

ISO/IEC 24759:2008-07 (E)

Information technology - Security techniques - Test requirements for cryptographic modules

Contents		Page
Foreword		iv
1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Abbreviated terms	4
5	Document Organization	5
5.1	General	5
5.2	Assertions and security requirements	5
5.3	Assertions with cross references	6
6	Security requirements	6
6.1	General test requirements	6
6.2	Cryptographic module specification	6
6.3	Cryptographic module ports and interfaces	14
6.4	Roles, services, and authentication	27
6.4.1	Roles	27
6.4.2	Services	28
6.4.3	Operator authentication	30
6.5	Finite state model	35
6.6	Physical security	39
6.6.1	General physical security requirements	39
6.6.2	Environmental failure protection/testing	55
6.7	Operational environment	57
6.8	Cryptographic key management	66
6.8.1	Random bit generators (RBGs)	67
6.8.2	Key generation	68
6.8.3	Key establishment	70
6.8.4	Key entry and output	71
6.8.5	Key storage	75
6.8.6	Key zeroisation	75
6.9	Self-tests	76
6.9.1	Power-up tests	79
6.9.2	Conditional tests	85
6.10	Design assurance	91
6.10.1	Configuration management	91
6.10.2	Delivery and operation	94
6.10.3	Development	95
6.10.4	Guidance documents	100
6.11	Mitigation of other attacks	101
6.12	Documentation requirements	102
6.13	Cryptographic module security policy	102
6.14	Approved protection profiles	103
6.15	Approved security functions	103
6.16	Approved key establishment methods	103
6.17	Recommended software development practices	103
6.18	Examples of mitigation of other attacks	103