DIN EN 17640:2022-12 (E)

Fixed-time cybersecurity evaluation methodology for ICT products

Contents

Page

European foreword 4

Introduction 5

1 Scope 7

2 Normative references 7

3 Terms and definitions 7

4 Conformance 9

5 General concepts 11
5.1 Usage of this methodology 11
5.2 Knowledge of the TOE 12
5.3 Development process evaluation 12
5.4 Attack Potential 12
5.5 Knowledge building 13

6 Evaluation tasks 13
6.1 Completeness check 13
6.1.1 Aim 13
6.1.2 Evaluation method 13
6.1.3 Evaluator competence 13
6.1.4 Evaluator work units 13
6.2 FIT Protection Profile Evaluation 14
6.2.1 Aim 14
6.2.2 Evaluation method 14
6.2.3 Evaluator competence 14
6.2.4 Evaluator work units 14
6.3 Review of security functionalities 15
6.3.1 Aim 15
6.3.2 Evaluation method 15
6.3.3 Evaluator competence 15
6.3.4 Evaluator work units 15
6.4 FIT Security Target Evaluation 16
6.4.1 Aim 16
6.4.2 Evaluation method 16
6.4.3 Evaluator competence 16
6.4.4 Evaluator work units 16
6.5 Development documentation 17
6.5.1 Aim 17
6.5.2 Evaluation method 17
6.5.3 Evaluator competence 17
6.5.4 Work units 17
6.6 Evaluation of TOE Installation 17
6.6.1 Aim 17
6.6.2 Evaluation method 18
6.6.3 Evaluator competence 18
6.6.4 Evaluator work units 18
6.7 Conformance testing 18
6.7.1 Aim 18

6.7.2 Evaluation method 18
6.7.3 Evaluator competence 19
6.7.4 Evaluator work units 19
6.8 Vulnerability review 20
6.8.1 Aim 20
6.8.2 Evaluation method 20
6.8.3 Evaluator competence 21
6.8.4 Evaluator work units 21
6.9 Vulnerability testing 21
6.9.1 Aim 21
6.9.2 Evaluation method 22
6.9.3 Evaluator competence 22
6.9.4 Evaluator work units 22
6.10 Penetration testing 24
6.10.1 Aim 24
6.10.2 Evaluation method 24
6.10.3 Evaluator competence 25
6.10.4 Evaluator work units 25
6.11 Basic crypto analysis 26
6.11.1 Aim 26
6.11.2 Evaluation method 26
6.11.3 Evaluator competence 26
6.11.4 Evaluator work units 26
6.12 Extended crypto analysis 27
6.12.1 Aim 27
6.12.2 Evaluation method 27
6.12.3 Evaluator competence 28
6.12.4 Evaluator work units 28

Annex A (informative) Example for a structure of a FIT Security Target (FIT ST) 30

Annex B (normative) The concept of a FIT Protection Profile (FIT PP) 32

Annex C (informative) Acceptance Criteria 33

Annex D (informative) Guidance for integrating the methodology into a scheme 40

Annex E (informative) Parameters of the methodology and the evaluation tasks 45

Annex F (normative) Calculating the Attack Potential 47

Annex G (normative) Reporting the results of an evaluation 52

Bibliography 54