This is a preview of "ASC X9 TR 31-2018". Click here to purchase the full version from the ANSI store.

ASC X9 TR 31-2018

Interoperable Secure Key Exchange Key Block Specification

Accredited Standards Committee X9, Incorporated
Financial Industry Standards

Date Registered: April 15, 2018

American National Standards Institute

American National Standards, Technical Reports and Guides developed through the Accredited Standards Committee X9, Inc., are copyrighted. Copying these documents for personal or commercial use outside X9 membership agreements is prohibited without express written permission of the Accredited Standards Committee X9, Inc. For additional information please contact ASC X9, Inc., 275 West Street Suite 107, Annapolis, Maryland 21401 USA.

This is a preview of "ASC X9 TR 31-2018". Click here to purchase the full version from the ANSI store.

This page intentionally left blank

This is a preview of "ASC X9 TR 31-2018". Click here to purchase the full version from the ANSI store.

This is a preview of "ASC X9 TR 31-2018". Click here to purchase the full version from the ANSI store.

Contents **Page**

This is a preview of "ASC X9 TR 31-2018". Click here to purchase the full version from the ANSI store.

Foreword

Publication of this Technical Report that has been registered with ANSI has been approved by the Accredited Standards Committee X9, Incorporated, 275 West Street, Suite 107, Annapolis, MD 21401. 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., 275 West Street, Suite 107, Annapolis, MD 21401,

Published by

Accredited Standards Committee X9, Incorporated
Financial Industry Standards
275 West Street, Suite 107
Annapolis, MD 21401 USA
X9 Online http://www.x9.org

Copyright © 2018 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.

This is a preview of "ASC X9 TR 31-2018". Click here to purchase the full version from the ANSI store.

Introduction

This Technical Report is a product of the Accredited Standards Committee X9 Financial Industry Standards, and was generated by the X9F Data and Information Security Subcommittee. 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.

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, 275 West Street, Suite 107, Annapolis, MD 21401 USA.

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

At the time this Technical Report was published, the X9 committee had the following members:

Roy C. DeCicco, X9 Chair
Angela Hendershott, X9 Vice Chair
Steve Stevens, X9 Executive Director
Janet Busch, Program Manager

Organization Represented	*Representative*
ACI Worldwide	Doug Grote
American Bankers Association	Diane Poole
American Express Company	David Moore
Bank of America	Daniel Welch
Bank of New York Mellon	Arthur Sutton
Blackhawk Network	Anthony Redondo
Bloomberg LP	Corby Dear
Capital One	Marie LaQuerre
Citigroup, Inc.	Karla McKenna
CLS Bank	Ram Komarraju
Conexxus, Inc.	Gray Taylor
CUSIP Service Bureau	Gerard Faulkner
Delap LLP	Andrea Beatty
Deluxe Corporation	Angela Hendershott
Diebold Nixdorf	Bruce Chapa
Discover Financial Services	Michelle Zhang
Dover Fueling Solutions	Steven Bowles
Dover Fueling Solutions	Bradford Loewy
eCurrency	David Wen
Federal Reserve Bank	Mary Hughes
First Data Corporation	Lisa Curry
FIS	Stephen Gibson-Saxty
Fiserv	Dan Otten

© ASC X9, Inc. 2018 – All rights reserved

This is a preview of "ASC X9 TR 31-2018". Click here to purchase the full version from the ANSI store.

FIX Protocol Ltd - FPL	Jim Northey
Futurex	Ryan Smith
Gilbarco	Bruce Welch
Harland Clarke	John McCleary
IBM Corporation	Todd Arnold
Ingenico	Rob Martin
ISARA Corporation	Alexander Truskovsky
ISITC	Lisa Iagatta
ITS, Inc. (SHAZAM Networks)	Manish Nathwani
J.P. Morgan Chase	Roy DeCicco
MagTek, Inc.	Mimi Hart
MasterCard Europe Sprl	Mark Kamers
NACHA The Electronic Payments Association	Priscilla Holland
National Security Agency	Paul Timmel
Nautilus Hyosung	Joe Militello
NCR Corporation	David Norris
Office of Financial Research, U.S. Treasury Department	Thomas Brown Jr.
PCI Security Standards Council	Troy Leach
RouteOne	Chris Irving
RouteOne	Jenna Wolfe
SWIFT/Pan Americas	Karin DeRidder
SWIFT/Pan Americas	Frank Vandriessche
Symcor Inc.	Debbi Fitzpatrick
TECSEC Incorporated	Ed Scheidt
The Clearing House	Sharon Jablon
U.S. Bank	John King
U.S. Commodity Futures Trading Commission (CFTC)	Robert Stowsky
USDA Food and Nutrition Service	Kathy Ottobre
Vantiv LLC	John Hall
VeriFone, Inc.	Dave Faoro
Viewpointe	Richard Luchak
VISA	Kim Wagner
Wells Fargo Bank	Mark Schaffer

