při základní výměně dat 63
- 10.13** Ochrana integrity uživatelských dat při přenosu mezi TSF (FDP_UIT) 63
 - 10.13.1** Chování rodiny 63
 - 10.13.2** Řazení komponent do úrovní 64
 - 10.13.3** Správa FDP_UIT.1, FDP_UIT.2, FDP_UIT.3 64
 - 10.13.4** Audit FDP_UIT.1 64
 - 10.13.5** Audit FDP_UIT.2, FDP_UIT.3 64
 - 10.13.6** FDP_UIT.1 Integrita výměny dat 64
 - 10.13.7** FDP_UIT.2 Obnova výměny zdrojových dat 65
 - 10.13.8** FDP_UIT.3 Obnova výměny cílových dat 65
- 11** Třída FIA: Identifikace a autentizace 65
 - 11.1** Selhání autentizace (FIA_AFL) 66
 - 11.1.1** Chování rodiny 66
 - 11.1.2** Řazení komponent do úrovní 66
 - 11.1.3** Správa FIA_AFL.1 66
 - 11.1.4** Audit FIA_AFL.1 67
 - 11.1.5** FIA_AFL.1 Postup v případě selhání autentizace 67
 - 11.2** Definice uživatelských atributů (FIA_ATD) 67
 - 11.2.1** Chování rodiny 67
 - 11.2.2** Řazení komponent do úrovní 67
 - 11.2.3** Správa FIA_ATD.1 67
 - 11.2.4** Audit FIA_ATD.1 67
 - 11.2.5** FIA_ATD.1 Definice atributu uživatele 67
 - 11.3** Specifikace tajných informací (FIA_SOS) 67
 - 11.3.1** Chování rodiny 67
 - 11.3.2** Řazení komponent do úrovní 68

- 11.3.3** Správa FIA_SOS.1 68
- 11.3.4** Správa FIA_SOS.2 68
- 11.3.5** Audit FIA_SOS.1, FIA_SOS.2 68
- 11.3.6** FIA_SOS.1 Ověření tajných informací 68
- 11.3.7** FIA_SOS.2 TSF Generování tajných informací 68
- 11.4** Autentizace uživatele (FIA_UAU) 68
 - 11.4.1** Chování rodiny 68
 - 11.4.2** Řazení komponent do úrovní 68
 - 11.4.3** Správa FIA_UAU.1 69
 - 11.4.4** Správa FIA_UAU.2 69
 - 11.4.5** Správa FIA_UAU.3, FIA_UAU.4, FIA_UAU.7 69
 - 11.4.6** Správa FIA_UAU.5 69
 - 11.4.7** Správa FIA_UAU.6 69
 - 11.4.8** Audit FIA_UAU.1 69
 - 11.4.9** Audit FIA_UAU.2 69
 - 11.4.10** Audit FIA_UAU.3 70
 - 11.4.11** Audit FIA_UAU.4 70
 - 11.4.12** Audit FIA_UAU.5 70
 - 11.4.13** Audit FIA_UAU.6 70
 - 11.4.14** Audit FIA_UAU.7 70
 - 11.4.15** FIA_UAU.1 Načasování autentizace 70
 - 11.4.16** FIA_UAU.2 Autentizace uživatele před jakoukoliv akcí 70
 - 11.4.17** FIA_UAU.3 Nezfalšovatelná autentizace 70
 - 11.4.18** FIA_UAU.4 Autentizační mechanismy pro jediné použití 71
 - 11.4.19** FIA_UAU.5 Násobné autentizační mechanismy 71
 - 11.4.20** FIA_UAU.6 Opakovaná autentizace 71
 - 11.4.21** FIA_UAU.7 Chráněná zpětná vazba autentizace 71

- 11.5** Identifikace uživatele (FIA_UID) 71
 - 11.5.1** Chování rodiny 71
 - 11.5.2** Řazení komponent do úrovní 71
 - 11.5.3** Správa FIA_UID.1 72
 - 11.5.4** Správa FIA_UID.2 72
 - 11.5.5** Audit FIA_UID.1, FIA_UID.2 72
 - 11.5.6** FIA_UID.1 Načasování identifikace 72
 - 11.5.7** FIA_UID.2 Identifikace uživatele před jakoukoliv akcí 72
- 11.6** Svázání uživatele se subjektem (FIA_USB) 72
 - 11.6.1** Chování rodiny 72
 - 11.6.2** Zařazení komponent do úrovní 72
 - 11.6.3** Správa FIA_USB.1 72
 - 11.6.4** Audit FIA_USB.1 73
 - 11.6.5** FIA_USB.1 Svázání uživatele se subjektem 73
- 12** Třída FMT: Správa bezpečnosti 73
 - 12.1** Správa funkcí v TSF (FMT_MOF) 74
 - 12.1.1** Chování rodiny 74
 - 12.1.2** Řazení komponent do úrovní 74
 - 12.1.3** Správa FMT_MOF.1 74
 - 12.1.4** Audit FMT_MOF.1 74
 - 12.1.5** FMT_MOF.1 Správa chování bezpečnostních funkcí 75
 - 12.2** Správa bezpečnostních atributů (FMT_MSA) 75
 - 12.2.1** Chování rodiny 75
 - 12.2.2** Řazení komponent do úrovní 75
 - 12.2.3** Správa FMT_MSA.1 75
 - 12.2.4** Správa FMT_MSA.2 75
 - 12.2.5** Správa FMT_MSA.3 75
 - 12.2.6** Správa FMT_MSA.4 75

- 12.2.7** Audit FMT_MSA.1 75
- 12.2.8** Audit FMT_MSA.2 76
- 12.2.9** Audit FMT_MSA.3 76
- 12.2.10** Audit FMT_MSA.4 76
- 12.2.11** FMT_MSA.1 Správa bezpečnostních atributů 76
- 12.2.12** FMT_MSA.2 Bezpečné bezpečnostní atributy 76
- 12.2.13** FMT_MSA.3 Inicializace statických atributů 76
- 12.2.14** FMT_MSA.4 Převzetí hodnoty bezpečnostních atributů 77
- 12.3** Správa dat TSF (FMT_MTD) 77

