ISO 9564-1:2017-11 (E)

Financial services - Personal Identification Number (PIN) management and security - Part 1: Basic p rinciples and requirements for PINs in card-based systems

Contents

Page

Foreword v

Introduction vi

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
5.3.1 Character set 7
5.3.2 Character representation 7

6 PIN security issues 7
6.1 PIN control requirements 7
6.1.1 PIN processing systems 7
6.1.2 Recording media 8
6.1.3 Oral communications 8
6.1.4 Telephone keypads 8
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
8.2.1 PIN establishment techniques 9
8.2.2 Assigned derived PIN 9
8.2.3 Assigned random PIN 10
8.2.4 Customer-selected PIN 10
8.3 PIN issuance and delivery to the cardholder 10
8.4 PIN selection 10
8.4.1 General 10
8.4.2 PIN conveyance 10
8.4.3 PIN selection at an issuer's location 11
8.4.4 PIN selection by mail 11
8.5 PIN change 11
8.5.1 General 11
8.5.2 PIN change in an interchange environment 11
8.5.3 PIN change at an attended terminal 11

8.5.4 PIN change at an unattended terminal 12
8.5.5 PIN change by mail 12
8.6 PIN replacement 12
8.6.1 Replacement of forgotten PIN 12
8.6.2 Re-advice of forgotten PIN 12
8.6.3 Replacement of compromised PIN 12
8.7 Disposal of waste material and returned PIN mailers 12
8.8 PIN activation 12
8.9 PIN storage 13
8.10 PIN deactivation 13
8.11 PIN mailers 13

9 Techniques for management/protection of transaction-related PIN functions 14
9.1 PIN entry 14
9.2 Protection of PIN during transmission 14
9.2.1 PIN protection during transmission to the issuer for online PIN verification 14
9.2.2 PIN protection during conveyance to the ICC for offline PIN verification 15
9.3 Compact PIN block formats 17
9.3.1 PIN block construction and format value assignment 17
9.3.2 Format 0 PIN block 17
9.3.3 Format 1 PIN block 18
9.3.4 Format 2 PIN block 18
9.3.5 Format 3 PIN block 19
9.3.6 Compact PIN block usage restrictions 20
9.4 Extended PIN blocks 21
9.4.1 General 21
9.4.2 Format 4 PIN block 21
9.5 PIN block format translation restrictions 25
9.6 Journalizing of transactions containing PIN data 25

Annex A (normative) Destruction of sensitive data 26

Annex B (informative) Additional guidelines for the design of a PIN entry device 28

Annex C (informative) Information for customers 31

Bibliography 32