American National Standard for Financial Services

X9.8–2003

BANKING - PERSONAL IDENTIFICATION NUMBER MANAGEMENT AND SECURITY

Part 1: PIN protection principles and techniques for online PIN verification in ATM & POS systems

Secretariat:
Accredited Standards Committee X9, Inc.

Approved: March 21, 2003

American National Standards Institute
Foreward

Approval of an American National Standard requires verification by ANSI that the requirements for due process, consensus, and other criteria for approval have been met by the standards developer.

Consensus is established when, in the judgment of the ANSI Board of Standards Review, substantial agreement has been reached by directly and materially affected interests. Substantial agreement means much more than a simple majority, but not necessarily unanimity. Consensus requires that all views and objections be considered, and that a concerted effort be made toward their resolution.

The use of American National Standards is completely voluntary; their existence does not in any respect preclude anyone, whether he has approved the standards or not from manufacturing, marketing, purchasing, or using products, processes, or procedures not conforming to the standards.

The American National Standards Institute does not develop standards and will in no circumstances give an interpretation of any American National Standard. Moreover, no person shall have the right or authority to issue an interpretation of an American National Standard in the name of the American National Standards Institute. Requests for interpretations should be addressed to the secretariat or sponsor whose name appears on the title page of this standard.

CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time. The procedures of the American National Standards Institute require that action be taken to reaffirm, revise, or withdraw this standard no later than five years from the date of approval.

Published by

Accredited Standards Committee X9, Incorporated
Financial Industry Standards
P. O. Box 4035
Annapolis, MD 21403
X9 Online http://www.x9.org

Copyright © 2003 by Accredited Standards Committee X9, Incorporated
All rights reserved.
No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without prior written permission of the publisher. Printed in the United States of America
This ANSI Standard is based on ISO 9564-1:2002(E) *Banking — Personal Identification Number (PIN) management and security — Part 1: PIN protection principles and techniques for online PIN verification in ATM and POS systems*. The ISO 9564-1:2002(E) has been reproduced in its entirety with the addition of "ANSI NOTE"s where required to adapt the text for use as an ANSI Standard. Where applicable, references to ANSI standards have been added.

Specific references to "ISO 9564" in the original ISO 9564 have been replaced with "ISO 9564 [this standard]", for the purpose of clarity.

"ANSI NOTE"s have been added to the following sections of ISO 9564-1:2001(E):

<table>
<thead>
<tr>
<th>Section</th>
<th>&quot;ANSI NOTE&quot;s</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1</td>
<td></td>
</tr>
<tr>
<td>6.2</td>
<td>(two Notes)</td>
</tr>
<tr>
<td>6.3.3</td>
<td></td>
</tr>
<tr>
<td>7.2.2</td>
<td></td>
</tr>
<tr>
<td>7.3.3.3</td>
<td></td>
</tr>
<tr>
<td>8.3.1</td>
<td></td>
</tr>
<tr>
<td>Annex A</td>
<td></td>
</tr>
<tr>
<td>Annex E</td>
<td></td>
</tr>
</tbody>
</table>


Annexes A, B, C, D, E, F and G are informative annexes, presented for information only.

ANS X9.8 consists of the following parts, under the general title Banking - Personal Identification Number (PIN) Management and Security:

- Part 1: PIN protection principles and techniques for online PIN verification in ATM & POS systems
- Part 2: Approved algorithm(s) for PIN encipherment
Contents