Strana

- 12.3.1** Chování rodiny 77
- 12.3.2** Řazení komponent do úrovní 77
- 12.3.3** Správa FMT_MTD.1 77
- 12.3.4** Správa FMT_MTD.2 77
- 12.3.5** Správa FMT_MTD.3 77
- 12.3.6** Audit FMT_MTD.1 77
- 12.3.7** Audit FMT_MTD.2 77
- 12.3.8** Audit FMT_MTD.3 77
- 12.3.9** FMT_MTD.1 Správa dat TSF 78
- 12.3.10** FMT_MTD.2 Správa limitů kladených na data TSF 78
- 12.3.11** FMT_MTD.3 Bezpečná data TSF 78
- 12.4** Revokace (FMT_REV) 78
 - 12.4.1** Chování rodiny 78
 - 12.4.2** Řazení komponent do úrovní 78
 - 12.4.3** Správa FMT_REV.1 78
 - 12.4.4** Audit FMT_REV.1 78
 - 12.4.5** FMT_REV.1 Revokace 78
- 12.5** Vypršení platnosti bezpečnostních atributů (FMT_SAE) 79

- 12.5.1** Chování rodiny 79
- 12.5.2** Řazení komponent do úrovní 79
- 12.5.3** Správa FMT_SAE.1 79
- 12.5.4** Audit FMT_SAE.1 79
- 12.5.5** FMT_SAE.1 Časově omezená autorizace 79
- 12.6** Specifikace funkcí správy (FMT_SMF) 79
 - 12.6.1** Chování rodiny 79
 - 12.6.2** Řazení komponent do úrovní 80
 - 12.6.3** Správa FMT_SMF.1 80
 - 12.6.4** Audit FMT_SMF.1 80
 - 12.6.5** FMT_SMF.1 Specifikace funkcí správy 80
- 12.7** Role správy bezpečnosti (FMT_SMR) 80
 - 12.7.1** Chování rodiny 80
 - 12.7.2** Řazení komponent do úrovní 80
 - 12.7.3** Správa FMT_SMR.1 80
 - 12.7.4** Správa FMT_SMR.2 80
 - 12.7.5** Správa FMT_SMR.3 80
 - 12.7.6** Audit FMT_SMR.1 80
 - 12.7.7** Audit FMT_SMR.2 81
 - 12.7.8** Audit FMT_SMR.3 81
 - 12.7.9** FMT_SMR.1 Bezpečnostní role 81
 - 12.7.10** FMT_SMR.2 Omezení bezpečnostních rolí 81
 - 12.7.11** FMT_SMR.3 Přijetí rolí 81
- 13** Třída FPR: Soukromí 81
 - 13.1** Anonymita (FPR_ANO) 82
 - 13.1.1** Chování rodiny 82
 - 13.1.2** Řazení komponent do úrovní 82

- 13.1.3** Správa FPR_ANO.1, FPR_ANO.2 82
- 13.1.4** Audit FPR_ANO.1, FPR_ANO.2 82
- 13.1.5** FPR_ANO.1 Anonymita 82
- 13.1.6** FPR_ANO.2 Anonymita bez získání informací 82
- 13.2** Pseudonymita (FPR_PSE) 83
 - 13.2.1** Chování rodiny 83
 - 13.2.2** Řazení komponent do úrovní 83
 - 13.2.3** Správa FPR_PSE.1, FPR_PSE.2, FPR_PSE.3 83
 - 13.2.4** Audit FPR_PSE.1, FPR_PSE.2, FPR_PSE.3 83
 - 13.2.5** FPR_PSE.1 Pseudonymita 83
 - 13.2.6** FPR_PSE.2 Reverzibilní pseudonymita 83
 - 13.2.7** FPR_PSE.3 Pseudonymita alias 84
- 13.3** Nespojitelnost (FPR_UNL) 84
 - 13.3.1** Chování rodiny 84
 - 13.3.2** Řazení komponent do úrovní 84
 - 13.3.3** Správa FPR_UNL.1 84
 - 13.3.4** Audit FPR_UNL.1 84
 - 13.3.5** FPR_UNL.1 Nespojitelnost 84
- 13.4** Nepozorovatelnost (FPR_UNO) 85
 - 13.4.1** Chování rodiny 85
 - 13.4.2** Řazení komponent do úrovní 85
 - 13.4.3** Správa FPR_UNO.1, FPR_UNO.2 85
 - 13.4.4** Správa FPR_UNO.3 85
 - 13.4.5** Správa FPR_UNO.4 85
 - 13.4.6** Audit FPR_UNO.1, FPR_UNO.2 85
 - 13.4.7** Audit FPR_UNO.3 85
 - 13.4.8** Audit FPR_UNO.4 85
 - 13.4.9** FPR_UNO.1 Nepozorovatelnost 85

13.4.10	FPR_UNO.2 Alokace informací ovlivňujících nepozorovatelnost	86
13.4.11	FPR_UNO.3 Nepozorovatelnost bez získání informací	86
13.4.12	FPR_UNO.4 Pozorovatelnost autorizovaným uživatelem	86
14	Třída FPT: Ochrana TSF	86
14.1	Bezpečné selhání (FPT_FLS)	88
14.1.1	Chování rodiny	88
14.1.2	Řazení komponent do úrovní	88
14.1.3	Správa FPT_FLS.1	88
14.1.4	Audit FPT_FLS.1	88
14.1.5	FPT_FLS.1 Selhání se zachováním bezpečného stavu	88
14.2	Dostupnost exportovaných dat TSF (FPT_ITA)	88
14.2.1	Chování rodiny	88
14.2.2	Řazení komponent do úrovní	88
14.2.3	Správa FPT_ITA.1	88
14.2.4	Audit FPT_ITA.1	88
14.2.5	FPT_ITA.1 Dostupnost mezi TSF v rámci definované metriky dostupnosti	88
14.3	Důvěrnost exportovaných dat TSF (FPT_ITC)	89
14.3.1	Chování rodiny	89
14.3.2	Řazení komponent do úrovní	89
14.3.3	Správa FPT_ITC.1	89
14.3.4	Audit FPT_ITC.1	89
14.3.4	FPT_ITC.1 Důvěrnost mezi TSF během přenosu	89
14.4	Integrita exportovaných dat TSF (FPT_ITI)	89
14.4.1	Chování rodiny	89
14.4.2	Řazení komponent do úrovní	89
14.4.3	Správa FPT_ITI.1	89
14.4.4	Správa FPT_ITI.2	89

