ISO 9564-1:2002-04 (E)

Banking - Personal Identification Number (PIN) management and security - Part 1: Basic principles and requirements for online h andling in ATM and POS systems

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Normative references 1

3 Terms and definitions 2

4 Basic principles of PIN management 4

5 PIN entry devices 5
5.1 Character set 5
5.2 Character representation 5
5.3 PIN entry 5
5.4 Packaging considerations 5

6 PIN security issues 6
6.1 PIN control requirements 6
6.2 PIN encipherment 7
6.3 Physical security 7

7 Techniques for management/protection of account-related PIN functions 8
7.1 PIN length 8
7.2 PIN selection 8
7.3 PIN issuance and delivery 9
7.4 PIN change 10
7.5 Disposal of waste material and returned PIN mailers 11
7.6 PIN activation 11
7.7 PIN storage 11
7.8 PIN deactivation 12

8 Techniques for management/protection of transaction-related PIN functions 12
8.1 PIN entry 12
8.2 Protection of PIN during transmission 12
8.3 Standard PIN block formats 12
8.4 Other PIN block formats 16
8.5 PIN verification 16
8.6 Journalizing of transactions containing PIN data 16

9 Approval procedure for encipherment algorithms 16

Annex A (informative) General principles of key management 17

Annex B (informative) PIN verification techniques 20

Annex C (informative) PIN entry device for online PIN encipherment 22

Annex D (informative) Example of pseudo-random PIN generation 24

Annex E (informative) Additional guidelines for the design of a PIN entry device 25

Annex F (informative) Guidance on clearing and destruction procedures for sensitive data 28

Annex G (informative) Information for customers 30