Foreword........................................................................................................................................................................ ii
Tables ........................................................................................................................................................................... ii
Introduction ................................................................................................................................................................ ii
1 Scope ..................................................................................................................................................................... 2
2 Normative references ............................................................................................................................................ 2
3 Definitions .............................................................................................................................................................. 2
4 Basic principles of PIN management .................................................................................................................. 2
5 PIN entry devices .................................................................................................................................................. 2
  5.1 Character set .................................................................................................................................................... 2
  5.2 Character representation ............................................................................................................................... 2
  5.3 PIN entry .......................................................................................................................................................... 2
  5.4 Packaging considerations .............................................................................................................................. 2
6 PIN security issues .............................................................................................................................................. 2
  6.1 PIN control requirements ................................................................................................................................ 2
    6.1.1 Hardware and software ............................................................................................................................ 2
    6.1.2 Recording media ....................................................................................................................................... 2
    6.1.3 Oral communications .................................................................................................................................. 2
    6.1.4 Telephone keypads .................................................................................................................................. 2
  6.2 PIN encipherment ............................................................................................................................................ 2
  6.3 Physical security .............................................................................................................................................. 2
    6.3.1 Physical security for PIN entry devices ................................................................................................. 2
    6.3.2 Physically secure device .......................................................................................................................... 2
    6.3.3 Physically secure environment ................................................................................................................ 2
    6.3.4 PIN entry device requirements ................................................................................................................ 2
7 Techniques for management/protection of account-related PIN functions ....................................................... 2
  7.1 PIN length ....................................................................................................................................................... 2
  7.2 PIN selection .................................................................................................................................................... 2
    7.2.1 PIN selection techniques ........................................................................................................................ 2
    7.2.2 Assigned derived PIN ............................................................................................................................. 2
    7.2.3 Assigned random PIN ............................................................................................................................. 2
    7.2.4 Customer selected PIN .......................................................................................................................... 2
  7.3 PIN issuance and delivery ............................................................................................................................... 2
    7.3.1 PIN issuance and delivery controls ......................................................................................................... 2
    7.3.2 Delivery of an assigned PIN ................................................................................................................ 2
    7.3.3 Delivery of customer selected PIN ...................................................................................................... 2
  7.4 PIN change ....................................................................................................................................................... 2
    7.4.1 PIN change in an interchange environment ............................................................................................ 2
    7.4.2 PIN change at an attended terminal ...................................................................................................... 2
    7.4.3 PIN change at an unattended terminal .................................................................................................. 2
    7.4.4 PIN change by mail ............................................................................................................................... 2
    7.4.5 Replacement of forgotten PIN ................................................................................................................ 2
    7.4.6 Replacement of compromised PIN ....................................................................................................... 2
  7.5 Disposal of waste material and returned PIN mailers .................................................................................. 2
Tables

Table 1 — Character representation .........................................................................................................................2

Table 2 — PIN entry device packaging consideration ...............................................................................................2
Introduction

The Personal Identification Number (PIN) is a means of verifying the identity of a customer within an electronic funds transfer (EFT) system.

The objective of PIN management is to protect the PIN against unauthorised disclosure, compromise, and misuse throughout its life cycle and in so doing to minimise the risk of fraud occurring within EFT systems. The secrecy of the PIN needs to be assured at all times during its life cycle which consists of its selection, issuance, activation, storage, entry, transmission, validation, deactivation, and any other use made of it.

PIN security also depends upon sound key management. Maintaining the secrecy of cryptographic keys is of the utmost importance because the compromise of any key allows the compromise of any PIN ever enciphered under it.

Wherever possible, this part of ISO 9564 [this standard] specifies requirements in absolute terms. In some instances a level of subjectivity cannot be practically avoided especially when discussing the degree or level of security desired or to be achieved.

The level of security to be achieved needs to be related to a number of factors, including the sensitivity of the data concerned and the likelihood that the data will be intercepted, the practicality of any envisaged encipherment process, and the cost of providing, and breaking, a particular means of providing security. It is, therefore, necessary for each card Acceptor, Acquirer and Issuer to agree on the extent and detail of security and PIN management procedures. Absolute security is not practically achievable; therefore, PIN management procedures should implement preventive measures to reduce the opportunity for a breach in security and aim for a "high" probability of detection of any illicit access or change to PIN material should these preventive measures fail. This applies at all stages of the generation, exchange and use of a PIN, including those processes that occur in cryptographic equipment and those related to communication of PINs.

This part of ISO 9564 [this standard] is designed so that Issuers can uniformly make certain, to whatever degree is practical, that a PIN, while under the control of other institutions, is properly managed. Techniques are given for protecting the PIN-based customer authentication process by safeguarding the PIN against unauthorised disclosure during the PIN's life cycle.

