ISO 9564-2:2014-08 (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 Triple Data Encryption Algorithm (TDEA) 1
3.1 Definition of the TDEA algorithm 1
3.2 Use of the TDEA algorithm 1

4 RSA encryption algorithm 1
4.1 Definition of the RSA algorithm 1
4.2 Use of the RSA algorithm 2

5 AES encryption algorithm 2
5.1 Definition of the AES algorithm 2
5.2 Use of the AES algorithm 2