- 14.4.5** Audit FPT_ITI.1 90
- 14.4.6** Audit FPT_ITI.2 90
- 14.4.7** FPT_ITI.1 Detekce modifikace mezi TSF 90
- 14.4.8** FPT_ITI.2 Detekce a korekce modifikace mezi TSF 90
- 14.5** Přenos dat TSF uvnitř TOE (FPT_ITT) 90
 - 14.5.1** Chování rodiny 90
 - 14.5.2** Řazení komponent do úrovní 90
 - 14.5.3** Správa FPT_ITT.1 91
 - 14.5.4** Správa FPT_ITT.2 91
 - 14.5.5** Správa FPT_ITT.3 91
 - 14.5.6** Audit FPT_ITT.1, FPT_ITT.2 91
 - 14.5.7** Audit FPT_ITT.3 91
 - 14.5.8** FPT_ITT.1 Základní ochrana přenosu dat uvnitř TSF 91
 - 14.5.9** FPT_ITT.2 Oddělení přenosu dat TSF 91
 - 14.5.10** FPT_ITT.3 Monitorování integrity dat TSF 91
- 14.6** Fyzická ochrana TSF (FPT_PHP) 92
 - 14.6.1** Chování rodiny 92
 - 14.6.2** Řazení komponent do úrovní 92
 - 14.6.3** Správa FPT_PHP.1 92
 - 14.6.4** Správa FPT_PHP.2 92
 - 14.6.5** Správa FPT_PHP.3 92
 - 14.6.6** Audit FPT_PHP.1 92
 - 14.6.7** Audit FPT_PHP.2 92
 - 14.6.8** Audit FPT_PHP.3 93
 - 14.6.9** FPT_PHP.1 Pasivní detekce fyzického útoku 93
 - 14.6.10** FPT_PHP.2 Oznámení fyzického útoku 93
 - 14.6.11** FPT_PHP.3 Odolnost proti fyzickému útoku 93
- 14.7** Důvěryhodná obnova (FPT_RCV) 93

- 14.7.1** Chování rodiny 93
- 14.7.2** Řazení komponent do úrovní 93
- 14.7.3** Správa FPT_RCV.1 94
- 14.7.4** Správa FPT_RCV.2, FPT_RCV.3 94
- 14.7.5** Správa FPT_RCV.4 94
- 14.7.6** Audit FPT_RCV.1, FPT_RCV.2, FPT_RCV.3 94
- 14.7.7** Audit FPT_RCV.4 94
- 14.7.8** FPT_RCV.1 Ruční obnova 94
- 14.7.9** FPT_RCV.2 Automatická obnova 94
- 14.7.10** FPT_RCV.3 Automatická obnova bez nepřiměřené ztráty 94
- 14.7.11** FPT_RCV.4 Obnova funkce 95
- 14.8** Detekce opakovaného přenosu (FPT_RPL) 95
 - 14.8.1** Chování rodiny 95
 - 14.8.2** Řazení komponent do úrovní 95
 - 14.8.3** Správa FPT_RPL.1 95
 - 14.8.4** Audit FPT_RPL.1 95
 - 14.8.5** FPT_RPL.1 Detekce opakovaného přenosu 95
- 14.9** Protokol synchronizace stavu (FPT_SSP) 96
 - 14.9.1** Chování rodiny 96
 - 14.9.2** Řazení komponent do úrovní 96
 - 14.9.3** Správa FPT_SSP.1, FPT_SSP.2 96
 - 14.9.4** Audit FPT_SSP.1, FPT_SSP.2 96
 - 14.9.5** FPT_SSP.1 Jednoduché důvěryhodné potvrzení 96
 - 14.9.6** FPT_SSP.2 Vzájemné důvěryhodné potvrzení 96
- 14.10** Vyznačení času (FPT_STM) 96
 - 14.10.1** Chování rodiny 96
 - 14.10.2** Řazení komponent do úrovní 96

- 14.10.3** Správa FPT_STM.1 96
- 14.10.4** Audit FPT_STM.1 97
- 14.10.5** FPT_STM.1 Spolehlivá vyznačení času 97
- 14.11** Konzistence dat TSF mezi TSF (FPT_TDC) 97
 - 14.11.1** Chování rodiny 97
 - 14.11.2** Řazení komponent do úrovní 97
 - 14.11.3** Správa FPT_TDC.1 97
 - 14.11.4** Audit FPT_TDC.1 97
 - 14.11.5** FPT_TDC.1 Základní konzistence dat TSF mezi TSF 97
- 14.12** Testování externích entit (FPT_TEE) 97
 - 14.12.1** Chování rodiny 97
 - 14.12.2** Řazení komponent do úrovní 98
 - 14.12.3** Správa FPT_TEE.1 98
 - 14.12.4** Audit FPT_TEE.1 98
 - 14.12.5** FPT_TEE.1 Testování extrémních entit 98
- 14.13** Konzistence replikace dat TSF uvnitř TOE (FPT_TRC) 98
 - 14.13.1** Chování rodiny 98
 - 14.13.2** Řazení komponent do úrovní 98
 - 14.13.3** Správa FPT_TRC.1 98
 - 14.13.4** Audit FPT_TRC.1 98
 - 14.13.5** FPT_TRC.1 Vnitřní konzistence TSF 98
- 14.14** Samotestování (self test) TSF (FPT_TST) 99
 - 14.14.1** Chování rodiny 99
 - 14.14.2** Řazení komponent do úrovní 99
 - 14.14.3** Správa FPT_TST.1 99
 - 14.14.4** Audit FPT_TST.1 99
 - 14.14.5** FPT_TST.1 Testování TSF 99

