

ISO/IEC TS 20540:2018-05 (E)

Information technology - Security techniques - Testing cryptographic modules in their operational environment

| Contents | | Page |
|--------------------|---|-------------|
| Foreword | | v |
| Introduction | | vi |
| 1 | Scope | 1 |
| 2 | Normative references | 1 |
| 3 | Terms and definitions | 2 |
| 4 | Abbreviated terms | 5 |
| 5 | Document organization | 5 |
| 6 | Context of operational 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 | Cryptographic module application environments | 8 |
| 7.4 | Security products with cryptographic modules | 9 |
| 7.5 | Security requirements for cryptographic modules | 10 |
| 7.5.1 | General | 10 |
| 7.5.2 | Security Level 1 | 10 |
| 7.5.3 | Security Level 2 | 11 |
| 7.5.4 | Security Level 3 | 11 |
| 7.5.5 | Security Level 4 | 12 |
| 7.6 | Life-cycle assurance of cryptographic modules | 12 |
| 7.7 | Cryptographic module security policy | 12 |
| 7.7.1 | General | 12 |
| 7.7.2 | Cryptographic module specification | 13 |
| 7.7.3 | Cryptographic module interfaces | 13 |
| 7.7.4 | Roles, services, and authentication | 13 |
| 7.7.5 | Software/firmware security | 13 |
| 7.7.6 | Operational environment | 14 |
| 7.7.7 | Physical security | 14 |
| 7.7.8 | Non-invasive security | 14 |
| 7.7.9 | Sensitive security parameters management | 14 |
| 7.7.10 | Self-tests | 14 |
| 7.7.11 | Life-cycle assurance | 15 |
| 7.7.12 | Mitigation of other attacks | 15 |
| 7.8 | Intended purpose of validated cryptographic modules | 15 |
| 8 | The application environment | 16 |
| 8.1 | Organizational security | 16 |

| | | |
|--------|--|----|
| 8.2 | Architecture of the application environment | 16 |
| 9 | The operational environment | 17 |
| 9.1 | Security requirements related to cryptographic modules for their operational environment | 17 |
| 9.1.1 | General | 17 |
| 9.1.2 | Entropy sources | 17 |
| 9.1.3 | Audit mechanism | 17 |
| 9.1.4 | Physically unclonable function | 17 |
| 9.2 | Security assumptions for the operational environment | 17 |
| 9.2.1 | General | 17 |
| 9.2.2 | Security Level 1 | 18 |
| 9.2.3 | Security Level 2 | 18 |
| 9.2.4 | Security Level 3 | 19 |
| 9.2.5 | Security Level 4 | 20 |
| 10 | How to select cryptographic modules | 21 |
| 10.1 | General | 21 |
| 10.2 | Use policy | 21 |
| 10.3 | Cryptographic module assurance | 23 |
| 10.4 | Interoperability | 23 |
| 10.5 | Selection of security rating for SSP protection | 23 |
| 11 | Principles for operational testing | 23 |
| 11.1 | General | 23 |
| 11.2 | Assumptions | 24 |
| 11.3 | Operational testing activities | 24 |
| 11.4 | Competence for operational testers | 25 |
| 11.5 | Use of validated evidence | 25 |
| 11.6 | Documentation | 25 |
| 11.7 | Operational testing procedure | 26 |
| 12 | Recommendations for operational testing | 26 |
| 12.1 | General | 26 |
| 12.2 | Recommendations for assessing the installation, configuration, and operation of the cryptographic module | 26 |
| 12.2.1 | General | 26 |
| 12.2.2 | Assessing installation of the cryptographic module | 27 |
| 12.2.3 | Assessing the configuration of the cryptographic module | 27 |
| 12.2.4 | Assessing the correct operation of the cryptographic module | 29 |
| 12.3 | Recommendations for inspecting a key management system | 29 |
| 12.4 | Recommendations for inspecting the security requirements of authentication credentials | 30 |
| 12.5 | Recommendations for assessing the availability of cryptographic modules | 31 |
| 12.6 | Recommendations for identifying potential residual vulnerabilities of cryptographic modules | 31 |
| 12.7 | Checking for the organization's security policies | 32 |
| 13 | Reporting the results of operational testing | 33 |
| | Annex A (informative) Examples of validated cryptographic modules lists | 34 |
| | Annex B (informative) Checklist for operational testing of cryptographic modules | 35 |
| | Bibliography | 39 |