DIN ISO/IEC 15408-2:2007-11 (E)

Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements (ISO/IEC 15408-2:2005); Text in English

Inhalt

Seite

Nationales Vorwort 6

Nationaler Anhang NA (informativ) **Begriffe** 7

Nationaler Anhang NB (informativ) **Symbole und Abkürzungen** 16

Nationaler Anhang NC (informativ) **Literaturhinweise** 17

Introduction 18

1 Scope 18

2 Normative references 18

3 Terms and definitions, symbols and abbreviated terms 18

4 Overview 19
4.1 Organisation of this part of ISO/IEC 15408 19

5 Functional requirements paradigm 19

6 Security functional components 24
6.1 Overview 24
6.2 Component catalogue 29

7 Class FAU: Security audit 30
7.1 Security audit automatic response (FAU_ARP) 31
7.2 Security audit data generation (FAU_GEN) 31
7.3 Security audit analysis (FAU_SAA) 33
7.4 Security audit review (FAU_SAR) 36
7.5 Security audit event selection (FAU_SEL) 37
7.6 Security audit event storage (FAU_STG) 38

8 Class FCO: Communication 41
8.1 Non-repudiation of origin (FCO_NRO) 41
8.2 Non-repudiation of receipt (FCO_NRR) 43

9 Class FCS: Cryptographic support 44
9.1 Cryptographic key management (FCS_CKM) 45
9.2 Cryptographic operation (FCS_COP) 47

10 Class FDP: User data protection 48
10.1 Access control policy (FDP_ACC) 51
10.2 Access control functions (FDP_ACF) 52
10.3 Data authentication (FDP_DAU) 53
10.4 Export to outside TSF control (FDP_ETC) 55
10.5 Information flow control policy (FDP_IFC) 56
10.6 Information flow control functions (FDP_IFF) 57
10.7 Import from outside TSF control (FDP_ITC) 62
10.8 Internal TOE transfer (FDP_ITT) 64
10.9 Residual information protection (FDP_RIP) 66
10.10 Rollback (FDP_ROL) 67
10.11 Stored data integrity (FDP_SDI) 69
10.12 Inter-TSF user data confidentiality transfer protection (FDP_UCT) 70
10.13 Inter-TSF user data integrity transfer protection (FDP_UIT) 71

11 Class FIA: Identification and authentication 73
11.1 Authentication failures (FIA_AFL) 74
11.2 User attribute definition (FIA_ATD) 75
11.3 Specification of secrets (FIA_SOS) 76
11.4 User authentication (FIA_UAU) 77
11.5 User identification (FIA_UID) 81

Seite

11.6 User-subject binding (FIA_USB) 82

12 Class FMT: Security management 83
12.1 Management of functions in TSF (FMT_MOF) 84
12.2 Management of security attributes (FMT_MSA) 85
12.3 Management of TSF data (FMT_MTD) 88
12.4 Revocation (FMT_REV) 90
12.5 Security attribute expiration (FMT_SAE) 91
12.6 Specification of Management Functions (FMT_SMF) 92
12.7 Security management roles (FMT_SMR) 92

13 Class FPR: Privacy 94
13.1 Anonymity (FPR_ANO) 95
13.2 Pseudonymity (FPR_PSE) 96
13.3 Unlinkability (FPR_UNL) 98
13.4 Unobservability (FPR_UNO) 99

14 Class FPT: Protection of the TSF 101
14.1 Underlying abstract machine test (FPT_AMT) 103
14.2 Fail secure (FPT_FLS) 103
14.3 Availability of exported TSF data (FPT_ITA) 104
14.4 Confidentiality of exported TSF data (FPT_ITC) 105
14.5 Integrity of exported TSF data (FPT_ITI) 106
14.6 Internal TOE TSF data transfer (FPT_ITT) 107
14.7 TSF physical protection (FPT_PHP) 109
14.8 Trusted recovery (FPT_RCV) 112
14.9 Replay detection (FPT_RPL) 114
14.10 Reference mediation (FPT_RVM) 115
14.11 Domain separation (FPT_SEP) 116
14.12 State synchrony protocol (FPT_SSP) 118
14.13 Time stamps (FPT_STM) 119
14.14 Inter-TSF TSF data consistency (FPT_TDC) 120
14.15 Internal TOE TSF data replication consistency (FPT_TRC) 121
14.16 TSF self test (FPT_TST) 121

15 Class FRU: Resource utilisation 123
15.1 Fault tolerance (FRU_FLT) 123
15.2 Priority of service (FRU_PRS) 124
15.3 Resource allocation (FRU_RSA) 125

16 Class FTA: TOE access 126
16.1 Limitation on scope of selectable attributes (FTA_LSA) 127
16.2 Limitation on multiple concurrent sessions (FTA_MCS) 128
16.3 Session locking (FTA_SSL) 129
16.4 TOE access banners (FTA_TAB) 131
16.5 TOE access history (FTA_TAH) 132
16.6 TOE session establishment (FTA_TSE) 133

17 Class FTP: Trusted path/channels 133
17.1 Inter-TSF trusted channel (FTP_ITC) 134
17.2 Trusted path (FTP_TRP) 135

Annex A (normative) **Security functional requirements application notes 137**
A.1 Structure of the notes 137
A.2 Dependency tables 139