- 15 Třída FRU: Využití zdrojů 100**
 - 15.1 Tolerance k chybě (FRU_FLT) 100**
 - 15.1.1 Chování rodiny 100**
 - 15.1.2 Řazení komponent do úrovní 100**
 - 15.1.3 Správa FRU_FLT.1, FRU_FLT.2 100**
 - 15.1.4 Audit FRU_FLT.1 100**
 - 15.1.5 AuditFRU_FLT.2 100**
 - 15.1.6 FRU_FLT.1 Snížená tolerance k chybě 100**
 - 15.1.7 FRU_FLT.2 Limitovaná tolerance k chybě 101**
 - 15.2 Priorita služby (FRU_PRS) 101**
 - 15.2.1 Chování rodiny 101**
 - 15.2.2 Řazení komponent do úrovní 101**
 - 15.2.3 Správa FRU_PRS.1, FRU_PRS.2 101**
 - 15.2.4 Audit FRU_PRS.1, FRU_PRS.2 101**
 - 15.2.5 FRU_PRS.1 Limitovaná priorita služby 101**
 - 15.2.6 FRU_PRS.2 Úplná priorita služby 101**
 - 15.3 Alokace zdrojů (FRU_RSA) 102**
 - 15.3.1 Chování rodiny 102**
 - 15.3.2 Řazení komponent do úrovní 102**
 - 15.3.3 Správa FRU_RSA.1 102**
 - 15.3.4 Správa FRU_RSA.2 102**
 - 15.3.5 Audit FRU_RSA.1, FRU_RSA.2 102**
 - 15.3.6 FRU_RSA.1 Maximální kvóty 102**
 - 15.3.7 FRU_RSA.2 Minimální a maximální kvóty 102**
- 16 Třída FTA: Přístup k TOE 103**
 - 16.1 Limitování rozsahu volitelných atributů (FTA_LSA) 103**
 - 16.1.1 Chování rodiny 103**
 - 16.1.2 Řazení komponent do úrovní 103**

16.1.3 Správa FTA_LSA.1 103

16.1.4 Audit FTA_LSA.1 104

16.1.5 FTA_LSA.1 Limitování rozsahu volitelných atributů 104

16.2 Limitování vícenásobných souběžných relací (FTA_MCS) 104

16.2.1 Chování rodiny 104

16.2.2 Řazení komponent do úrovní 104

Strana

16.2.3 Správa FTA_MCS.1 104

16.2.4 Správa FTA_MCS.2 104

16.2.5 Audit FTA_MCS.1, FTA_MCS.2 104

16.2.6 FTA_MCS.1 Základní limitování vícenásobných souběžných relací 104

16.2.7 FTA_MCS.2 Limitování vícenásobných souběžných relací na atribut uživatele 105

16.3 Uzamknutí a ukončení relace (FTA_SSL) 105

16.3.1 Chování rodiny 105

16.3.2 Řazení komponent do úrovní 105

16.3.3 Správa FTA_SSL.1 105

16.3.4 Správa FTA_SSL.2 105

16.3.5 Správa FTA_SSL.3 105

16.3.6 Správa FTA_SSL.4 105

16.3.7 Audit FTA_SSL.1, FTA_SSL.2 105

16.3.8 Audit FTA_SSL.3 106

16.3.9 Audit FTA_SSL.4 106

16.3.10 FTA_SSL.1 Uzamknutí relace iniciované TSF 106

16.3.11 FTA_SSL.2 Uzamknutí iniciované uživatelem 106

16.3.12 FTA_SSL.3 Ukončení iniciované TSF 106

16.3.13 FTA_SSL.4 Ukončení iniciované uživatelem 106

16.4 Upozornění při přístupu k TOE (FTA_TAB) 107

16.4.1 Chování rodiny 107

- 16.4.2** Řazení komponent do úrovní 107
- 16.4.3** Správa FTA_TAB.1 107
- 16.4.4** Audit FTA_TAB.1 107
- 16.4.5** FTA_TAB.1 Předdefinované upozornění pro přístup k TOE 107
- 16.5** Historie přístupu k TOE (FTA_TAH) 107
 - 16.5.1** Chování rodiny 107
 - 16.5.2** Řazení komponent do úrovní 107
 - 16.5.3** Správa FTA_TAH.1 107
 - 16.5.4** Audit FTA_TAH.1 107
 - 16.5.5** FTA_TAH.1 Historie přístupu k TOE 107
- 16.6** Ustavení relace TOE (FTA_TSE) 108
 - 16.6.1** Chování rodiny 108
 - 16.6.2** Řazení komponent do úrovní 108
 - 16.6.3** Správa FTA_TSE.1 108
 - 16.6.4** Audit FTA_TSE.1 108
 - 16.6.5** FTA_TSE.1 Ustavení relace TOE 108
- 17** Třída FTP: Důvěryhodná cesta/kanály 108
 - 17.1** Důvěryhodný kanál mezi TSF (FTP_ITC) 109
 - 17.1.1** Chování rodiny 109
 - 17.1.2** Řazení komponent do úrovní 109
 - 17.1.3** Správa FTP_ITC.1 109
 - 17.1.4** Audit FTP_ITC.1 109
 - 17.1.5** FTP_ITC.1 Důvěryhodný kanál mezi TSF 109
 - 17.2** Důvěryhodná cesta (FTP_TRP) 109
 - 17.2.1** Chování rodiny 109
 - 17.2.2** Řazení komponent do úrovní 110
 - 17.2.3** Správa FTP_TRP.1 110

17.2.4 Audit FTP_TRP.1 110

17.2.5 FTP_TRP.1 Důvěryhodná cesta 110

Příloha A (normativní) Aplikační poznámky týkající se bezpečnostních funkčních požadavků
111

