DIN ISO/IEC 15408-3:2007-11 (E)

Information technology - Security techniques - Evaluation criteria for IT Security - Part 3: Security assurance requirements (ISO/IEC 15408-3:2005); Text in English

Inhalt

Seite

Nationales Vorwort 4

Nationaler Anhang NA (informativ) **Begriffe** 5

Nationaler Anhang NB (informativ) **Symbole und Abkürzungen** 14

Introduction 15

1 **Scope** 15

2 **Normative references** 15

3 **Terms and definitions, symbols and abbreviated terms** 15

4 **Overview** 16
4.1 **Organisation of this part of ISO/IEC 15408** 16

5 **ISO/IEC 15408 assurance paradigm** 16
5.1 **ISO/IEC 15408 philosophy** 16
5.2 **Assurance approach** 16
5.3 **ISO/IEC 15408 evaluation assurance scale** 18

6 **Security assurance requirements** 18
6.1 **Structures** 18
6.2 **Component taxonomy** 24
6.3 **Protection Profile and Security Target evaluation criteria class structure** 25
6.4 **Usage of terms in this part of ISO/IEC 15408** 25
6.5 **Assurance categorisation** 27
6.6 **Assurance class and family overview** 27

7 **Protection Profile and Security Target evaluation criteria** 31
7.1 **Overview** 31
7.2 **Protection Profile criteria overview** 32
7.3 **Security Target criteria overview** 33

8 **Class APE: Protection Profile evaluation** 34
8.1 **TOE description (APE_DES)** 34
8.2 **Security environment (APE_ENV)** 35
8.3 **PP introduction (APE_INT)** 36
8.4 **Security objectives (APE_OBJ)** 37
8.5 **IT security requirements (APE_REQ)** 38
8.6 **Explicitly stated IT security requirements (APE_SRE)** 40

9 **Class ASE: Security Target evaluation** 42
9.1 **TOE description (ASE_DES)** 43
9.2 **Security environment (ASE_ENV)** 43
9.3 **ST introduction (ASE_INT)** 44
9.4 **Security objectives (ASE_OBJ)** 45
9.5 **PP claims (ASE_PPC)** 46
9.6 **IT security requirements (ASE_REQ)** 47
9.7 **Explicitly stated IT security requirements (ASE_SRE)** 50
9.8 **TOE summary specification (ASE_TSS)** 51

10 **Evaluation assurance levels** 53
10.1 **Evaluation assurance level (EAL) overview** 54
10.2 **Evaluation assurance level details** 55
10.3 **Evaluation assurance level 1 (EAL1) – functionally tested** 55
10.4 **Evaluation assurance level 2 (EAL2) – structurally tested** 56
10.5 **Evaluation assurance level 3 (EAL3) – methodically tested and checked** 57
10.6 **Evaluation assurance level 4 (EAL4) – methodically designed, tested, and reviewed** 58
10.7 **Evaluation assurance level 5 (EAL5) – semiformally designed and tested** 59

10.8 Evaluation assurance level 6 (EAL6) – semiformally verified design and tested 60
10.9 Evaluation assurance level 7 (EAL7) – formally verified design and tested 61

11 Assurance classes, families, and components 63

12 Class ACM: Configuration management 63
12.1 CM automation (ACM_AUT) 63
12.2 CM capabilities (ACM_CAP) 66
12.3 CM scope (ACM_SCP) 74

13 Class ADO: Delivery and operation 77
13.1 Delivery (ADO_DEL) 77
13.2 Installation, generation and start-up (ADO_IGS) 79

14 Class ADV: Development 81
14.1 Functional specification (ADV_FSP) 85
14.2 High-level design (ADV_HLD) 89
14.3 Implementation representation (ADV_IMP) 96
14.4 TSF internals (ADV_INT) 99
14.5 Low-level design (ADV_LLD) 104
14.6 Representation correspondence (ADV_RCR) 109
14.7 Security policy modeling (ADV_SPM) 111

15 Class AGD: Guidance documents 115
15.1 Administrator guidance (AGD_ADM) 115
15.2 User guidance (AGD_USR) 117

16 Class ALC: Life cycle support 118
16.1 Development security (ALC_DVS) 118
16.2 Flaw remediation (ALC_FLR) 120
16.3 Life cycle definition (ALC_LCD) 124
16.4 Tools and techniques (ALC_TAT) 128

17 Class ATE: Tests 131
17.1 Coverage (ATE_COV) 131
17.2 Depth (ATE_DPT) 134
17.3 Functional tests (ATE_FUN) 137
17.4 Independent testing (ATE_IND) 140

18 Class AVA: Vulnerability assessment 144
18.1 Covert channel analysis (AVA_CCA) 145
18.2 Misuse (AVA_MSU) 149
18.3 Strength of TOE security functions (AVA_SOF) 154
18.4 Vulnerability analysis (AVA_VLA) 155

Annex A (informative) **Cross reference of assurance component dependencies 162**

Annex B (informative) **Cross reference of EALs and assurance components 166**