This standard includes the following annexes:

a) annex A covers general principles of key management;
b) annex B covers techniques for PIN verification;
c) annex C deals with implementation concepts for a PIN entry device for online PIN encipherment;
d) annex D identifies an example of pseudo-random PIN generation;
e) annex E indicates additional guidelines for the design of a PIN entry device;
f) annex F specifies guidance on clearing and destruction procedures for sensitive data;
g) annex G gives information for customers.
In ISO 9564-2, [this standard - part 2] approved encipherment algorithms to be used in the protection of the PIN are specified. Application of the requirements of this part of ISO 9564 [this standard] requires bilateral agreements to be made, including the choice of algorithms specified in ISO 9564-2 [this standard - part 2].

This part of ISO 9564 [this standard] is one of a series that describes requirements for security in the retail banking environment, as follows:


ISO DIS 9564-3, Banking - Personal Identification Number management and security - Part 3, PIN protection principles for offline PIN handling in ATM and POS systems

ISO 10202, Financial transaction cards - Security architecture of financial transaction systems using integrated circuit cards –(all parts)

ISO 11568, Key management (retail) - (all parts)

ISO 13491, Secure cryptographic devices - (all parts)

ISO 15668, Banking - Financial transaction cards - Secure file transfer (retail)

ISO DIS 16609, Banking - requirements for message authentication

Suggestions for the improvement of this standard will be welcome. They should be sent to the ASC X9 Secretariat, Accredited Standards Committee X9, Incorporated, P. O. Box 4035, Annapolis, MD 21403.

This Standard was processed and approved for submittal to ANSI by the Accredited Standards Committee on Financial Services, X9. Committee approval of the Standard does not necessarily imply that all the committee members voted for its approval.

The X9 committee had the following members:

Harold Deal, X9 Chairman
Vincent DeSantis, X9 Vice-Chairman
Cynthia Fuller, Executive Director
Isabel Bailey, Managing Director

<table>
<thead>
<tr>
<th>Organization Represented</th>
<th>Representative</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACI Worldwide</td>
<td>Cindy Rink</td>
</tr>
<tr>
<td>ACI Worldwide</td>
<td>Jim Shaffer</td>
</tr>
<tr>
<td>American Bankers Association</td>
<td>Doug Johnson</td>
</tr>
<tr>
<td>American Bankers Association</td>
<td>Don Rhodes</td>
</tr>
<tr>
<td>American Bankers Association</td>
<td>Stephen Schutze</td>
</tr>
<tr>
<td>American Bankers Association</td>
<td>Michael Scully</td>
</tr>
<tr>
<td>American Express Company</td>
<td>Mike Jones</td>
</tr>
<tr>
<td>American Express Company</td>
<td>Gerry Smith</td>
</tr>
<tr>
<td>American Express Company</td>
<td>Barbara Wakefield</td>
</tr>
<tr>
<td>American Financial Services Association</td>
<td>John Freeman</td>
</tr>
<tr>
<td>American Financial Services Association</td>
<td>Mark Zalewski</td>
</tr>
</tbody>
</table>

