

# ISO/IEC 19790:2006-03 (E)

## Information technology - Security techniques - Security requirements for cryptographic modules

---

<b>Contents</b>		<b>Page</b>
Foreword .....		iv
Introduction .....		v
1	Scope .....	1
2	Normative references .....	1
3	Terms and definitions .....	1
4	Abbreviated terms .....	9
5	Cryptographic module security levels .....	9
5.1	Security Level 1 .....	10
5.2	Security Level 2 .....	10
5.3	Security Level 3 .....	10
5.4	Security Level 4 .....	11
6	Functional security objectives .....	11
7	Security requirements .....	12
7.1	Cryptographic module specification .....	14
7.2	Cryptographic module ports and interfaces .....	15
7.3	Roles, services, and authentication .....	16
7.4	Finite state model .....	18
7.5	Physical security .....	19
7.6	Operational environment .....	26
7.7	Cryptographic key management .....	29
7.8	Self-tests .....	31
7.9	Design assurance .....	34
7.10	Mitigation of other attacks .....	36
Annex A (normative) Documentation requirements .....		38
Annex B (normative) Cryptographic module security policy .....		42
Annex C (normative) Approved protection profiles .....		44
Annex D (informative) Approved security functions .....		45
Annex E (informative) Approved key establishment methods .....		47
Annex F (informative) Recommended software development practices .....		48
Annex G (informative) Examples of mitigation of other attacks .....		50
Bibliography .....		51