ISO/IEC TS 20540:2025-05 (E)

Information security, cybersecurity and privacy protection - Testing cryptographic modules in their field

Contents

Page

Foreword v

Introduction vi

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Abbreviated terms 5

5 Document organization 5

6 Developing, validating and field testing 6

7 Cryptographic modules 7
7.1 General 7
7.2 Types of cryptographic modules 7
7.2.1 General 7
7.2.2 Software module 8
7.2.3 Firmware module 8
7.2.4 Hardware module 8
7.2.5 Hybrid software module 8
7.2.6 Hybrid firmware module 8
7.3 Security requirements for cryptographic modules 9
7.3.1 General 9
7.3.2 Security level 1 9
7.3.3 Security level 2 10
7.3.4 Security level 3 10
7.3.5 Security level 4 11
7.4 Life-cycle assurance of cryptographic modules 11
7.5 Security policy of the module 12
7.5.1 General 12
7.5.2 Cryptographic module specification 12
7.5.3 Cryptographic module interfaces 12
7.5.4 Roles, services, and authentication 12
7.5.5 Software/firmware security 13
7.5.6 Operational environment 13
7.5.7 Physical security 13
7.5.8 Non-invasive security 13
7.5.9 Sensitive security parameters management 14
7.5.10 Self-tests 14
7.5.11 Life-cycle assurance 14
7.5.12 Mitigation of other attacks 14
7.6 Intended purpose or use of the validated cryptographic modules 15

8 Application environment 15
8.1 Organizational security 15
8.2 Architecture of the application environment 16
8.3 Application environments for the cryptographic modules 16

8.4 Security products with cryptographic modules 17

9 Field 18
9.1 Security requirements related to cryptographic modules for their field 18
9.1.1 General 18
9.1.2 Entropy sources 19
9.1.3 Audit mechanism 19
9.1.4 Physically unclonable function 19
9.2 Security assumptions for the field 19
9.2.1 General 19

9.2.2 Security level 1 19
9.2.3 Security level 2 20
9.2.4 Security level 3 21
9.2.5 Security level 4 21

10 How to select cryptographic modules 22
10.1 General 22
10.2 Use policy 23
10.3 Cryptographic module assurance 24
10.4 Interoperability 24
10.5 Selection of security rating for SSP protection 24

11 Principles for field testing 25
11.1 General 25
11.2 Assumptions 26
11.3 Field testing activities 26
11.4 Competence for field testers 27
11.5 Use of validated evidence 27
11.6 Documentations 27
11.7 Field testing procedure 27

12 Recommendations for field testing 28
12.1 General 28
12.2 Installation, configuration, and operation of the cryptographic module 28
12.2.1 General 28
12.2.2 Assessing installation of the cryptographic module 28
12.2.3 Assessing the configuration of the cryptographic module 29
12.2.4 Assessing the correct operation of the cryptographic module 30
12.3 Key management system 30
12.4 Security requirements of authentication credentials 31
12.5 Availability of cryptographic modules 32
12.6 Potential residual vulnerabilities of cryptographic modules 32
12.7 Security toolkit for the application system of cryptographic modules 33
12.8 Organization's security policies 33

13 Reporting the results of field testing 34

Annex A (informative) Examples of validated cryptographic modules lists 35

Annex B (informative) Security toolkit for application system of cryptographic modules in their field 36

Annex C (informative) Checklist for field testing of cryptographic modules 40

Bibliography 44