ISO/IEC 24759:2014-02 (E)

Information technology - Security techniques - Test requirements for cryptographic modules

Contents

Page

Foreword v

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Symbols and abbreviated terms 1

5 Document organization 1
5.1 General 1
5.2 Assertions and security requirements 1

6 Security requirements 2
6.1 General 2
6.2 Cryptographic module specification 3
6.2.1 Cryptographic module specification general requirements 3
6.2.2 Types of cryptographic modules 3
6.2.3 Cryptographic boundary 5
6.2.4 Modes of operations 13
6.3 Cryptographic module interfaces 17
6.3.1 Cryptographic module interfaces general requirements 17
6.3.2 Types of interfaces 20
6.3.3 Definition of interfaces 20
6.3.4 Trusted channel 29
6.4 Roles, services, and authentication 31
6.4.1 Roles, services, and authentication general requirements 31
6.4.2 Roles 32
6.4.3 Services 33
6.4.4 Authentication 41
6.5 Software/Firmware security 49
6.6 Operational environment 56
6.6.1 Operational environment general requirements 56
6.6.2 Operating system requirements for limited or non-modifiable operational environments 57
6.6.3 Operating system requirements for modifiable operational environments 57
6.7 Physical security 67
6.7.1 Physical security embodiments 67
6.7.2 Physical security general requirements 68
6.7.3 Physical security requirements for each physical security embodiment 74
6.7.4 Environmental failure protection/testing 85
6.8 Non-invasive security 88
6.9 Sensitive security parameter management 90
6.9.1 Sensitive security parameter management general requirements 90
6.9.2 Random bit generators 92
6.9.3 Sensitive security parameter generation 92
6.9.4 Sensitive security parameter establishment 93
6.9.5 Sensitive security parameter entry and output 94
6.9.6 Sensitive security parameter storage 98
6.9.7 Sensitive security parameter zeroisation 98
6.10 Self-tests 101

6.10.1 Self-test general requirements 101
6.10.2 Pre-operational self-tests 105
6.10.3 Conditional self-tests 108
6.11 Life-cycle assurance 118
6.11.1 Life-cycle assurance general requirements 118
6.11.2 Configuration management 119
6.11.3 Design 120
6.11.4 Finite state model 120
6.11.5 Development 124
6.11.6 Vendor testing 129
6.11.7 Delivery and operation 129
6.11.8 End of life 130
6.11.9 Guidance documents 131
6.12 Mitigation of other attacks 132
6.A Documentation requirements 133
6.B Cryptographic module security policy 133
6.C Approved security functions 134
6.D Approved sensitive security parameter generation and establishment methods 134
6.E Approved authentication mechanisms 134
6.F Approved non-invasive attack mitigation test metrics 135