TR-31 2005

Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms

Accredited Standards Committee X9, Incorporated
Financial Industry Standards

Contents

Page

Figures

Tables

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

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	Representative
ACI Worldwide	Jim Shaffer
American Express Company	Mike Jones
American Financial Services Association	Mark Zalewski
Bank of America	Daniel Welch
Bank One Corporation	Jacqueline Pagan
BB and T	Woody Tyner
Cable & Wireless America	Kevin M. Nixon CISSP CISM
Citigroup, Inc.	Daniel Schutzer
Deluxe Corporation	Bill Ferguson
Diebold, Inc.	Bruce Chapa
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

Organization Represented	Representative
3PEA Technologies, Inc.	Mark Newcomer
ACI Worldwide	Jim Shaffer
American Financial Services Association	Mark Zalewski
Bank of America	Mack Hicks
Bank One Corporation	Jacqueline Pagan
BB and T	Woody Tyner
Cable & Wireless America	Kevin M. Nixon CISSP CISM
Deluxe Corporation	Bill Ferguson
Diebold, Inc.	Bruce Chapa
Discover Financial Services	Todd Douthat
Diversinet Corporation	Rick (Richard P.) Kastner
eFunds Corporation	Chuck Bram
Ferris and Associates, Inc.	J. Martin Ferris
First Data Corporation	Gene Kathol
Fiserv	Bud Beattie
Hewlett Packard	Larry Hines
Hypercom	Scott Spiker
IBM Corporation	Todd Arnold
Identrus	Brandon Brown
InfoGard Laboratories	Tom Caddy
Ingenico	John Sheets
International Biometric Group	Mcken Mak CISSP
Jones Futurex, Inc.	Ray Bryan
KPMG LLP	Alfred F. Van Ranst Jr.
MagTek, Inc.	Terry Benson
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
NIST	Elaine Barker
NTRU Cryptosystems, Inc.	William Whyte
Orion Security Solutions	Miles Smid
Pitney Bowes, Inc.	Leon Pintsov
R Squared Academy Ltd.	Ralph Spencer Poore
RSA Security	Burt Kaliski
Star Systems, Inc.	Michael Wade
Surety, Inc.	Dimitrios Andivahis
TECSEC Incorporated	Ed Scheidt
Thales e-Security, Inc.	James Torjussen
VeriFone, Inc.	Dave Faoro
VISA International	Richard Hite
Wachovia Bank	Ray Gatland
Wells Fargo Bank	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 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