X9 TR-31 2010

Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms

A Technical Report prepared by:
Accredited Standards Committee X9, Incorporated
Financial Industry Standards

Registered with American National Standards Institute

Date Registered: December 9, 2010

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, 1212 West Street, Suite 200, Annapolis, MD 21401. This document is registered as a Technical Report according to the ñProcedures for the Registration of Technical Reports with ANSI.ò 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., 1212 West Street, Suite 200, Annapolis, MD 21401.

CAUTION NOTICE: This Technical Report may be revised or withdrawn at any time.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 technical report no later than five years from the date of approval.

Published by

Accredited Standards Committee X9, Incorporated
Financial Industry Standards
1212 West Street, Suite 200
Annapolis, MD 21401 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 move from Single DES to Triple DEA (TDEA) encryption 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 non-discriminatory 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, 1212 West Street, Suite, Annapolis, MD 21401 USA.

This Technical Report was processed and approved for submittal to 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:
Roy DeCicco, X9 Chairman
Claudia Swendseid, X9 Vice-Chairman
Cynthia Fuller, Executive Director
Janet Busch, Program Manager

Organization Represented	Representative	
ACI Worldwide	Doug	Grote
American Bankers Association	C. Diane	Poole
American Express Company	Ted	Peirce
Apriva	Len	Sutton
Bank of America	Daniel	Welch
Certicom Corporation	Daniel	Brown
Citigroup, Inc.	Karla	McKenna
CUSIP Service Bureau	James	Taylor
Deluxe Corporation	Ralph	Stolp
Diebold, Inc.	Bruce	Chapa
Discover Financial Services	Michelle	Zhang
Federal Reserve Bank	Claudia	Swendseid
First Data Corporation	Rick	Van Luvender
Fiserv	Skip	Smith

FIX Protocol Ltd	Jim	Northey
Harland Clarke	John	McCleary
Hewlett Packard	Larry	Hines
IBM Corporation	Todd	Arnold
Independent Community Bankers of America	Viveca	Ware
Ingenico	John	Spence
ISITC	Tara	Gonzales
J.P. Morgan Chase & Co	Roy	DeCicco
Key Innovations	Scott	Spiker
KPMG LLP	Mark	Lundin
MasterCard International	Mark	Kamers
Metavante Image Solutions	Stephen	Gibson-Saxty
National Association of Convenience Stores	Michael	Davis
NCR Corporation	Steve	Stevens
RouteOne	Mark	Leonard
SWIFT/Pan Americas	Juliette	Kennel
Symantec Corportation	Alex	Deacon
Symcor Inc.	Brian	Salway
TECSEC Incorporated	Ed	Scheidt
The Clearing House	Sharon	Jablon
U.S. Bank	Brian	Fickling
University Bank	Stephen	Ranzini
USDA Food and Nutrition Service	Kathy	Ottobre
VeriFone, Inc.	Brad	McGuinness
VISA	Kim	Wagner
Wells Fargo Bank	Mark	Tiggas
Wincor Nixdorf Inc	Ramesh	Arunashalam
XBRL US, Inc.	Mark	Bolgiano

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

Ed ScheidtChairperson

Organization Represented	**Representative**	
American Bankers Association	Tom	Judd
Bank of America	Andi	Coleman
Burroughs Payments Systems, Inc.	David J.	Concannon
Certicom Corporation	Daniel	Brown
Citigroup, Inc.	Dr. Chii-Ren	Tsai
Communications Security Establishment	Alan	Poplove