1 To be published
<table>
<thead>
<tr>
<th>Organization Represented</th>
<th>Representative</th>
</tr>
</thead>
<tbody>
<tr>
<td>BancTec, Inc.</td>
<td>Rosemary Butterfield</td>
</tr>
<tr>
<td>BancTec, Inc.</td>
<td>Christopher Dowdell</td>
</tr>
<tr>
<td>BancTec, Inc.</td>
<td>David Hunt</td>
</tr>
<tr>
<td>Bank of America</td>
<td>Mack Hicks</td>
</tr>
<tr>
<td>Bank of America</td>
<td>Richard Phillips</td>
</tr>
<tr>
<td>Bank of America</td>
<td>Daniel Welch</td>
</tr>
<tr>
<td>Bank One Corporation</td>
<td>Jacqueline Pagan</td>
</tr>
<tr>
<td>BB and T</td>
<td>Michael Saviak</td>
</tr>
<tr>
<td>BB and T</td>
<td>Woody Tyner</td>
</tr>
<tr>
<td>Caradas</td>
<td>John Gould</td>
</tr>
<tr>
<td>Caradas</td>
<td>Tom Johnston</td>
</tr>
<tr>
<td>Carreker</td>
<td>Rick (Richard P.) Kastner</td>
</tr>
<tr>
<td>Carreker</td>
<td>Jerry Bowman</td>
</tr>
<tr>
<td>Carreker</td>
<td>Harry Hankla</td>
</tr>
<tr>
<td>Carreker</td>
<td>Don Harman</td>
</tr>
<tr>
<td>Carreker</td>
<td>Ron Schultz</td>
</tr>
<tr>
<td>Carreker</td>
<td>Daniel Schutzer</td>
</tr>
<tr>
<td>Carreker</td>
<td>Mark Scott</td>
</tr>
<tr>
<td>Carreker</td>
<td>Skip Zehnder</td>
</tr>
<tr>
<td>Carreker</td>
<td>Maury Jansen</td>
</tr>
<tr>
<td>Carreker</td>
<td>Bruce Chapa</td>
</tr>
<tr>
<td>Carreker</td>
<td>Anne Doland</td>
</tr>
<tr>
<td>Carreker</td>
<td>Judy Edwards</td>
</tr>
<tr>
<td>Carreker</td>
<td>Pamela Ellington</td>
</tr>
<tr>
<td>Carreker</td>
<td>Masood Mirza</td>
</tr>
<tr>
<td>Carreker</td>
<td>Patsie Rinchiuso</td>
</tr>
<tr>
<td>Carreker</td>
<td>Chuck Bram</td>
</tr>
<tr>
<td>Carreker</td>
<td>Richard Fird</td>
</tr>
<tr>
<td>Carreker</td>
<td>Daniel Rick</td>
</tr>
<tr>
<td>Carreker</td>
<td>Joseph Stein</td>
</tr>
<tr>
<td>Carreker</td>
<td>Cory Surges</td>
</tr>
<tr>
<td>Citigroup, Inc.</td>
<td>Bud Beattie</td>
</tr>
<tr>
<td>Citigroup, Inc.</td>
<td>Kevin Finn</td>
</tr>
<tr>
<td>Citigroup, Inc.</td>
<td>Linda Low</td>
</tr>
<tr>
<td>Citigroup, Inc.</td>
<td>Dan Otten</td>
</tr>
<tr>
<td>Deluxe Corporation</td>
<td>Jeannine M. DeLano</td>
</tr>
<tr>
<td>Diebold, Inc.</td>
<td>Dexter Holt</td>
</tr>
<tr>
<td>Diebold, Inc.</td>
<td>Laura Walker</td>
</tr>
<tr>
<td>Diebold, Inc.</td>
<td>Gene Kathol</td>
</tr>
<tr>
<td>Discover Financial Services</td>
<td>Harriette Griffin</td>
</tr>
<tr>
<td>Discover Financial Services</td>
<td>Phil Griffin</td>
</tr>
<tr>
<td>Discover Financial Services</td>
<td>Larry Hines</td>
</tr>
<tr>
<td>Discover Financial Services</td>
<td>Gary Lefkowitz</td>
</tr>
<tr>
<td>Discover Financial Services</td>
<td>Todd Arnold</td>
</tr>
<tr>
<td>Discover Financial Services</td>
<td>Michael Kelly</td>
</tr>
<tr>
<td>Discover Financial Services</td>
<td>Dick Sweeney</td>
</tr>
<tr>
<td>Discover Financial Services</td>
<td>Mark Lundin</td>
</tr>
<tr>
<td>Discover Financial Services</td>
<td>Al Van Ranst</td>
</tr>
<tr>
<td>Discover Financial Services</td>
<td>Jeff Stapleton</td>
</tr>
<tr>
<td>Discover Financial Services</td>
<td>Terry Benson</td>
</tr>
<tr>
<td>Discover Financial Services</td>
<td>Jeff Duncan</td>
</tr>
<tr>
<td>Discover Financial Services</td>
<td>Mimi Hart</td>
</tr>
<tr>
<td>Discover Financial Services</td>
<td>Carlos Morales</td>
</tr>
<tr>
<td>Discover Financial Services</td>
<td>Caroline Dionisio</td>
</tr>
</tbody>
</table>
ANS X9.8–2003

