

# ISO 11568-1:2005-06 (E)

## Banking - Key management (retail) - Part 1: Principles

---

<b>Contents</b>		<b>Page</b>
Foreword .....		iv
Introduction .....		v
1	Scope .....	1
2	Normative references .....	1
3	Terms and definitions .....	2
4	Aspects of key management .....	3
4.1	Purpose of security .....	3
4.2	Level of security .....	3
4.3	Key management objectives .....	3
5	Principles of key management .....	3
6	Cryptosystems .....	4
6.1	Overview .....	4
6.2	Cipher systems .....	4
6.3	Symmetric cipher systems .....	4
6.4	Asymmetric cipher systems .....	5
6.5	Other cryptosystems .....	5
7	Physical security for cryptographic environments .....	6
7.1	Physical security considerations .....	6
7.2	Secure cryptographic device .....	6
7.3	Physically secure environment .....	6
8	Security considerations .....	7
8.1	Cryptographic environments for secret/private keys .....	7
8.2	Cryptographic environments for public keys .....	7
8.3	Protection against counterfeit devices .....	7
9	Key management services for cryptosystems .....	7
9.1	General .....	7
9.2	Separation .....	7
9.3	Substitution prevention .....	7
9.4	Identification .....	7
9.5	Synchronization (availability) .....	8
9.6	Integrity .....	8
9.7	Confidentiality .....	8
9.8	Compromise detection .....	8
10	Key life cycles .....	8
10.1	General .....	8
10.2	Common requirements for key life cycles .....	8
10.3	Additional requirements for asymmetric cryptosystems .....	9
Annex A (normative)	Procedure for approval of additional cryptographic algorithms .....	10
Annex B (informative)	Example of a retail banking environment .....	12
Annex C (informative)	Examples of threats in the retail banking environment .....	14
Bibliography .....		16