# ISO 11568-2:2012-02 (E)

## Financial services - Key management (retail) - Part 2: Symmetric ciphers, their key management and life cycle

## Contents

Page


Foreword ..... iv

Introduction ..... v

1 Scope ..... 1

2 Normative references ..... 1

3 Termsanddefinitions ..... 1

4 General environment for key management techniques ..... 4
4.1 General ..... 4
4.2 Functionality of a secure cryptographic device ..... 4
4.3 Key generation ..... 5
4.4 Key calculation (variants) ..... 6
4.5 Key hierarchies ..... 6
4.6 Key life cycle ..... 7
4.7 Key storage ..... 9
4.8 Key restoration from back-up ..... 10
4.9 Key distribution and loading ..... 10
4.10 Key use ..... 11
4.11 Key cryptoperiod ..... 11
4.12 Key replacement ..... 12
4.13 Key destruction ..... 12
4.14 Key deletion ..... 12
4.15 Key archive ..... 13
4.16 Key termination ..... 13

5 Techniques for the provision of key management services ..... 13
5.1 General ..... 13
5.2 Key encipherment ..... 13
5.3 Key variants ..... 13
5.4 Key derivation ..... 14
5.5 Key transformation ..... 14
5.6 Key offsetting ..... 15
5.7 Key notarization ..... 16
5.8 Key tagging ..... 16
5.9 Keyverification ..... 18
5.10 Keyidentification ..... 18
5.11 Controls and audit ..... 19
5.12 Key integrity ..... 19

6 Symmetric key life cycle ..... 20
6.1 General ..... 20
6.2 Key generation ..... 20
6.3 Key storage ..... 20
6.4 Key restoration from back-up ..... 21
6.5 Key distribution and loading ..... 21
6.6 Key use ..... 23
6.7 Key replacement ..... 23
6.8 Key destruction, deletion, archive and termination ..... 23

**7 Key management services cross-reference ..... 24**

**Annex B (normative) Approved algorithms for symmetric key management ..... 27**

**Annex C (normative) Abbreviations ..... 28**

**Bibliography ..... 29**