MasterCard International  
MasterCard International  
Mellon Bank, N.A.  
Mellon Bank, N.A.  
National Association of Convenience Stores  
National Association of Convenience Stores  
National Association of Convenience Stores  
National Security Agency  
NCR Corporation  
NCR Corporation  
New York Clearing House  
New York Clearing House  
Niteo Partners  
Niteo Partners  
Silas Technologies  
Silas Technologies  
Star Systems, Inc.  
Star Systems, Inc.  
Symmetricom  
Symmetricom  
Symmetricom  
Unisys Corporation  
Unisys Corporation  
VeriFone, Inc.  
VeriFone, Inc.  
VeriFone, Inc.  
VeriFone, Inc.  
VISA International  
Wells Fargo Bank  
Wells Fargo Bank  

Naiyre Foster  
Ron Karlin  
Richard H. Adams  
David Taddeo  
John Hervey  
Teri Richman  
Robert Swanson  
Sheila Brand  
David Norris  
Steve Stevens  
Vincent DeSantis  
John Dunn  
Charles Friedman  
Michael Versace  
Andrew Garner  
Ray Gatland  
Elizabeth Lynn  
Michael Wade  
John Bernardi  
Sandra Lambert  
Jerry Willett  
David J. Concannon  
Navnit Shah  
David Ezell  
Dave Faoro  
Brad McGuinness  
Brenda Watlington  
Patricia Greenhalgh  
Terry Leahy  
Gordon Martin
At the time it approved this standard, the X9F Subcommittee on Data and Information Security had the following members:

Dick Sweeney, Chairman

**Organization**

3PEA Technologies, Inc.
3PEA Technologies, Inc.
ACI Worldwide
ACI Worldwide
American Bankers Association
American Bankers Association
American Express Company
American Express Company
American Express Company
American Express Company
American Financial Services Association
American Financial Services Association
BancTec, Inc.
Bank of America
Bank of America
Bank of America
Bank of America
Bank One Corporation
BB and T
BB and T
Caradas
Caradas
Caradas
Carreker
Carreker
Carreker
Certicom Corporation
Chrysalis-ITS
Communications Security Establishment
Communications Security Establishment
Deluxe Corporation
Diebold, Inc.
Diebold, Inc.
Diebold, Inc.
Discover Financial Services
Discover Financial Services
Diversinet Corporation
eFunds Corporation
Electronic Industries Alliance
Electronic Industries Alliance
Electronic Industries Alliance
Entrust, Inc.
Federal Reserve Bank
Ferris and Associates, Inc.
First Data Corporation
Griffin Consulting
Griffin Consulting

**Representative**

Mark Newcomer
Daniel Spence
Cindy Rink
Jim Shaffer
Doug Johnson
Don Rhodes
William J. Gray
Mike Jones
Mark Merkow
Gerry Smith
John Freeman
Mark Zalewski
Christopher Dowdell
Andi Coleman
Mack Hicks
Richard Phillips
Daniel Welch
Craig Worstell
Jacqueline Pagan
Michael Saviak
Woody Tyner
John Gould
Tom Johnston
Rick (Richard P.) Kastner
Jerry Bowman
Harry Hankla
Ron Schultz
Daniel Brown
Terry Fletcher
Mike Chawrun
Alan Poplove
Maury Jansen
Bruce Chapa
Anne Doland
Judy Edwards
Pamela Ellington
Masood Mirza
Michael Crerar
Chuck Bram
Edward Mikoski
Kevin M. Nixon CISSP
Donald L. Skillman
Miles Smid
Neil Hersch
J. Martin Ferris
Gene Kathol
Harriette Griffin
Phil Griffin
Under ASC X9 procedures, a working group may be established to address specific segments of work under the ASC X9 Committee or one of its subcommittees. A working group exists only to develop standard(s) or guideline(s) in a specific area and is then disbanded. The individual experts are listed with their affiliated organizations. However, this does not imply that the organization has approved the content of the standard or guideline. (Note: Per X9 policy, company names of non-member participants are listed only if, at time of publication, the X9 Secretariat received an original signed release permitting such company names to appear in print.)