Cryptographic Assurance Services	Ralph	Poore
CUSIP Service Bureau	Scott	Preiss
DeLap LLP	Darlene	Kargel
Deluxe Corporation	Andy	Vo
Depository Trust and Clearing Corporation	Mr. Robert	Palatnick
Diebold, Inc.	Bruce	Chapa
Discover Financial Services	Mr. Jordan	Schaefer
Federal Reserve Bank	Deb	Hjortland
Ferris and Associates, Inc.	J. Martin	Ferris
First Data Corporation	Lisa	Curry
Fiserv	Bud	Beattie
GEOBRIDGE Corporation	Jason	Way
Harland Clarke	John	Petrie
Heartland Payment Systems	Glenda	Preen
Hewlett Packard	Larry	Hines
Hypercom	Gary	Zempich
IBM Corporation	Todd	Arnold
InfoGard Laboratories	Doug	Biggs
Ingenico	John	Spence
ITS, Inc. (SHAZAM Networks)	Mr. Manish	Nathwani
J.P. Morgan Chase & Co	Edward	Koslow
Key Innovations	Scott	Spiker
KPMG LLP	Mark	Lundin
MasterCard International	Michael	Ward
Merchant Link	Scott	Franklin
National Institute of Standards and Technology	Elaine	Barker
National Security Agency	Paul	Timmel
NCR Corporation	David	Norris
Pitney Bowes, Inc.	Rick	Ryan
Rosetta Technologies	Jim	Maher
Rosetta Technologies	Paul	Malinowski
Security Innovation	William	Whyte
STAR	Lilik	Kazaryan
Surety, Inc.	Dimitrios	Andivahis
Symcor Inc.	Brian	Salway
TECSEC Incorporated	Ed	Scheidt
Thales e-Security, Inc.	James	Torjussen
Trustwave	John	Amaral
University Bank	Stephen	Ranzini
VeriFone, Inc.	Dave	Faoro
VISA	Kim	Wagner
Voltage Security, Inc.	Luther	Martin

Wells Fargo Bank	Mark	Tiggas
Wincor Nixdorf Inc	Michael	Nolte
World Pay	Dan	Collins

The X9F6 working group that revised this standard consisted of the following members:

John Sheets, Chairperson

Organization Represented	Representative	
ACI Worldwide	Doug	Grote
ACI Worldwide	Dan	Kinney
Apriva	Len	Sutton
Bank of America	Andi	Coleman
DeLap LLP	Darlene	Kargel
Diebold, Inc.	Bruce	Chapa
Diebold, Inc.	Anne	Konecny
Dresser Wayne	Tim	Weston
First Data Corporation	Andrea	Beatty
First Data Corporation	Lisa	Curry
First Data Corporation	Lilik	Kazaryan
Fiserv	Dan	Otten
Futurex	Chris	Hamlett
GEOBRIDGE Corporation	Jason	Way
Gilbarco	Bruce	Welch
Heartland Payment Systems	Sarah	McCrary
Heartland Payment Systems	Glenda	Preen
Hewlett Packard	Larry	Hines
Hewlett Packard	Susan	Langford
Hypercom	Mohammad	Arif
Hypercom	LeAnn	Brown
Hypercom	Gary	Zempich
IBM Corporation	Todd	Arnold
Ingenico	John	Spence
J.P. Morgan Chase & Co	Donna	Meagher
K3DES LLC	Azie	Amini
K3DES LLC	James	Richardson
Keely Consulting	Martha	Keely
Key Innovations	Scott	Spiker
MagTek, Inc.	Larry	Meyers
Merchant Advisory Group	Brad	Andrews
Merchant Advisory Group	Dodd	Roberts
Mustang Microsystems, Inc.	Tom	Galloway

National Association of Convenience Stores	Alan	Thiemann
NCR Corporation	Charlie	Harrow
Pitney Bowes, Inc.	Leon	Pintsov
SafeNet, Inc.	Brett	Thompson
STAR	Scott	Quinn
Thales e-Security, Inc.	Jose	Diaz
Thales e-Security, Inc.	James	Torjussen
VeriFone, Inc.	Dave	Faoro
VeriFone, Inc.	Doug	Manchester
VeriFone, Inc.	Joachim	Vance
VISA	Hap	Huynh
VISA	John	Sheets
VISA	Kim	Wagner
Voltage Security, Inc.	Luther	Martin
Wincor Nixdorf Inc	Michael	Nolte

This is the second release of this document. A new key derivation method has been added. Key types and usages have also been clarified.

This document is to be used in conjunction with implementation of ANS X9.8 and ANS X9.24 Part 1.

X9 TR-31 2010

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 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