

# ISO 11568-4:2007-07 (E)

## Banking - Key management (retail) - Part 4: Asymmetric cryptosystems - Key management and life cycle

---

<b>Contents</b>		<b>Page</b>
Foreword .....		iv
Introduction .....		v
1	Scope .....	1
2	Normative references .....	1
3	Terms and definitions .....	2
4	Uses of asymmetric cryptosystems in retail financial services systems .....	3
4.1	General .....	3
4.2	Establishment and storage of symmetric keys .....	4
4.3	Storage and distribution of asymmetric public keys .....	4
4.4	Storage and transfer of asymmetric private keys .....	4
5	Techniques for the provision of key management services .....	4
5.1	Introduction .....	4
5.2	Key encipherment .....	4
5.3	Public key certification .....	5
5.4	Key separation techniques .....	6
5.5	Key verification .....	6
5.6	Key integrity techniques .....	7
6	Asymmetric key life cycle .....	8
6.1	Key life cycle phases .....	8
6.2	Key life cycle stages -- Generation .....	9
6.3	Key storage .....	12
6.4	Public key distribution .....	14
6.5	Asymmetric key pair transfer .....	14
6.6	Authenticity prior to use .....	16
6.7	Use .....	17
6.8	Public key revocation .....	17
6.9	Replacement .....	18
6.10	Public key expiration .....	18
6.11	Private key destruction .....	18
6.12	Private key deletion .....	19
6.13	Public key archive .....	19
6.14	Private key termination .....	19
6.15	Erasure summary .....	20
6.16	Optional life cycle processes .....	20
Annex A (normative) Approved algorithms .....		21
Bibliography .....		22