TR-31 2005

Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms

Accredited Standards Committee X9, Incorporated
Financial Industry Standards
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Foreword</td>
<td>iii</td>
</tr>
<tr>
<td>Introduction</td>
<td>iv</td>
</tr>
<tr>
<td>1 Scope</td>
<td>1</td>
</tr>
<tr>
<td>2 References</td>
<td>1</td>
</tr>
<tr>
<td>3 Terms and definitions</td>
<td>2</td>
</tr>
<tr>
<td>4 Symbols and abbreviated terms</td>
<td>2</td>
</tr>
<tr>
<td>5 Key Block Properties and Characteristics</td>
<td>3</td>
</tr>
<tr>
<td>5.1 Key Block Elements</td>
<td>3</td>
</tr>
<tr>
<td>5.2 Confidential Data to be Exchanged/Stored</td>
<td>3</td>
</tr>
<tr>
<td>5.3 Key Block Binding Method</td>
<td>4</td>
</tr>
<tr>
<td>5.4 TRSM Validation of Incoming Key Block</td>
<td>4</td>
</tr>
<tr>
<td>Annex A CBC MAC Key Block with Optional Block</td>
<td>5</td>
</tr>
<tr>
<td>A.1 Introduction</td>
<td>5</td>
</tr>
<tr>
<td>A.2 Key Block Header (KBH)</td>
<td>5</td>
</tr>
<tr>
<td>A.3 Encryption</td>
<td>8</td>
</tr>
<tr>
<td>A.4 MAC</td>
<td>8</td>
</tr>
<tr>
<td>A.5 Defined values for Key Block Headers</td>
<td>9</td>
</tr>
<tr>
<td>A.5.1 Key Usage</td>
<td>9</td>
</tr>
<tr>
<td>A.5.2 Algorithm</td>
<td>10</td>
</tr>
<tr>
<td>A.5.3 Mode of Use</td>
<td>10</td>
</tr>
<tr>
<td>A.5.4 Key Version Number</td>
<td>11</td>
</tr>
<tr>
<td>A.5.5 Exportability</td>
<td>11</td>
</tr>
<tr>
<td>A.5.6 Optional block ID</td>
<td>12</td>
</tr>
<tr>
<td>A.6 Encoding</td>
<td>14</td>
</tr>
<tr>
<td>A.7 Key Block Examples</td>
<td>15</td>
</tr>
<tr>
<td>A.7.1 Notation Used</td>
<td>15</td>
</tr>
<tr>
<td>A.7.2 Example 1: Key Block without Optional Blocks</td>
<td>15</td>
</tr>
<tr>
<td>A.7.3 Example 2: Key Block with Optional Block</td>
<td>17</td>
</tr>
<tr>
<td>Annex B Process for Approval of New Field Values</td>
<td>21</td>
</tr>
<tr>
<td>B.1 Introduction</td>
<td>21</td>
</tr>
<tr>
<td>B.2 Origination</td>
<td>21</td>
</tr>
<tr>
<td>B.3 Justification for Proposal</td>
<td>21</td>
</tr>
<tr>
<td>B.4 Examination of Proposals</td>
<td>21</td>
</tr>
<tr>
<td>B.5 Appeals Procedure</td>
<td>22</td>
</tr>
<tr>
<td>B.6 Approved List Of Key Block Field Values</td>
<td>22</td>
</tr>
<tr>
<td>B.7 TR-31 Revision</td>
<td>22</td>
</tr>
<tr>
<td>Annex C New Field Value Request Form</td>
<td>23</td>
</tr>
</tbody>
</table>
Figures
Figure A-1 — CBC MAC Key Block .......................................................................................................................... 5
Figure A-2 — Examples of KBH and Optional Blocks ............................................................................................. 13

Tables
Table 5-1. Encryption IV ............................................................................................................................................ 4
Table A-1. KBH for CBC MAC Binding Method ...................................................................................................... 6
Table A-2. Example of confidential data for a double-length TDEA key ................................................................. 8
Table A-3. Defined Key Usage Values ...................................................................................................................... 9
Table A-4. Defined Algorithm Values ..................................................................................................................... 10
Table A-5. Defined Mode of Use Values .................................................................................................................. 10
Table A-6. Key Version Number definition ........................................................................................................... 11
Table A-7. Defined Values for Exportability Byte ................................................................................................. 11
Table A-8. Defined Values for Optional Block ID .................................................................................................. 14
Table A-9. Key Block Values Version IDs Optional Block ....................................................................................... 14
Foreword

Publication of this Technical Report that has been registered with ANSI has been approved by the Accredited Standards Committee X9, Incorporated, P.O. Box 4035, Annapolis, MD 21403. This document is registered as a Technical Report according to the “Procedures for the Registration of Technical Reports with ANSI.” This document is not an American National Standard and the material contained herein is not normative in nature. Comments on the content of this document should be sent to: Attn: Executive Director, Accredited Standards Committee X9, Inc., P.O. Box 4035, Annapolis, MD 21403.

