

TR-31 2005

Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms



Accredited Standards Committee X9, Incorporated
Financial Industry Standards

This is a preview of "X9 TR-31:2005". [Click here to purchase the full version from the ANSI store.](#)

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

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

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.
Discover Financial Services
eFunds Corporation
Federal Reserve Bank
First Data Corporation
Fiserv
Hewlett Packard
Hypercom
IBM Corporation
Ingenico
KPMG LLP
MagTek, Inc.
MasterCard International
Mellon Bank, N.A.
National Association of Convenience Stores
National Security Agency
NCR Corporation
Niteo Partners
Star Systems, Inc.
Symmetricom
The Clearing House
Unisys Corporation
VeriFone, Inc.
VISA International
Wachovia Bank
Wells Fargo Bank

Representative

Jim Shaffer
Mike Jones
Mark Zalewski
Daniel Welch
Jacqueline Pagan
Woody Tyner
Kevin M. Nixon CISSP CISM
Daniel Schutzer
Bill Ferguson
Bruce Chapa
Jon Mills
Cory Surges
Dexter Holt
Gene Kathol
Bud Beattie
Larry Hines
Scott Spiker
Todd Arnold
John Sheets
Alfred F. Van Ranst Jr.
Carlos Morales
William Poletti
David Taddeo
John Hervey
Sheila Brand
David Norris
Michael Versace
Michael Wade
Sandra Lambert
Vincent DeSantis
David J. Concannon
Brad McGuinness
Patricia Greenhalgh
Ray Gatland
Terry Leahy

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

ACI Worldwide
ACI Worldwide
Alliance Data Systems
Bank of America
DeLap, White, Caldwell and Croy, LLP
Diebold, Inc.
Diebold, Inc.
Diversinet Corporation
eFunds Corporation
Eracom Technologies
Fagan and Associates, LLC
First Data Corporation
First Data Corporation
First Data Corporation
First Data Corporation
Fiserv
Fiserv
Gilbarco
Hewlett Packard
Hypercom
iS3
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

Representative

Julie Samson
Jim Shaffer
Steve Case
Andi Coleman
Darlene Kargel
Bruce Chapa
Anne Doland
Rick (Richard P.) Kastner
Chuck Bram
Berry Borgers
Jeanne Fagan
Lisa Curry
Martha Keely
Bruce Sussman
Kristi White
Bud Beattie
Dan Otten
Tim Weston
Larry Hines
Scott Spiker
John Clark
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

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.

This is a preview of "X9 TR-31:2005". [Click here to purchase the full version from the ANSI store.](#)

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 ANS 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.

1. ANS X9.24 Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques: 2004
2. ANS X9.24 Retail Financial Services Symmetric Key Management Part 2: Using Asymmetric Techniques for the Distribution of Symmetric Keys; (draft)
3. ANS X3.92 Data Encryption Algorithm (DEA)
4. ANS X9.52:1998 Triple Data Encryption Algorithm Modes of Operations
5. ISO 9797 Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 1: Mechanisms using a block cipher: 1999
6. ANS X9 TG 3 PIN Security Compliance Guideline
7. ANS 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