ISO 9564-2:2025-08 (E)

Financial services - Personal Identification Number (PIN) management and security - Part 2: Approved algorithms for PIN encipherment

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 General 1

5 Triple data encryption algorithm (TDEA) 2
5.1 Definition of the TDEA algorithm 2
5.2 Use of the TDEA algorithm 2

6 RSA encryption algorithm 2
6.1 Definition of the RSA algorithm 2
6.2 Use of the RSA algorithm 2

7 AES encryption algorithm 2
7.1 Definition of the AES algorithm 2
7.2 Use of the AES algorithm 2

8 SM4 encryption algorithm 2
8.1 Definition of the SM4 algorithm 2
8.2 Use of the SM4 algorithm 3

9 ECIES algorithm 3
9.1 Definition of the ECIES algorithm 3
9.2 Use of the ECIES algorithm 3

Annex A (informative) Using key encapsulation mechanisms for establishment of ephemeral PIN encryption keys 4

Bibliography 13