© ASC X9, Inc. 2018 – All rights reserved

This is a preview of "ASC X9 TR 31-2018". Click here to purchase the full version from the ANSI store.

The X9F subcommittee on Data and Information Security had the following members:

Dave Faoro, Chair
Steven Bowles, Vice Chair
Ed Scheidt, Vice Chair

Organization Represented	*Representative*
ACI Worldwide	Doug Grote
ACI Worldwide	Dan Kinney
ACI Worldwide	Julie Samson
American Bankers Association	Tom Judd
American Express Company	Gail Chapman
American Express Company	Farid Hatefi
American Express Company	David Moore
American Express Company	John Timar
American Express Company	Kevin Welsh
Bank of America	Amanda Adams
Bank of America	Peter Capraro
Bank of America	Andi Coleman
Bank of America	Lawrence LaBella
Bank of America	Will Robinson
Bank of America	Michael Smith
Bank of America	Daniel Welch
BlackBerry Limited	Daniel Brown
Blackhawk Network	Vijay Bolina
Blackhawk Network	Anthony Redondo
Bloomberg LP	Erik Anderson
Bloomberg LP	Corby Dear
Capital One	Marie LaQuerre
Capital One	Johnny Lee
Cipherithm	Scott Spiker
comForte 21 GmbH	Thomas Gloerfeld
comForte 21 GmbH	Henning Horst
Communications Security Establishment	Jonathan Hammell
Communications Security Establishment	David Smith
Conexxus, Inc.	Alan Thiemann
CUSIP Service Bureau	Scott Preiss
Delap LLP	Andrea Beatty
Delap LLP	David Buchanan
Deluxe Corporation	Angela Hendershott
Deluxe Corporation	Margiore Romay
Deluxe Corporation	Andy Vo
Diebold Nixdorf	Christoph Bruecher
Diebold Nixdorf	Andrea Carozzi
Diebold Nixdorf	Bruce Chapa
Diebold Nixdorf	Michael Nolte
Diebold Nixdorf	Michael Ott
Diebold Nixdorf	Dave Phister
Digicert	Tim Hollebeek
Discover Financial Services	Cheryl Mish
Discover Financial Services	Diana Pauliks
Discover Financial Services	Jordan Schaefer
Dover Fueling Solutions	Steven Bowles
Dover Fueling Solutions	Bradford Loewy

© ASC X9, Inc. 2018 – All rights reserved

This is a preview of "ASC X9 TR 31-2018". Click here to purchase the full version from the ANSI store.

eCurrency	David Wen
Federal Reserve Bank	Patrick Adler
Federal Reserve Bank	Guy Berg
Federal Reserve Bank	Marianne Crowe
Federal Reserve Bank	Amanda Dorphy
Federal Reserve Bank	Mary Hughes
Federal Reserve Bank	Heather Hultquist
Federal Reserve Bank	Janet LaFrence
Federal Reserve Bank	Susan Pandy
Federal Reserve Bank	Patti Ritter
First Data Corporation	Lisa Curry
First Data Corporation	Kalli Davidson
First National Bank of Omaha	Sherry Rewolinski
First National Bank of Omaha	Kristi White
FIS	Saman Amighi
FIS	John Soares
FIS	Sunny Wear
Fiserv	Bud Beattie
Fiserv	Dan Otten
Futurex	Ryan Smith
Futurex	Tim Weston
GEOBRIDGE Corporation	Donna Gem
GEOBRIDGE Corporation	Jason Way
Gilbarco	Scott Turner
Gilbarco	Bruce Welch
Harland Clarke	Joseph Filer
Heartland Payment Systems	Scott Meeker
IBM Corporation	Todd Arnold
IBM Corporation	Richard Kisley
Ingenico	Nabil Hamzi
Ingenico	Rob Martin
ISARA Corporation	Mike Brown
ISARA Corporation	Philip Lafrance
ISARA Corporation	Alexander Truskovsky
ITS, Inc. (SHAZAM Networks)	Manish Nathwani
J.P. Morgan Chase	Kathleen Krupa
J.P. Morgan Chase	Jackie Pagán
J.P. Morgan Chase	Darryl Scott
K3DES LLC	Azie Amini
MagTek, Inc.	Jeff Duncan
MagTek, Inc.	Mimi Hart
MasterCard Europe Sprl	Mark Kamers
MasterCard Europe Sprl	Joshua Knopp
MasterCard Europe Sprl	Larry Newell
MasterCard Europe Sprl	Adam Sommer
MasterCard Europe Sprl	Michael Ward
Micro Focus	Luther Martin
National Institute of Standards and Technology (NIST)	Elaine Barker
National Institute of Standards and Technology (NIST)	Lily Chen
National Security Agency	Mike Boyle
National Security Agency	Paul Timmel
Nautilus Hyosung	Joe Militello
Nautilus Hyosung	Jay Shin
NCR Corporation	Tanika Eng
NCR Corporation	Charlie Harrow