A.1 Struktura poznámek 111

A.1.1 Struktura třídy 111

A.1.2 Struktura rodiny 111

A.1.3 Struktura komponenty 112

A.2 Tabulky závislostí 113

Příloha B (normativní) Funkční třídy, rodiny a komponenty 119

Příloha C (normativní) Třída FAU: Bezpečnostní audit 120

C.1 Požadavky auditu v distribuovaném prostředí 120

C.2 Automatická odezva bezpečnostního auditu (FAU_ARP) 121

C.2.1 Poznámky pro uživatele 121

C.2.2 FAU_ARP.1 Bezpečnostní alarmy 121

C.3 Generování dat bezpečnostního auditu (FAU_GEN) 122

C.3.1 Poznámky pro uživatele 122

C.3.2 FAU_GEN.1 Generování auditních dat 123

C.3.3 FAU_GEN.2 Přidružení identity k uživateli 123

C.4 Analýza bezpečnostního auditu (FAU_SAA) 123

C.4.1 Poznámky pro uživatele 123

C.4.2 FAU_SAA.1 Analýza potenciálního narušení 124

C.4.3 FAU_SAA.2 Detekce anomálie založená na profilu 124

C.4.4 FAU_SAA.3 Heuristika jednoduchého útoku 125

C.4.5 FAU_SAA.4 Heuristika komplexního útoku 125

C.5 Revize bezpečnostního auditu (FAU_SAR) 126

C.5.1 Poznámky pro uživatele 126

C.5.2 FAU_SAR.1 Revize auditu 127

- C.5.3** FAU_SAR.2 Omezená revize auditu 127
- C.5.4** FAU_SAR.3 Volitelná revize auditu 127
- C.6** Výběr událostí bezpečnostního auditu (FAU_SEL) 127
 - C.6.1** Poznámky pro uživatele 127
 - C.6.2** FAU_SEL.1 Selektivní audit 128
- C.7** Uchovávání událostí bezpečnostního auditu (FAU_STG) 128
 - C.7.1** Poznámky pro uživatele 128
 - C.7.2** FAU_STG.1 Chráněné uchovávání auditních záznamů 128
 - C.7.3** FAU_STG.2 Záruky dostupnosti auditních dat 128
 - C.7.4** FAU_STG.3 Akce v případě možné ztráty auditních dat 129
 - C.7.5** FAU_STG.4 Prevence ztráty auditních dat 129

Strana

Příloha D (normativní) Třída FCO: Komunikace 130

- D.1** Nepopiratelnost původu (FCO_NRO) 130
 - D.1.1** Poznámky pro uživatele 130
 - D.1.2** FCO_NRO.1 Selektivní prokázání původu 130
 - D.1.3** FCO_NRO.2 Prosazené prokázání původu 131
- D.2** Nepopiratelnost přijetí (FCO_NRR) 131
 - D.2.1** Poznámky pro uživatele 131
 - D.2.2** FCO_NRR.1 Selektivní prokázání přijetí 132
 - D.2.3** FCO_NRR.2 Prosazené prokázání přijetí 132

Příloha E (normativní) Třída FCS: Kryptografická podpora 134

- E.1** Správa kryptografických klíčů (FCS_CKM) 135
 - E.1.1** Poznámky pro uživatele 135
 - E.1.2** FCS_CKM.1 Generování kryptografických klíčů 135
 - E.1.3** FCS_CKM.2 Distribuce kryptografických klíčů 135
 - E.1.4** FCS_CKM.3 Přístup ke kryptografickým klíčům 136
 - E.1.5** FCS_CKM.4 Zničení kryptografických klíčů 136

