American National Standard for Financial Services

ANS X9.24-2004

Retail Financial Services
Symmetric Key Management
Part 1: Using Symmetric Techniques

Secretariat

Accredited Standards Committee X9, Inc.

Approved: February 4, 2004

American National Standards Institute
Foreword

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 interpretation 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CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time.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 USA
X9 Online http://www.x9.org

Copyright © 2004 Accredited Standards Committee X9, Inc.
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.
Contents

Foreword .................................................................................................................................................. i
Figures .................................................................................................................................................... iv
Tables ..................................................................................................................................................... v
Introduction .............................................................................................................................................. vi

1 Purpose ................................................................................................................................................. 1
2 Scope .................................................................................................................................................... 1
2.1 Application ....................................................................................................................................... 2
3 References ........................................................................................................................................... 2

4 Terms and Definitions ............................................................................................................................ 2
5 Standard Organization ............................................................................................................................. 8
6 Environment .......................................................................................................................................... 8
6.1 General ............................................................................................................................................... 8
6.2 Cardholder and Card Issuer ............................................................................................................... 8
6.3 Card Acceptor .................................................................................................................................. 8
6.4 Acquirer ............................................................................................................................................ 9

7 Key Management Requirements ........................................................................................................... 9
7.1 General ............................................................................................................................................. 9
7.2 Tamper-Resistant Security Modules (TRSM) used for Key Management ......................................... 10
7.3 A Secure Environment ...................................................................................................................... 11
7.4 Key Generation ................................................................................................................................ 11
7.5 Symmetric Key Distribution ............................................................................................................. 12
7.5.1 Manual Distribution .................................................................................................................... 12
7.5.2 Key Initialization Facility ........................................................................................................... 12
7.5.3 Key Loading Device .................................................................................................................... 13
7.6 Key Utilization .................................................................................................................................. 13
7.7 Key Replacement .............................................................................................................................. 13
7.8 Key Destruction and Archival .......................................................................................................... 13
7.9 Key Encryption/Decryption ................................................................................................................ 14

8 Key Management Specifications ............................................................................................................ 14
8.1 General ............................................................................................................................................. 14
8.2 Methods of Key Management ......................................................................................................... 14
8.2.1 Key Management Methods Requiring Compromise Prevention Controls .................................. 15
8.2.2 Key Management Method Requiring Compromise Detection Controls ................................... 15
8.3 Key Identification Techniques ........................................................................................................ 15
8.3.1 Implicit Key Identification .......................................................................................................... 16
8.3.2 Key Identification by Name ........................................................................................................ 16
8.4 Security Management Information Data (SMID) Element ................................................................. 16
8.4.1 Notations, Abbreviations and Conventions ............................................................................ 17
8.4.2 Representation ............................................................................................................................. 18
8.4.3 Key Naming .................................................................................................................................. 21
8.5 Method: Fixed Transaction Keys ...................................................................................................... 22
8.5.1 SMID ............................................................................................................................................ 22
ANS X9.24-2004

8.5.2 Additional Key Management Requirements ......................................................... 22
8.5.3 Additional Notes ..................................................................................................... 22
8.6 Method: Master Keys / Transaction Keys ................................................................. 23
8.6.1 SMID ..................................................................................................................... 23
8.6.2 Additional Key Management Requirements ....................................................... 23
8.6.3 Additional Notes ..................................................................................................... 24
8.7 Method: DUKPT (Derived Unique Key Per Transaction) ....................................... 24
8.7.1 SMID ..................................................................................................................... 26
8.7.2 Additional Key Management Requirements ....................................................... 27
8.7.3 Additional Notes ..................................................................................................... 27

Annex A (Informative) Derived Unique Key Per Transaction ......................................... 29
A.1 Storage Areas ............................................................................................................. 29
A.1.1 PIN Processing ....................................................................................................... 29
A.1.2 Key Management .................................................................................................. 29
A.2 Processing Algorithms ............................................................................................. 30
A.3 Key Management Technique ................................................................................... 34
A.4 DUKPT Test Data Examples ................................................................................... 37
A.4.1 Initial Sequence ..................................................................................................... 39
A.4.2 MSB Rollover Sequence ....................................................................................... 41
A.4.3 Message Authentication ....................................................................................... 42
A.5 "Security Module" Algorithm For Automatic PIN Entry Device Checking ............... 42
A.6 Derivation Of The Initial Key ................................................................................... 43