© ASC X9, Inc. 2018 – All rights reserved

This is a preview of "ASC X9 TR 31-2018". Click here to purchase the full version from the ANSI store.

NCR Corporation	David Norris
Onboard Security	Mark Etzel
Onboard Security	Virendra Kumar
Onboard Security	William Whyte
Onboard Security	Lee Wilson
Onboard Security	Zhenfei Zhang
PCI Security Standards Council	Leon Fell
PCI Security Standards Council	Troy Leach
PCI Security Standards Council	Ralph Poore
RSA, The Security Division of EMC	Steve Schmalz
SafeNet Infotech Pvt. Ltd.	Amit Sinha
SafeNet Infotech Pvt. Ltd.	Devesh Tewari
Safeway	Gary Zempich
TECSEC Incorporated	Ed Scheidt
TECSEC Incorporated	Dr. Wai Tsang
TECSEC Incorporated	Jay Wack
Thales UK Limited	Larry Hines
Thales UK Limited	James Torjussen
The Clearing House	Mark Fitlin
The Clearing House	Sharon Jablon
The Clearing House	Hirak Patel
The Clearing House	Miguel Sanchez
Trustwave	John Amaral
U.S. Bank	Stephen Case
U.S. Bank	Peter Skirvin
Vantiv LLC	John Hall
Vantiv LLC	Jeffrey Singleton
Vantiv LLC	Bill Weingart
VeriFone, Inc.	John Barrowman
VeriFone, Inc.	David Ezell
VeriFone, Inc.	Dave Faoro
VeriFone, Inc.	Doug Manchester
VeriFone, Inc.	Brad McGuinness
VeriFone, Inc.	Saxon Noh
VeriFone, Inc.	Joachim Vance
VISA	Shahzad Khan
VISA	Eric Le Saint
VISA	Kim Wagner
Wells Fargo Bank	Allen Ausec
Wells Fargo Bank	David Cooper
Wells Fargo Bank	William Felts, IV
Wells Fargo Bank	Matthew Greenwell
Wells Fargo Bank	Phillip Griffin
Wells Fargo Bank	Jan Kohl
Wells Fargo Bank	Garrett Macey
Wells Fargo Bank	Kelly O'Donnell
Wells Fargo Bank	Mark Schaffer
Wells Fargo Bank	Maria Schuett
Wells Fargo Bank	Jeff Stapleton
White and Williams LLP	Emma Bechara
White and Williams LLP	Richard Borden
White and Williams LLP	Joshua Mooney
White and Williams LLP	Laura Schmidt
White and Williams LLP	Kate Woods
XYPRO Technology	Steve Tcherchian

© ASC X9, Inc. 2018 – All rights reserved

This is a preview of "ASC X9 TR 31-2018". Click here to purchase the full version from the ANSI store.

Under ASC X9, Inc. procedures, a working group may be established to address specific segments of work under the ASC X9 Committee or one of its subcommittees. A working group exists only to develop standard(s) or guideline(s) in a specific area and is then disbanded. The individual experts are listed with their affiliated organizations. However, this does not imply that the organization has approved the content of the standard or guideline. (Note: Per X9 policy, company names of non-member participants are listed only if, at the time of publication, the X9 Secretariat received an original signed release permitting such company names to appear in print.)