E.2 Kryptografická operace (FCS_COP) 136

E.2.1 Poznámky pro uživatele 136

E.2.2 FCS_COP.1 Kryptografická operace 137

Příloha F (normativní) Třída FDP: Ochrana uživatelských dat 138

F.1 Politika řízení přístupu (FDP_ACC) 141

F.1.1 Poznámky pro uživatele 141

F.1.2 FDP_ACC.1 Řízení přístupu k podmnožině 141

F.2 Funkce řízení přístupu (FDP_ACF) 142

F.2.1 Poznámky pro uživatele 142

F.2.2 FDP_ACF.1 Řízení přístupu založené na bezpečnostních atributech 142

F.3 Autentizace dat (FDP_DAU) 143

F.3.1 Poznámky pro uživatele 143

F.3.2 FDP_DAU.1 Základní autentizace dat 143

F.3.3 FDP_DAU.2 Autentizace dat s identitou zaručitele 144

F.4 Export mimo oblast řízení TOE (FDP_ETC) 144

F.4.1 Poznámky pro uživatele 144

F.4.2 FDP_ETC.1 Export uživatelských dat bez bezpečnostních atributů 144

F.4.3 FDP_ETC.2 Export uživatelských dat s bezpečnostními atributy 144

F.5 Politika řízení toku informací (FDP_IFC) 145

F.5.1 Poznámky pro uživatele 145

F.5.2 FDP_IFC.1 Řízení toku informací podmnožiny 145

F.5.3 FDP_IFC.2.Úplné řízení toku informací 146

F.6 Funkce řízení toku informací (FDP_IFF) 146

F.6.1 Poznámky pro uživatele 146

F.6.2 FDP_IFF.1 Jednoduché bezpečnostní atributy 147

F.6.3 FDP_IFF.2 Hierarchické bezpečnostní atributy 147

F.6.4 FDP_IFF.3 Limitované nelegální toky informací 148

- F.6.5** FDP_IFF.4 Částečná eliminace nelegálních toků informací 149
- F.6.6** FDP_IFF.5 Žádné nelegální toky informací 149
- F.6.7** FDP_IFF.6 Monitorování nelegálních toků informací 149
- F.7** Import z oblasti mimo řízení TOE (FDP_ITC) 150
 - F.7.1** Poznámky pro uživatele 150
 - F.7.2** FDP_ITC.1 Import uživatelských dat bez bezpečnostních atributů 151
 - F.7.3** FDP_ITC.2 Import uživatelských dat s bezpečnostními atributy 151
- F.8** Přenos uvnitř TOE (FDP_ITT) 151
 - F.8.1** Poznámky pro uživatele 151
 - F.8.2** FDP_ITT.1 Základní ochrana vnitřního přenosu 152
 - F.8.3** FDP_ITT.2 Oddělení přenosu pomocí atributu 152
 - F.8.4** FDP_ITT.3 Monitorování integrity 152
 - F.8.5** FDP_ITT.4 Monitorování integrity založené na attributech 153
- F.9** Ochrana zbytkových informací (FDP_RIP) 153
 - F.9.1** Poznámky pro uživatele 153
 - F.9.2** FDP_RIP.1 Ochrana zbytkových informací podmnožiny 154
 - F.9.3** FDP_RIP.2 Úplná ochrana zbytkových informací 154
- F.10** Návrat zpracování (FDP_ROL) 154
 - F.10.1** Poznámky pro uživatele 154
 - F.10.2** FDP_ROL.1 Základní návrat zpracování 155
 - F.10.3** FDP_ROL.2 Progresivní návrat 155
- F.11** Integrita uchovávaných dat (FDP_SDI) 156
 - F.11.1** Poznámky pro uživatele 156
 - F.11.2** FDP_SDI.1 Monitorování integrity uchovávaných dat 156
 - F.11.3** FDP_SDI.2 Monitorování integrity uchovávaných dat a následná akce 156
- F.12** Ochrana důvěrnosti uživatelských dat při přenosu mezi TSF (FDP_UCT) 156
 - F.12.1** Poznámky pro uživatele 156
 - F.12.2** FDP_UCT.1 Důvěrnost výměny základních dat 156

F.13 Ochrana integrity uživatelských dat při přenosu mezi TSF (FDP_UIT) 157

F.13.1 Poznámky pro uživatele 157

F.13.2 FDP_UIT.1 Integrita výměny dat 157

F.13.3 FDP_UIT.2 Obnova při výměně zdrojových dat 157

F.13.4 FDP_UIT.3 Obnova při výměně cílových dat 158

Příloha G (normativní) Třída FIA: Identifikace a autentizace 159

G.1 Selhání autentizace (FIA_AFL) 160

G.1.1 Poznámky pro uživatele 160

G.1.2 FIA_AFL.1 Postupy v případě selhání autentizace 160

G.2 Definice uživatelských atributů (FIA_ATD) 161

G.2.1 Poznámky pro uživatele 161

G.2.2 FIA_ATD.1 Definice uživatelských atributů 161

G.3 Specifikace tajných informací (FIA_SOS) 162

G.3.1 Poznámky pro uživatele 162

G.3.2 FIA_SOS.1 Ověření tajných informací 162

Strana

G.3.3 FIA_SOS.2 Generování tajných informací funkcí TSF 162

G.4 Autentizace uživatele (FIA_UAU) 163

G.4.1 Poznámky pro uživatele 163

G.4.2 FIA_UAU.1.Načasování autentizace 163

G.4.3 FIA_UAU.2 Autentizace uživatele před jakoukoliv akcí 163

G.4.4 FIA_UAU.3 Nezfalšovatelná autentizace 163

G.4.5 FIA_UAU.4.Autentizační mechanismy s jedním použitím 163

G.4.6 FIA_UAU.5 Násobné autentizační mechanismy 164

G.4.7 FIA_UAU.6 Opakovaná autentizace 164

G.4.8 FIA_UAU.7 Chráněná zpětná vazba autentizace 165

G.5 Identifikace uživatele (FIA_UID) 165

G.5.1 Poznámky pro uživatele 165

G.5.2	FIA_UID.1 Načasování identifikace	165
G.5.3	FIA_UID.2 Identifikace uživatele před jakoukoliv akcí	165
G.6	Svázání uživatele se subjektem (FIA_USB)	165
G.6.1	Poznámky pro uživatele	165
G.6.2	FIA_USB.1 Svázání uživatele se subjektem	165
Příloha H	(normativní) Třída FMT: Správa bezpečnosti	167
H.1	Správa funkcí v TSF (FMT_MOF)	167
H.1.1	Poznámky pro uživatele	167
H.1.2	FMT_MOF.1 Správa chování bezpečnostních funkcí	168
H.2	Správa bezpečnostních atributů (FMT_MSA)	168
H.2.1	Poznámky pro uživatele	168
H.2.2	FMT_MSA.1 Správa bezpečnostních atributů	168
H.2.3	FMT_MSA.2 Bezpečné bezpečnostní atributy	169
H.2.4	FMT_MSA.3 Inicializace statických atributů	169
H.2.5	FMT_MSA.4 Převzetí hodnoty uživatelských atributů	170
H.3	Správa dat TSF (FMT_MTD)	170
H.3.1	Poznámky pro uživatele	170
H.3.2	FMT_MTD.1 Správa dat TSF	170
H.3.3	FMT_MTD.2 Správa limitů pro data TSF	171
H.3.4	FMT_MTD.3 Bezpečná data TSF	171
H.4	Revokace (FMT_REV)	171
H.4.1	Poznámky pro uživatele	171
H.4.2	FMT_REV.1 Revokace	171
H.5	Vypršení platnosti bezpečnostních atributů (FMT_SAE)	172
H.5.1	Poznámky pro uživatele	172
H.5.2	FMT_SAE.1 Časově limitovaná autorizace	172
H.6	Specifikace funkcí správy (FMT_SMF)	172
H.6.1	Poznámky pro uživatele	172