Annex B (Informative) SMID Examples ......................................................................... 44

Annex C (Informative) Example: Manual Key Distribution .......................................... 49

Annex D (Informative) Summary of X9.17 Financial Institution Key Management (Wholesale) ......................................................... 52
D.1 Automated Key Management Architecture ........................................................... 52
D.2 Key Encryption and Decryption ............................................................................... 53
D.3 Key Counters and Key Offsetting ........................................................................... 53
D.4 Key Notarization ..................................................................................................... 54
D.5 Automated Key Distribution Protocols ................................................................. 54
D.6 Point-To-Point Environment ................................................................................... 55
D.7 Key Center Environments ....................................................................................... 56

Annex E (Informative) Key Set Identifiers .................................................................... 57
E.1 An Example Key Serial Number Format ............................................................... 57
E.1.1 IIN - 3 Bytes - Issuer Identification Number ....................................................... 58
E.1.2 CID - 1 Byte - Customer ID ................................................................................ 58
E.1.3 GID - 1 Byte - Group ID ....................................................................................... 58
E.1.4 DID - 19 Bit Device ID ......................................................................................... 58
E.1.5 TCTR - 21 Bit Transaction Counter ..................................................................... 59
Figures

Figure 1 – DUKPT at Receiving TRSM ....................................................................................................................25
Figure 2 – DUKPT at Originating TRSM ..................................................................................................................26
Figure A-1 – Simplified DUKPT Data Flow ............................................................................................................35
Figure C-1 – Generating Key Check Value ..............................................................................................................51
Figure D-1 – Keying relations in the point-to-point environment ............................................................................53
Figure D-2 – Keying relations in the key center environments .............................................................................54
Figure D-3 – Message flow in the point-to-point environment .............................................................................55
Figure D-4 – Message flow in the key center environments ..................................................................................56
Figure E-1 – Key Serial Number Format Example ...............................................................................................58
Tables

Table C-1 – Example of Pair-wise XOR Combination of Key components for DEA.................................................. 50
Introduction

Today, billions of dollars in funds are transferred electronically by various communication methods. Transactions are often entered remotely, off-premise from financial institutions, by retailers or by customers directly. Such transactions are transmitted over potentially non-secure media. The vast range in value, size, and the volume of such transactions expose institutions to severe risks, which may be uninsurable.

To protect these financial messages and other sensitive information, many institutions are making increased use of the American National Standards Institute Triple Data Encryption Algorithm (TDEA). Specific examples of its use include standards for message authentication, personal identification number encryption, other data encryption, and key encryption.

The TDEA is in the public domain. The security and reliability of any process based on the TDEA is directly dependent on the protection afforded to secret numbers called cryptographic keys. This part of ANS X9.24-2004 deals exclusively with management of symmetric keys using symmetric techniques. Additional parts may be created in the future to address other methods of key management.

A familiar analogy may be found in the combination lock of a vault. The lock design is public knowledge. Security is provided by keeping a number, the combination, a secret. Secure operation also depends on protective procedures and features which prevent surreptitious viewing or determination of the combination by listening to its operation. Procedures are also required to ensure that the combination is random and cannot be modified by an unauthorized individual without detection.

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

The standard was processed and approved for submittal to the American National Standards Institute by the Accredited Standards Committee X9 - Financial Services. Committee approval of the standard does not necessarily imply that all committee members voted for its approval. At the time it approved this standard, the X9 Committee had the following members:

Gene Kathol, X9 Chairman
Vincent DeSantis, X9 Vice Chairman
Cynthia L. Fuller, Executive Director
Isabel Bailey, Managing Director

**Organization Represented**

- ACI Worldwide
- American Express Company
- American Financial Services Association
- Bank of America
- Bank One Corporation
- BB and T
- Cable & Wireless America
- Citigroup, Inc.
- Deluxe Corporation
- Diebold, Inc.

