ISO/IEC 24759:2025-02 (E)

Information security, cybersecurity and privacy protection - Test requirements for cryptographic modules

Contents

Page

Foreword v

Introduction vi

1 Scope 1

2 Normative references 1

3 Termsanddefinitions 1

4 Symbols and abbreviated terms 2

5 Document organization 2
5.1 General 2
5.2 Assertions and security requirements 3
5.3 Assertions with cross references 3

6 Security requirements 4
6.1 General 4
6.2 Cryptographic module specification 5
6.2.1 Cryptographic module specification general requirements 5
6.2.2 Types of cryptographic modules 5
6.2.3 Cryptographic boundary 6
6.2.4 Module operations 16
6.3 Cryptographic module interfaces 23
6.3.1 Cryptographic module interfaces general requirements 23
6.3.2 Categories of interfaces 26
6.3.3 Plaintext trusted path 35
6.3.4 Protected internal paths 38
6.4 Roles, services, and authentication 39
6.4.1 Roles, services, and authentication general requirements 39
6.4.2 Roles 40
6.4.3 Services 41
6.4.4 Authentication 49
6.5 Software/firmware security 59
6.5.1 Software/firmware security general requirements 59
6.5.2 Security level 1 62
6.5.3 Security level 2 67
6.5.4 Security levels 3 and 4 68
6.6 Operational environment 69
6.6.1 Operational environment general requirements 69
6.6.2 Clause applicability 70
6.6.3 Operating system requirements for modifiable operational environments 71
6.7 Physical security 83
6.7.1 Physical security embodiments 83
6.7.2 Physical security general requirements 84
6.7.3 Physical security requirements for each physical security embodiment 95
6.7.4 Environmental failure protection/testing 100
6.7.5 Environmental failure protection features 100
6.7.6 Environmental failure testing procedures 101
6.8 Non-invasive security 104
6.8.1 Non-invasive security general requirements 104

6.8.2 Security levels 1 and 2 104
6.8.3 Security level 3 105
6.8.4 Security level 4 105
6.9 Sensitive security parameter management 106
6.9.1 Sensitive security parameter management general requirements 106
6.9.2 Random bit generators 108
6.9.3 Sensitive security parameter generation 110
6.9.4 Automated sensitive security parameter establishment 110

6.9.5 Sensitive security parameter entry and output 111
6.9.6 Sensitive security parameter storage 117
6.9.7 Sensitive security parameter zeroization 118
6.10 Self-tests 122
6.10.1 Self-test general requirements 122
6.10.2 Security levels 3 and 4 126
6.10.3 Pre-operational self-tests 127
6.10.4 Conditional self-tests 130
6.11 Life-cycle assurance 143
6.11.1 Life-cycle assurance general requirements 143
6.11.2 Configuration management 143
6.11.3 Design 145
6.11.4 Finite state model 145
6.11.5 Development 149
6.11.6 Vendor testing 155
6.11.7 Delivery and operation 157
6.11.8 Guidance documents 160
6.12 Mitigation of other attacks 161
6.12.1 Mitigation of other attacks general requirements 161
6.12.2 Security levels 1, 2 and 3 161
6.12.3 Security level 4 161

7 Documentation requirements 162
7.1 Purpose 162
7.2 Items 163
7.2.1 Cryptographic module specification 163
7.2.2 Cryptographic module interfaces 164
7.2.3 Roles, services, and authentication 164
7.2.4 Software/Firmware security 165
7.2.5 Operational environment 165
7.2.6 Physical security 166
7.2.7 Non-invasive security 167
7.2.8 Sensitive security parameter management 167
7.2.9 Self-tests 169
7.2.10 Life-cycle assurance 169
7.2.11 Mitigation of other attacks 171

8 Cryptographic module security policy 172
8.1 General 172
8.2 Items 173
8.2.1 General 173
8.2.2 Cryptographic module specification 174
8.2.3 Cryptographic module interfaces 175
8.2.4 Roles, services, and authentication 175
8.2.5 Software/Firmware security 176
8.2.6 Operational environment 177
8.2.7 Physical security 178
8.2.8 Non-invasive security 179
8.2.9 Sensitive security parameters management 179
8.2.10 Self-tests 180
8.2.11 Life-cycle assurance 180
8.2.12 Mitigation of other attacks 181

Bibliography 182