H.6.2 FMT_SMF.1 Specifikace funkcí správy 172

H.7 Role správy bezpečnosti (FMT_SMR) 173

H.7.1 Poznámky pro uživatele 173

Strana

H.7.2 FMT_SMR.1 Bezpečnostní role 173

H.7.3 FMT_SMR.2 Omezení kladená na bezpečnostní role 173

H.7.4 FMT_SMR.3 Přejímání rolí 173

Příloha I (normativní) Třída FPR: Soukromí 174

I.1 Anonymita (FPR_ANO) 175

I.1.1 Poznámky pro uživatele 175

I.1.2 FPR_ANO.1 Anonymita 175

I.1.3 FPR_ANO.2 Anonymita bez získání informací 175

I.2 Pseudonymita (FPR_PSE) 176

I.2.1 Poznámky pro uživatele 176

I.2.2 FPR_PSE.1 Pseudonymita 177

I.2.3 FPR_PSE.2 Reverzibilní pseudonymita 177

I.2.4 FPR_PSE.3 Pseudonymita alias 178

I.3 Nespojitelnost (FPR_UNL) 179

I.3.1 Poznámky pro uživatele 179

I.3.2 FPR_UNL.1 Nespojitelnost 179

I.4 Nepozorovatelnost (FPR_UNO) 180

I.4.1 Poznámky pro uživatele 180

I.4.2 FPR_UNO.1 Nepozorovatelnost 180

I.4.3 FPR_UNO.2 Alokace informací ovlivňujících nepozorovatelnost 181

I.4.4 FPR_UNO.3 Nepozorovatelnost bez získání informací 181

I.4.5 FPR_UNO.4 Pozorovatelnost ze strany autorizovaných uživatelů 182

Příloha J (normativní) Třída FPT: Ochrana TSF 183

J.1 Bezpečné selhání (FPT_FLS) 185

- J.1.1** Poznámky pro uživatele 185
- J.1.2** FPT_FLS.1 Selhání se zachováním bezpečného stavu 185
- J.2** Dostupnost exportovaných dat TSF (FPT_ITA) 185
 - J.2.1** Poznámky pro uživatele 185
 - J.2.2** FPT_ITA.1 Dostupnost mezi TSF v rámci definované metriky dostupnosti 185
- J.3** Důvěrnost exportovaných dat TSF (FPT_ITC) 185
 - J.3.1** Poznámky pro uživatele 185
 - J.3.2** FPT_ITC.1 Důvěrnost během přenosu mezi TSF 186
- J.4** Integrita exportovaných dat TSF (FPT_ITI) 186
 - J.4.1** Poznámky pro uživatele 186
 - J.4.2** FPT_ITI.1 Detekce modifikace mezi TSF 186
 - J.4.3** FPT_ITI.2 Detekce a korekce modifikace mezi TSF 186
- J.5** Přenos dat TSF uvnitř TOE (FPT_ITT) 187
 - J.5.1** Poznámky pro uživatele 187
 - J.5.2** Poznámky pro hodnotitele 187
 - J.5.3** FPT_ITT.1 Základní ochrana přenosu dat uvnitř TSF 187
 - J.5.4** FPT_ITT.2 Oddělení přenosu dat TSF 187
 - J.5.5** FPT_ITT.3 Monitorování integrity dat TSF 187
- J.6** Fyzická ochrana TSF (FPT_PHP) 188
 - J.6.1** Poznámky pro uživatele 188
 - J.6.2** FPT_PHP.1 Pasivní detekce fyzického útoku 188
 - J.6.3** FPT_PHP.2 Oznámení 188
 - J.6.4** FPT_PHP.3 Odolnost vůči fyzickému útoku 189
- J.7** Důvěryhodná obnova (FPT_RCV) 189
 - J.7.1** Poznámky pro uživatele 189
 - J.7.2** FPT_RCV.1 Ruční obnova 190
 - J.7.3** FPT_RCV.2 Automatická obnova 190

- J.7.4** FPT_RCV.3 Automatická obnova bez nepřiměřené ztráty 191
- J.7.5** FPT_RCV.4 Obnova funkce 191
- J.8** Detekce opakovaného přenosu (FPT_RPL) 192
 - J.8.1** Poznámky pro uživatele 192
 - J.8.2** FPT_RPL.1 Detekce opakovaného přenosu 192
- J.9** Protokol synchronizace stavu (FPT_SSP) 192
 - J.9.1** Poznámky pro uživatele 192
 - J.9.2** FPT_SSP.1 Jednoduché důvěryhodné potvrzení 192
 - J.9.3** FPT_SSP.2 Vzájemné důvěryhodné potvrzení 192
- J.10** Vyznačení času (FPT_STM) 193
 - J.10.1** Poznámky pro uživatele 193
 - J.10.2** FPT_STM.1 Spolehlivá vyznačení času 193
- J.11** Konzistence dat TSF mezi TSF (FPT_TDC) 193
 - J.11.1** Poznámky pro uživatele 193
 - J.11.2** FPT_TDC.1 Konzistence základních dat TSF mezi TSF 193
- J.12** Testování externích entit (FPT_TEE) 193
 - J.12.1** Poznámky pro uživatele 193
 - J.12.2** Poznámky pro hodnotitele 194
 - J.12.3** FPT_TEE.1 Testování externích entit 194
- J.13** Konzistence replikace dat TSF uvnitř TOE (FPT_TRC) 194
 - J.13.1** Poznámky pro uživatele 194
 - J.13.2** FPT_TRC.1 Konzistence uvnitř TSF 195
- J.14** Samotestování TSF (FPT_TST) 195
 - J.14.1** Poznámky pro uživatele 195
 - J.14.2** FPT_TST.1 Testování TSF 195
- Příloha K** (normativní) Třída FRU: Využití zdrojů 196
 - K.1** Tolerance k chybě (FRU_FLT) 196
 - K.1.1** Poznámky pro uživatele 196

- K.1.2** FRU_FLT.1 Snížená tolerance k chybě 196
- K.1.3** FRU_FLT.2 Limitovaná tolerance k chybě 197
- K.2** Priorita služby (FRU_PRS) 197
 - K.2.1** Poznámky pro uživatele 197
 - K.2.2** FRU_PRS.1 Limitovaná priorita služby 197
 - K.2.3** FRU_PRS.2 Úplná priorita služby 197
- K.3** Alokace zdrojů (FRU_RSA) 198
 - K.3.1** Poznámky pro uživatele 198