**Representative**

- Jim Shaffer
- Mike Jones
- Mark Zalewski
- Daniel Welch
- Jacqueline Pagan
- Woody Tyner
- Kevin M. Nixon CISSP CISM
- Daniel Schutzer
- Bill Ferguson
- Bruce Chapa
ANS X9.24-2004

Discover Financial Services  Jon Mills
eFunds Corporation  Cory Surges
Federal Reserve Bank  Dexter Holt
First Data Corporation  Gene Kathol
Fiserv  Bud Beattie
Hewlett Packard  Larry Hines
Hypercom  Scott Spiker
IBM Corporation  Todd Arnold
Ingenico  John Sheets
KPMG LLP  Alfred F. Van Ranst Jr.
MagTek, Inc.  Carlos Morales
MasterCard International  William Poletti
Mellon Bank, N.A.  David Taddeo
National Association of Convenience Stores  John Hervey
National Security Agency  Sheila Brand
NCR Corporation  David Norris
Niteo Partners  Michael Versace
Star Systems, Inc.  Michael Wade
Symmetricom  Sandra Lambert
The Clearing House  Vincent DeSantis
Unisys Corporation  David J. Concannon
VeriFone, Inc.  Brad McGuinness
VISA International  Patricia Greenhalgh
Wachovia Bank  Ray Gatland
Wells Fargo Bank  Terry Leahy

At the time it approved this standard, the X9F Subcommittee on Data and Information Security had the following members:

Dick Sweeney, Chairperson

<table>
<thead>
<tr>
<th>Organization Represented</th>
<th>Representative</th>
</tr>
</thead>
<tbody>
<tr>
<td>3PEA Technologies, Inc.</td>
<td>Mark Newcomer</td>
</tr>
<tr>
<td>ACI Worldwide</td>
<td>Jim Shaffer</td>
</tr>
<tr>
<td>American Financial Services Association</td>
<td>Mark Zalewski</td>
</tr>
<tr>
<td>Bank of America</td>
<td>Mack Hicks</td>
</tr>
<tr>
<td>Bank One Corporation</td>
<td>Jacqueline Pagan</td>
</tr>
<tr>
<td>BB and T</td>
<td>Woody Tyner</td>
</tr>
<tr>
<td>Cable &amp; Wireless America</td>
<td>Kevin M. Nixon CISSP CISM</td>
</tr>
<tr>
<td>Deluxe Corporation</td>
<td>Bill Ferguson</td>
</tr>
<tr>
<td>Diebold, Inc.</td>
<td>Bruce Chapa</td>
</tr>
<tr>
<td>Discover Financial Services</td>
<td>Todd Douthat</td>
</tr>
<tr>
<td>Diversinet Corporation</td>
<td>Rick (Richard P.) Kastner</td>
</tr>
<tr>
<td>eFunds Corporation</td>
<td>Chuck Bram</td>
</tr>
<tr>
<td>Ferris and Associates, Inc.</td>
<td>J. Martin Ferris</td>
</tr>
<tr>
<td>First Data Corporation</td>
<td>Gene Kathol</td>
</tr>
<tr>
<td>Fiserv</td>
<td>Bud Beattie</td>
</tr>
<tr>
<td>Hewlett Packard</td>
<td>Larry Hines</td>
</tr>
<tr>
<td>Hypercom</td>
<td>Scott Spiker</td>
</tr>
<tr>
<td>IBM Corporation</td>
<td>Todd Arnold</td>
</tr>
<tr>
<td>Identrus</td>
<td>Brandon Brown</td>
</tr>
</tbody>
</table>
The X9F6 working group that revised this standard consisted of the following members:

John Sheets, Chairperson

<table>
<thead>
<tr>
<th>Organization Represented</th>
<th>Representative</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACI Worldwide</td>
<td>Julie Samson</td>
</tr>
<tr>
<td>ACI Worldwide</td>
<td>Jim Shaffer</td>
</tr>
<tr>
<td>Alliance Data Systems</td>
<td>Steve Case</td>
</tr>
<tr>
<td>Bank of America</td>
<td>Andi Coleman</td>
</tr>
<tr>
<td>DeLap, White, Caldwell and Croy, LLP</td>
<td>Darlene Kargel</td>
</tr>
<tr>
<td>Diebold, Inc.</td>
<td>Bruce Chapa</td>
</tr>
<tr>
<td>Diebold, Inc.</td>
<td>Anne Doland</td>
</tr>
<tr>
<td>Diversinet Corporation</td>
<td>Rick (Richard P.) Kastner</td>
</tr>
<tr>
<td>eFunds Corporation</td>
<td>Chuck Bram</td>
</tr>
<tr>
<td>Eracom Technologies</td>
<td>Berry Borgers</td>
</tr>
<tr>
<td>Fagan and Associates, LLC</td>
<td>Jeanne Fagan</td>
</tr>
<tr>
<td>First Data Corporation</td>
<td>Lisa Curry</td>
</tr>
<tr>
<td>First Data Corporation</td>
<td>Martha Keely</td>
</tr>
<tr>
<td>First Data Corporation</td>
<td>Bruce Sussman</td>
</tr>
<tr>
<td>First Data Corporation</td>
<td>Kristi White</td>
</tr>
<tr>
<td>Fiserv</td>
<td>Bud Beattie</td>
</tr>
<tr>
<td>Fiserv</td>
<td>Dan Otten</td>
</tr>
<tr>
<td>Gilbarco</td>
<td>Tim Weston</td>
</tr>
<tr>
<td>Hewlett Packard</td>
<td>Larry Hines</td>
</tr>
<tr>
<td>Hypercom</td>
<td>Scott Spiker</td>
</tr>
<tr>
<td>iS3</td>
<td>John Clark</td>
</tr>
</tbody>
</table>
ANS X9.24-2004

iS3
IBM Corporation
Ingenico
Ingenico
KPMG LLP
KPMG LLP
MagTek, Inc.
nCipher Corporation Ltd.
NCR Corporation
Star Systems, Inc.
Star Systems, Inc.
TECSEC Incorporated
Thales e-Security, Inc.
Trusted Security Solutions, Inc.
VeriFone, Inc.
VISA
VISA International

Michael McKay
Todd Arnold
John Sheets
John Spence
Azita Amini
Jeff Stapleton
Terry Benson
Ron Carter
Charlie Harrow
Hugh Burke
Michael Wade
Pud Reaver
Brian Sullivan
Dennis Abraham
Dave Faoro
Stoddard Lambertson
Richard Hite
Retail Financial Services
Symmetric Key Management
Part 1: Using Symmetric Techniques

1 Purpose

This key management standard, utilized in conjunction with the American National Standard Triple Data Encryption Algorithm (TDEA) (see Reference 3), should be used to manage symmetric keys that can be used to protect messages and other sensitive information in a financial services environment. The security and reliability of any process based on the TDEA is directly dependent on the protection afforded to secret parameters called cryptographic keys.

This standard establishes requirements and guidelines for the secure management and application-level interoperability of keying operations. Such keys could be used for authenticating messages (see Reference 5), for encrypting Personal Identification Numbers (PIN) (see Reference 4), for encrypting other data, and for encrypting other keys.

2 Scope

This part of ANS X9.24-2004 covers both the manual and automated management of keying material used for financial services such as point-of-sale (POS) transactions (debit and credit), automated teller machine (ATM) transactions, messages among terminals and financial institutions, and interchange messages among acquirers, switches and card issuers. This part of ANS X9.24-2004 deals exclusively with management of symmetric keys using symmetric techniques. Additional parts may be created in the future to address other methods of key management.

This part of ANS X9.24-2004 specifies the minimum requirements for the management of keying material. Addressed are all components of the key management life cycle including generation, distribution, utilization, storage, archiving, replacement and destruction of the keying material. An institution's key management process, whether implemented in a computer or a terminal, is not to be implemented or controlled in a manner that has less security, protection, or control than described herein. It is intended that two nodes, if they implement compatible versions of:

— the same secure key management method,
— the same secure key identification technique approved for a particular method, and
— the same key separation methodologies

in accordance with this part of ANS X9.24-2004 will be interoperable at the application level. Other characteristics may be necessary for node interoperability; however, this part of ANS X9.24-2004 does not cover such characteristics as message format, communications protocol, transmission speed, or device interface.