ISO/IEC TR 15443-1:2012-11 (E)

Information technology - Security techniques - Security assurance framework - Part 1: Introduction and concepts

Contents

Page

Foreword v

Introduction vi

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Abbreviated Terms 6

5 Concepts of security assurance 8
5.1 Security assurance 8
5.2 Assurance is distinguishable from confidence 9
5.3 The need for security assurance 9
5.4 Security assurance is intangible 10
5.5 Security assurance reduces security risk 10
5.6 Security assurance provided is related to the effort expended 10
5.7 Security assurance does not improve the product 11
5.8 Security assurance stakeholders 11
5.8.1 Those requiring confidence in SACA results 11
5.8.2 Approval and assurance authorities 11
5.9 Security assurance pervasiveness 12
5.9.1 Pass-through security assurance 14
5.9.2 Boundaries of deliverables 14
5.9.3 Transfer of deliverables 18
5.10 Organisational aspects of SACA 18

6 The structure of security assurance 19
6.1 Security assurance requirements specification 20
6.2 Security assurance cases 20
6.2.1 Developing a security assurance case 21
6.2.2 Communicating a security assurance case 21
6.3 Security assurance evidence 21
6.4 Security assurance claims 21
6.5 Security assurance arguments 22

7 SACA techniques 23
7.1 Techniques 23
7.1.1 Effectiveness (or evaluation) 24
7.1.2 Correctness (or conformance) 24
7.1.3 Predictive assurance 24
7.2 Selecting security assurance techniques 24
7.2.1 Optimisation considerations 25

8 SACA methods 26
8.1 Security Assurance Conformity Assessment (SACA) Methods 26
8.1.2 The composition of a security assurance conformance assessment method 27
8.1.3 Methods specific to security assurance 28
8.1.4 Methods not specific to security assurance 29

8.2 Approaches of SACA methods 29
8.2.1 Approach types 29
8.2.2 Combining approaches 30
8.3 Coverage of life cycle phases 31
8.3.1 Security assurance conformity assessors 32
8.3.2 Efficiency of a SACA method 32
8.4 The relationship between security criteria and assessment methods 33
8.5 Security assurance ratings 33
8.6 SACA tools 34
8.7 Outputs from the application of SACA methods 34

9 CASCO 35
9.1 Standards supporting conformity assessment 35

10 SACA Paradigms 36
10.1 SACA schemes 36
10.2 SACA conformity assessment bodies 37
10.2.1 Type A conformity assessments 37
10.2.2 Second party conformity assessment bodies 37
10.2.3 Third party conformity assessment bodies 38
10.3 Example models of SACA paradigms 38
10.3.1 Common Criteria 38
10.3.2 The Cryptographic Module Validation Program (CMVP) 39
10.3.3 The Payment Card Industry 40

11 Aspects of the composition of security assurance 41
11.1 Developing an assurance case in a compositional setting 42
11.1.1 General problems of composition 43
11.1.2 General aspects of composition re-use 43
11.1.3 Composition using different assurance techniques 44
11.2 Types of composition 44
11.2.1 Layering 44
11.2.2 Network 46
11.2.3 Component 48
11.3 Further activities 49

Bibliography 50