Strana

- K.3.2** FRU_RSA.1 Maximální kvóty 198
- K.3.3** FRU_RSA.2 Minimální a maximální kvóty 198
- Příloha L** (normativní) Třída FTA: Přístup k TOE 200
 - L.1** Limitování rozsahu volitelných atributů (FTA_LSA) 200
 - L.1.1** Poznámky pro uživatele 200
 - L.1.2** FTA_LSA.1 Limitování rozsahu volitelných atributů 201
 - L.2** Limitování násobných souběžných relací (FTA_MCS) 201
 - L.2.1** Poznámky pro uživatele 201
 - L.2.2** FTA_MCS.1 Základní limitování násobných souběžných relací 201
 - L.2.3** FTA_MCS.2 Limitování atributů uživatele u násobných souběžných relací 201
 - L.3** Uzamknutí a ukončení relace (FTA_SSL) 201
 - L.3.1** Poznámky pro uživatele 201
 - L.3.2** FTA_SSL.1 Uzamknutí relace iniciované TSF 202
 - L.3.3** FTA_SSL.2 Uzamknutí iniciované uživatelem 202
 - L.3.4** FTA_SSL.3 Ukončení iniciované TSF 202
 - L.3.5** FTA_SSL.4 Ukončení iniciované uživatelem 203
 - L.4** Upozornění při přístupu k TOE (FTA_TAB) 203
 - L.4.1** Poznámky pro uživatele 203
 - L.4.2** FTA_TAB.1 Předdefinovaná upozornění při přístupu k TOE 203

L.5 Historie přístupu k TOE (FTA_TAH) 203

L.5.1 Poznámky pro uživatele 203

L.5.2 FTA_TAH.1 Historie přístupu k TOE 203

L.6 Ustavení relace s TOE (FTA_TSE) 204

L.6.1 Poznámky pro uživatele 204

L.6.2 FTA_TSE.1 Ustavení relace TOE 204

Příloha M (normativní) Třída FTP: Důvěryhodná cesta/kanály 205

M.1 Důvěryhodný kanál mezi TSF (FTP_ITC) 205

M.1.1 Poznámky pro uživatele 205

M.1.2 FTP_ITC.1 Důvěryhodný kanál mezi TSF 205

M.2 Důvěryhodná cesta (FTP_TRP) 206

M.2.1 Poznámky pro uživatele 206

M.2.2 FTP_TRP.1 Důvěryhodná cesta 206

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, na jejichž základě 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, že vznikne problém, který se týká souboru, informujte o tom Ústřední sekretariát ISO na níže uvedené adrese.



DOKUMENT CHRÁNĚNÝ COPYRIGHTEM

© ISO 2008

Veškerá práva vyhrazena. Pokud není specifikováno jinak, nesmí být žádná část této publikace reprodukována nebo používána v jakékoliv 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

E-mail copyright@iso.org

Web www.iso.org

Published in Switzerland

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 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 % hlasujících národních orgánů.

Pozornost je věnována možnosti, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO a IEC nepřebírají zodpovědnost za identifikaci jakýchkoliv nebo všech takových patentových práv.

Mezinárodní norma ISO/IEC 15408-2 byla připravena společnou technickou komisí ISO/IEC JTC 1, Informační technologie, subkomisí 27, *Bezpečnostní techniky IT*. Identický text ISO/IEC 15408-2 je zveřejněn organizacemi sponzorujícími projekt Common Criteria pod názvem Společná kritéria pro hodnocení bezpečnosti informačních technologií. Společný zdroj XML pro obě publikace je uveden v <http://www.oc.ccn.cni.es/xml>.

Toto třetí vydání ruší a nahrazuje druhé vydání (ISO/IEC 15408-2:2005), které bylo technicky revidováno.

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 záruky bezpečnosti.*

PŘÁVNÍ POZNÁMKA:

Dále uvedené vládní organizace přispěly k vývoji této verze Společných kritérií pro hodnocení bezpečnosti informačních tecchnologií. Jako společní držitelé autorských práv dokumentu Společná kritéria pro hodnocení bezpečnosti informačních technologií, verze 3.1, část 1 až 3 (nazývaných „CC 3.1“) přidělují tímto organizaci ISO/IEC neexkluzivní licenci 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.

Australia/New Zealand: The Defence Signals Directorate and the
Government Communications Security Bureau
respectively;

Canada: Communications Security Establishment;

France: Direction Centrale de la Sécurité des Systemes d'Information;

Germany: Bundesamt für Sicherheit in der Informationstechnik;

Japan: Information Technology Promotion Agency;.

Netherlands: Netherlands national Communications Security Agency;

Spain: Ministerio de Administraciones Públicas and Centro Criptológico Nacional;

United Kingdom: Communications-Electronic Security Group;

United States: The National Security Agency and the National Institute of Standards and Technology

Úvod

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 (tj. vstupy, výstupy) s IT nebo odezvou IT 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, pracovníkům vývoje a hodnotitelům bezpečných produktů IT. Kapitola 5 ISO/IEC 15408-1 poskytuje další informace o cílových uživateli ISO/IEC 15408 a o použití ISO/IEC 15408 skupinami, které zahrnují tyto uživatele. Tyto skupiny mohou použít tuto část ISO/IEC 15408 následovně.

- a. Spotřebitelé, kteří používají při výběru komponent tuto část ISO/IEC 15408, aby vyjádřili funkční požadavky k uspokojení bezpečnostních cílů vyjádřených v PP nebo ST. ISO/IEC 15408-1 poskytuje podrobnější informace o vztahu mezi bezpečnostními cíli a bezpečnostními požadavky.
- b. Pracovníci vývoje, kteří odpovídají na aktuální nebo zaznamenané 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.
- c. 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.

1 Předmět normy

Tato část ISO/IEC 15408 definuje požadovanou strukturu a obsah bezpečnostních funkčních komponent pro účely hodnocení bezpečnosti. Obsahuje katalog funkčních komponent, které splňují

společné bezpečnostní funkční požadavky mnoha produktů IT.

Konec náhledu - text dále pokračuje v placené verzi ČSN.