ISO 9564-1:2011-02 (E)

Financial services - Personal Identification Number (PIN) management and security - Part 1: Basic principles and requirements f or PINs in card-based 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 5
4.1 General 5
4.2 Principles 5

5 PIN handling devices 6
5.1 PIN handling device security requirements 6
5.2 Physical security for IC readers 7
5.3 PIN entry device characteristics 7

6 PIN security issues 7
6.1 PIN control requirements 7
6.2 PIN encipherment 8

7 PIN verification 9
7.1 General 9
7.2 Online PIN verification 9
7.3 Offline PIN verification 9

8 Techniques for management/protection of account-related PIN functions 9
8.1 PIN length 9
8.2 PIN establishment 9
8.3 PIN issuance and delivery to the cardholder 10
8.4 PIN selection 10
8.5 PIN change 11
8.6 PIN replacement 12
8.7 Disposal of waste material and returned PIN mailers 12
8.8 PIN activation 13
8.9 PIN storage 13
8.10 PIN deactivation 13
8.11 PIN mailers 14

9 Techniques for management/protection of transaction-related PIN functions 14
9.1 PIN entry 14
9.2 Protection of PIN during transmission 14
9.3 Compact PIN block formats 17
9.4 Extended PIN blocks 22
9.5 Journalizing of transactions containing PIN data 22

10 Approval procedure for encipherment algorithms 22

Annex A (normative) Destruction of sensitive data 23

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

Annex C (informative) Information for customers 28

Bibliography 29