Annex B (normative) **Functional classes, families, and components 146**

Annex C (normative) **Class FAU: Security audit 147**
C.1 Audit requirements in a distributed environment 147
C.2 Security audit automatic response (FAU_ARP) 148

Seite

C.3 Security audit data generation (FAU_GEN) ... 149
C.4 Security audit analysis (FAU_SAA) ... 151
C.5 Security audit review (FAU_SAR) ... 154
C.6 Security audit event selection (FAU_SEL) ... 156
C.7 Security audit event storage (FAU_STG) ... 156

Annex D (normative) **Class FCO: Communication ... 159**
D.1 Non-repudiation of origin (FCO_NRO) ... 159
D.2 Non-repudiation of receipt (FCO_NRR) ... 161

Annex E (normative) **Class FCS: Cryptographic support ... 164**
E.1 Cryptographic key management (FCS_CKM) ... 165
E.2 Cryptographic operation (FCS_COP) ... 167

Annex F (normative) **Class FDP: User data protection ... 169**
F.1 Access control policy (FDP_ACC) ... 173
F.2 Access control functions (FDP_ACF) ... 174
F.3 Data authentication (FDP_DAU) ... 176
F.4 Export to outside TSF control (FDP_ETC) ... 177
F.5 Information flow control policy (FDP_IFC) ... 178
F.6 Information flow control functions (FDP_IFF) ... 180
F.7 Import from outside TSF control (FDP_ITC) ... 184
F.8 Internal TOE transfer (FDP_ITT) ... 186
F.9 Residual information protection (FDP_RIP) ... 188
F.10 Rollback (FDP_ROL) ... 189
F.11 Stored data integrity (FDP_SDI) ... 191
F.12 Inter-TSF user data confidentiality transfer protection (FDP_UCT) ... 192
F.13 Inter-TSF user data integrity transfer protection (FDP_UIT) ... 192

Annex G (normative) **Class FIA: Identification and authentication ... 195**
G.1 Authentication failures (FIA_AFL) ... 196
G.2 User attribute definition (FIA_ATD) ... 197
G.3 Specification of secrets (FIA_SOS) ... 198
G.4 User authentication (FIA_UAU) ... 199
G.5 User identification (FIA_UID) ... 202
G.6 User-subject binding (FIA_USB) ... 203

Annex H (normative) **Class FMT: Security management ... 204**
H.1 Management of functions in TSF (FMT_MOF) ... 205
H.2 Management of security attributes (FMT_MSA) ... 206
H.3 Management of TSF data (FMT_MTD) ... 207
H.4 Revocation (FMT_REV) ... 209
H.5 Security attribute expiration (FMT_SAE) ... 210
H.6 Specification of Management Functions (FMT_SMF) ... 210
H.7 Security management roles (FMT_SMR) ... 210

Annex I (normative) **Class FPR: Privacy ... 213**
I.1 Anonymity (FPR_ANO) ... 214
I.2 Pseudonymity (FPR_PSE) ... 215
I.3 Unlinkability (FPR_UNL) ... 219
I.4 Unobservability (FPR_UNO) ... 220

Annex J (normative) **Class FPT: Protection of the TSF ... 224**
J.1 Underlying abstract machine test (FPT_AMT) ... 227
J.2 Fail secure (FPT_FLS) ... 228
J.3 Availability of exported TSF data (FPT_ITA) ... 228
J.4 Confidentiality of exported TSF data (FPT_ITC) ... 229
J.5 Integrity of exported TSF data (FPT_ITI) ... 229
J.6 Internal TOE TSF data transfer (FPT_ITT) ... 230
J.7 TSF physical protection (FPT_PHP) ... 231

J.8 Trusted recovery (FPT_RCV) 233
J.9 Replay detection (FPT_RPL) 236
J.10 Reference mediation (FPT_RVM) 237
J.11 Domain separation (FPT_SEP) 238
J.12 State synchrony protocol (FPT_SSP) 239
J.13 Time stamps (FPT_STM) 240
J.14 Inter-TSF TSF data consistency (FPT_TDC) 240
J.15 Internal TOE TSF data replication consistency (FPT_TRC) 241
J.16 TSF self test (FPT_TST) 242

Annex K (normative) **Class FRU: Resource utilisation 244**
K.1 Fault tolerance (FRU_FLT) 244
K.2 Priority of service (FRU_PRS) 245
K.3 Resource allocation (FRU_RSA) 246

Annex L (normative) **Class FTA: TOE access 249**
L.1 Limitation on scope of selectable attributes (FTA_LSA) 249
L.2 Limitation on multiple concurrent sessions (FTA_MCS) 250
L.3 Session locking (FTA_SSL) 251
L.4 TOE access banners (FTA_TAB) 252
L.5 TOE access history (FTA_TAH) 253
L.6 TOE session establishment (FTA_TSE) 253

Annex M (normative) **Class FTP: Trusted path/channels 255**
M.1 Inter-TSF trusted channel (FTP_ITC) 255
M.2 Trusted path (FTP_TRP) 256