The standard was revised by a subset of the X9F6 Financial Service Data and Information Security working group. At the time it approved this standard, the X9F6 working group consisted of the following members:

John Sheets, Chairman

**Organization**                      **Representative**
3PEA Technologies, Inc.               Jim Forestal
3PEA Technologies, Inc.               Mark Newcomer
3PEA Technologies, Inc.               Daniel Spence
ACI Worldwide                          Cindy Rink
ACI Worldwide                          Julie Samson
ACI Worldwide                          Jim Shaffer
ACOM Solutions                         Gregory T. Church
ACOM Solutions                         Carl Grant
ACS State and Local Solutions         Pat Solitro
Advanced Financial Solutions           Mark Craig
Advanced Financial Solutions           Stephen Gibson-Saxty
Albertsons                             Don Stewart
Alliance Data Systems                  Steve Case
Alliance Data Systems                  Charles Richardson
Alliance Data Systems                  Andy Trawick
American Bankers Association           Doug Johnson
American Bankers Association           Don Rhodes
American Bankers Association           Stephen Schutze
American Bankers Association           Michael Scully
American Express Company               William J. Gray
American Express Company               Mike Jones
American Express Company               Mark Merkow
American Express Company               Richard Rodriguez
American Express Company               Vicky Sammons
American Express Company               Gerry Smith
American Express Company               Barbara Wakefield
American Financial Services Association John Freeman
American Financial Services Association Mark Zalewski
BancTec, Inc.                          Rosemary Butterfield
BancTec, Inc.                          Christopher Dowdell
BancTec, Inc.                          David Hunt
BancTec, Inc.                          Alex Parkov
Bank of America
Bank of America
Bank of America
Bank of America
Bank of America
Bank of America
Bank of America
Bank of America
Bank of America
Bank One Corporation
BB and T
BB and T
Boise Cascade Paper
Booz-Allen and Hamilton Inc.
Burger, Carroll and Associates
Burger, Carroll and Associates
Canadian Payments Association
Canadian Payments Association
Caradas
Caradas
Caradas
Caradas
Carreker
Carreker
Carreker
Carreker
Certicom Corporation
Certicom Corporation
Certicom Corporation
Chaddsford Planning Associates
CheckTech
CheckTech
Chicago Clearing House Association
Chrysalis-ITS
Cisco Systems
Citigroup, Inc.
Citigroup, Inc.
Citigroup, Inc.
Citigroup, Inc.
Citigroup, Inc.
Citigroup, Inc.
Citigroup, Inc.
Citigroup, Inc.
Clarke American Checks, Inc.
Clarke American Checks, Inc.
ClearWave Electronics
ClearWave Electronics
Comerica
Comerica
Communications Security Establishment
Communications Security Establishment
Custom Direct, Incorporated
Custom Direct, Incorporated
First Data Corporation
First Data Corporation
First Data Corporation
First Data Corporation
First Data Corporation
First Data Corporation
Fleet One
Fleet One
Food Marketing Institute
Gilbarco
Gilbarco
Griffin Consulting
Griffin Consulting
GTECH Corp
GTECH Corp
Hagenuk USA Inc.
Heidelberg Digital LLC
Heidelberg Digital LLC
Hewlett Packard
Hewlett Packard
Hypercom
Hypercom
iS3
iS3
IBM Corporation
IBM Corporation
IBM Corporation
Identrus
Identrus
Ingenico Canada Ltd.
Ingenico Canada Ltd.
Inovant
International Biometric Group
International Biometric Group
J.P. Morgan Chase and Co.
J.P. Morgan Chase and Co.
J.P. Morgan Chase and Co.
John H. Harland Company
Jones Futurex, Inc.
Jones Futurex, Inc.
Jones Futurex, Inc.
Jones Futurex, Inc.
Jordan and Jordan
Jordan and Jordan
K3DES LLC
KPMG LLP
KPMG LLP
KPMG LLP
KPMG LLP
KPMG LLP
Landgrave Smith
Liberty Enterprises, Inc.