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 © 2005 ASC 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. Published in the United States of America.
Introduction

The retail financial transactions industry has in the past lacked an interoperable method for secure key exchange. While this has always been an issue, the planned move to Triple DEA (TDEA) encryption has made this issue more acute, as methods for the secure exchange of TDEA keys are non-obvious. This Technical Report is intended to give the reader an implementation that meets the requirements for secure key management as set forth in ANS X9.24 Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques.

NOTE The user's attention is called to the possibility that compliance with this technical report may require use of an invention covered by patent rights.

By publication of this technical report, no position is taken with respect to the validity of this claim or of any patent rights in connection therewith. The patent holder has, however, filed a statement of willingness to grant a license under these rights on reasonable and nondiscriminatory terms and conditions to applicants desiring to obtain such a license. Details may be obtained from the standards developer.

Suggestions for the improvement or revision of this Technical Report are welcome. They should be sent to the X9 Committee Secretariat, Accredited Standards Committee X9, Inc., Financial Industry Standards, P.O. Box 4035 Annapolis, MD 21403 USA.

This Technical Report was processed and approved for registration with ANSI by the Accredited Standards Committee on Financial Services, X9. Committee approval of this Technical Report does not necessarily imply that all the committee members voted for its approval.

The X9 committee had the following members:
Gene Kathol, 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>Jim Shaffer</td>
</tr>
<tr>
<td>American Express Company</td>
<td>Mike Jones</td>
</tr>
<tr>
<td>American Financial Services Association</td>
<td>Mark Zalewski</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>Woody Tyner</td>
</tr>
<tr>
<td>Cable &amp; Wireless America</td>
<td>Kevin M. Nixon CISSP CISM</td>
</tr>
<tr>
<td>Citigroup, Inc.</td>
<td>Daniel Schutzer</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>Jon Mills</td>
</tr>
<tr>
<td>eFunds Corporation</td>
<td>Cory Surges</td>
</tr>
<tr>
<td>Federal Reserve Bank</td>
<td>Dexter Holt</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>Ingenico</td>
<td>John Sheets</td>
</tr>
<tr>
<td>KPMG LLP</td>
<td>Alfred F. Van Ranst Jr.</td>
</tr>
<tr>
<td>MagTek, Inc.</td>
<td>Carlos Morales</td>
</tr>
<tr>
<td>MasterCard International</td>
<td>William Poletti</td>
</tr>
<tr>
<td>Mellon Bank, N.A.</td>
<td>David Taddeo</td>
</tr>
<tr>
<td>National Association of Convenience Stores</td>
<td>John Hervey</td>
</tr>
<tr>
<td>National Security Agency</td>
<td>Sheila Brand</td>
</tr>
<tr>
<td>NCR Corporation</td>
<td>David Norris</td>
</tr>
<tr>
<td>Niteo Partners</td>
<td>Michael Versace</td>
</tr>
<tr>
<td>Star Systems, Inc.</td>
<td>Michael Wade</td>
</tr>
<tr>
<td>Symmetricom</td>
<td>Sandra Lambert</td>
</tr>
<tr>
<td>The Clearing House</td>
<td>Vincent DeSantis</td>
</tr>
<tr>
<td>Unisys Corporation</td>
<td>David J. Concannon</td>
</tr>
<tr>
<td>VeriFone, Inc.</td>
<td>Brad McGuinness</td>
</tr>
<tr>
<td>VISA International</td>
<td>Patricia Greenhalgh</td>
</tr>
<tr>
<td>Wachovia Bank</td>
<td>Ray Gatland</td>
</tr>
<tr>
<td>Wells Fargo Bank</td>
<td>Terry Leahy</td>
</tr>
</tbody>
</table>
At the time it approved this standard, the X9F Subcommittee on Data and Information Security had the following members:

Dick Sweeney, Chairperson

**Organization Represented**
- 3PEA Technologies, Inc.
- ACI Worldwide
- American Financial Services Association
- Bank of America
- Bank One Corporation
- BB and T
- Cable & Wireless America
- Deluxe Corporation
- Diebold, Inc.
- Discover Financial Services
- Diversinet Corporation
- eFunds Corporation
- Ferris and Associates, Inc.
- First Data Corporation
- Fiserv
- Hewlett Packard
- Hypercom
- IBM Corporation
- Identrus
- InfoGard Laboratories
- Ingenico
- International Biometric Group
- Jones Futurex, Inc.
- KPMG LLP
- MagTek, Inc.
- Mellon Bank, N.A.
- National Association of Convenience Stores
- National Security Agency
- NCR Corporation
- Niteo Partners
- NIST
- NTRU Cryptosystems, Inc.
- Orion Security Solutions
- Pitney Bowes, Inc.
- R Squared Academy Ltd.
- RSA Security
- Star Systems, Inc.
- Surety, Inc.
- TECSEC Incorporated
- Thales e-Security, Inc.
- VeriFone, Inc.
- VISA International
- Wachovia Bank
- Wells Fargo Bank

**Representative**
- Mark Newcomer
- Jim Shaffer
- Mark Zalewski
- Mack Hicks
- Jacqueline Pagan
- Woody Tyner
- Kevin M. Nixon CISSP CISM
- Bill Ferguson
- Bruce Chapa
- Todd Douthat
- Rick (Richard P.) Kastner
- Chuck Bram
- J. Martin Ferris
- Gene Kathol
- Bud Beattie
- Larry Hines
- Scott Spiker
- Todd Arnold
- Brandon Brown
- Tom Caddy
- John Sheets
- Mcken Mak CISSP
- Ray Bryan
- Alfred F. Van Ranst Jr.
- Terry Benson
- David Taddeo
- John Hervey
- Sheila Brand
- David Norris
- Michael Versace
- Elaine Barker
- William Whyte
- Miles Smid
- Leon Pintsov
- Ralph Spencer Poore
- Burt Kaliski
- Michael Wade
- Dimitrios Andivahis
- Ed Scheidt
- James Torjussen
- Dave Faoro
- Richard Hite
- Ray Gatland
- Terry Leahy
The X9F6 working group that revised this standard consisted of the following members:

John Sheets, Chairperson

**Organization Represented** | **Representative**
--- | ---
ACI Worldwide | Julie Samson
ACI Worldwide | Jim Shaffer
Alliance Data Systems | Steve Case
Bank of America | Andi Coleman
DeLap, White, Caldwell and Croy, LLP | Darlene Kargel
Diebold, Inc. | Bruce Chapa
Diebold, Inc. | Anne Doland
Diversinet Corporation | Rick (Richard P.) Kastner
eFunds Corporation | Chuck Bram
Eracom Technologies | Berry Borgers
Fagan and Associates, LLC | Jeanne Fagan
First Data Corporation | Lisa Curry
First Data Corporation | Martha Keely
First Data Corporation | Bruce Sussman
First Data Corporation | Kristi White
Fiserv | Bud Beattie
Fiserv | Dan Otten
Gilbarco | Tim Weston
Hewlett Packard | Larry Hines
Hypercom | Scott Spiker
iS3 | John Clark
iS3 | Michael McKay
IBM Corporation | Todd Arnold
Ingenico | John Sheets
Ingenico | John Spence
KPMG LLP | Azita Amini
KPMG LLP | Jeff Stapleton
MagTek, Inc. | Terry Benson
nCipher Corporation Ltd. | Ron Carter
NCR Corporation | Charlie Harrow
Star Systems, Inc. | Hugh Burke
Star Systems, Inc. | Michael Wade
TECSEC Incorporated | Pud Reaver
Thales e-Security, Inc. | Brian Sullivan
Trusted Security Solutions, Inc. | Dennis Abraham
VeriFone, Inc. | Dave Faoro
VISA | Stoddard Lambertson
VISA International | Richard Hite

This is the first release of this document.

This document is to be used in conjunction with implementation of ANS X9.8-2003 and ANS X9.24 Part 1-2004.
TR-31 2005

Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms

1 Scope

This document describes a method consistent with the requirements of ANSI X9.24 Retail Financial Services Symmetric Key Management Part 1 for the secure exchange of keys and other sensitive data between two devices that share a symmetric key exchange key. This method may also be used for the storage of keys under a symmetric key. This method is designed to operate within the existing capabilities of devices used in the retail financial services industry.

This document is not a security standard and is not intended to establish security requirements. It is intended instead to provide an interoperable method of implementing security requirements and policies.

2 References

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

2. ANSI X9.24 Retail Financial Services Symmetric Key Management Part 2: Using Asymmetric Techniques for the Distribution of Symmetric Keys; (draft)
3. ANSI X3.92 Data Encryption Algorithm (DEA)
6. ANSI X9 TG 3 PIN Security Compliance Guideline
7. ANSI X9 TG 7 Initial DEA Key Distribution for PIN Entry and Transaction Originating Devices Guideline
8. ISO 16609-2004, Banking – Requirements for message authentication using symmetric techniques