M. Blake Greenlee Associates, Ltd.
Mag-Tek, Inc.
Mag-Tek, Inc.
Tina McGowan
Carol Simon
Bruce Sussman
Jeanne M. Vacula
Lynn Wheeler
Kristi White
Cynthia Cunningham
Ted Sanft
Ted Mason
Timothy Dickson
Tim Weston
Harriette Griffin
Phil Griffin
Mirek Kula
Brian Ruptash
Kees-Jan Delst
Aaron Lazar
Kathleen Roland
Larry Hines
Gary Lefkowitz
Marcia Johnson
Scott Spiker
John Clark
Michael McKay
Todd Arnold
Michael Kelly
Allen Roginsky
Brandon Brown
Trent Henry
John Sheets
John Spence
Dick Sweeney
Mcken Mak CISSP
Mike Thieme
Jacqueline Binder
Joe Nelson
Paul Simon
Curt Siroky
Jason Anderson
Ray Bryan
Scott Davis
Barry Golden
Steve Junod
Kimberly Sever
Mary Lou Von Kaenel
James Richardson
Azita Amini
Eric Longo
Mark Lundin
Al Van Ranst
Jeff Stapleton
Landgrave Smith, Jr.
Richard Pliml
M. Blake Greenlee
Terry Benson
Jeff Duncan
Oce Printing Systems
Oce Printing Systems
Omgeo
Omgeo
Paychex Inc
Phoenix-Maximus
Piracle
Piracle
Pitney Bowes, Inc.
Pitney Bowes, Inc.
Pitney Bowes, Inc.
PNC Bank, NA,
Pulse EFT Association
Pulse EFT Association
R Squared Academy Ltd.
R Squared Academy Ltd.
RDM Corporation
RDM Corporation
Relizon
Relizon
Relyco Sales Inc
Reynolds and Reynolds Co.
Reynolds and Reynolds Co.
Rosetta Technologies
Rosetta Technologies
RSA Security
Schwab Capital Market L.P.
Schwab Capital Market L.P.
Secure Products
Secure Products
Silas Technologies
Silas Technologies
Software and Information Industry Association
Software and Information Industry Association
Software and Information Industry Association
Source Technologies Inc
Source Technologies Inc
Standard and Poors CUSIP Bureau
Standard and Poors CUSIP Bureau
Standard and Poors CUSIP Bureau
Standard Register Company
Standard Register Company
Star Systems, Inc.
Star Systems, Inc.
Star Systems, Inc.
Star Systems, Inc.
Star Systems, Inc.
Stored Value Systems
Sun Microsystems PS
Sun Microsystems PS
Suntrust Banks
Surety, Inc.
Symmetricom
Symmetricom
Symmetricom
Telekurs USA, Inc.
Banking — Personal Identification Number management and security —
Part 1: Basic principles, and requirements for online PIN handling in ATM and POS systems

1 Scope

This part of ISO 9564 [this standard] specifies:

a) Basic principles and techniques which provide the minimum security measures required for effective international PIN management. These measures are applicable to those institutions responsible for implementing techniques for the management and protection of PINs.

b) PIN protection techniques applicable to financial transaction card originated transactions in an online environment and a standard means of interchanging PIN data. These techniques are applicable to those institutions responsible for implementing techniques for the management and protection of the PIN at Automated Teller Machines (ATM) and acquirer sponsored Point-of-Sale (POS) terminals.

The provisions of this part of ISO 9564 [this standard] are not intended to cover:

a) PIN management and security in the offline PIN environment, which is covered in part 3,

b) PIN management and security in the electronic commerce environments, which is to be covered in a subsequent part of ISO 9564 [this standard],

c) the protection of the PIN against loss or intentional misuse by the customer or authorised employees of the issuer,

d) privacy of non-PIN transaction data,

e) protection of transaction messages against alteration or substitution, e.g. an authorisation response to a PIN verification,

f) protection against replay of the PIN or transaction,

g) specific key management techniques.

2 Normative references

The following standards contain provisions which, through reference in this text, constitute provisions of this part of ISO 9564 [this standard]. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this part of ISO 9564 [this standard] are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.