The X9F6 Cardholder Authentication and ICC's group which developed this standard had the following members:

Scott Spiker, Chair
Andrea Beatty, Vice Chair
Larry Hines, Project Editor

Organization Represented	*Representative*
ACI Worldwide	Doug Grote
ACI Worldwide	Dan Kinney
ACI Worldwide	Julie Samson
American Bankers Association	Tom Judd
American Express Company	Gail Chapman
American Express Company	Alan Fong
American Express Company	Michael Hyzer
American Express Company	Kenneth Mealey
American Express Company	David Moore
American Express Company	Hing Too
American Express Company	Clyde Van Blarcum
American Express Company	Kevin Welsh
Bank of America	Amanda Adams
Bank of America	Dion Bellamy
Bank of America	Peter Capraro
Bank of America	Terrelle Carswell
Bank of America	Andi Coleman
Bank of America	Chuck Gruesbeck
Bank of America	Lawrence LaBella
Bank of America	Chris Schrick
Bank of America	Michael Smith
Bank of America	Daniel Welch
Bank of America	Terri Willis
BetterBuyDesign	Steve Mott
BlackBerry Limited	Daniel Brown
BlackBerry Limited	John O. Goyo
Blackhawk Network	Vijay Bolina
Blackhawk Network	Anthony Redondo
Bloomberg LP	Erik Anderson
Capital One	Johnny Lee
Cipherithm	Scott Spiker
comForte 21 GmbH	Henning Horst
comForte 21 GmbH	Michael Horst
Conduent	Jennifer Baur
Conexxus, Inc.	Ann Seki
Conexxus, Inc.	Alan Thiemann
Conexxus, Inc.	Linda Toth
CUSIP Service Bureau	Scott Preiss
Delap LLP	Andrea Beatty

© ASC X9, Inc. 2018 – All rights reserved

This is a preview of "ASC X9 TR 31-2018". Click here to purchase the full version from the ANSI store.

Delap LLP	David Buchanan
Diebold Nixdorf	Christoph Bruecher
Diebold Nixdorf	Rick Brunt
Diebold Nixdorf	Andrea Carozzi
Diebold Nixdorf	Bruce Chapa
Diebold Nixdorf	Scott Harroff
Diebold Nixdorf	Anne Konecny
Diebold Nixdorf	Michael Nolte
Diebold Nixdorf	Michael Ott
Diebold Nixdorf	Dave Phister
Diebold Nixdorf	Matthias Runowski
Digicert	Tim Hollebeek
Discover Financial Services	Debbie Holfeld
Discover Financial Services	David Kloser
Discover Financial Services	Cheryl Mish
Discover Financial Services	Diana Pauliks
Discover Financial Services	Julie Quandt
Discover Financial Services	Lakshmi Ramanathan
Discover Financial Services	Jordan Schaefer
Discover Financial Services	Michelle Zhang
Dover Fueling Solutions	Steven Bowles
Dover Fueling Solutions	Bradford Loewy
eCurrency	David Wen
Federal Reserve Bank	Patrick Adler
Federal Reserve Bank	Guy Berg
Federal Reserve Bank	Pieralberto Deganello
Federal Reserve Bank	Amanda Dorphy
Federal Reserve Bank	Mary Hughes
Federal Reserve Bank	Heather Hultquist
Federal Reserve Bank	Bob Hunt
Federal Reserve Bank	Janet LaFrence
Federal Reserve Bank	Paul Nunnally
Federal Reserve Bank	Susan Pandy
Federal Reserve Bank	John Rhodes
Federal Reserve Bank	Patti Ritter
Federal Reserve Bank	Charles Tsai
First Data Corporation	Lisa Curry
First Data Corporation	Kerry Deardorff
First Data Corporation	Jodi Delaney
First Data Corporation	Jacqueline Dill
First Data Corporation	Angela Ghetu
First Data Corporation	Brian Kean
First Data Corporation	Brian Murray
First Data Corporation	Randall Rieth
First National Bank of Omaha	Sherry Rewolinski
First National Bank of Omaha	Kristi White
FIS	Tami Harris
Fiserv	Bud Beattie
Fiserv	Dan Otten
Futurex	Chris Hamlett
Futurex	Ryan Smith
Futurex	Tim Weston
GEOBRIDGE Corporation	Donna Gem
GEOBRIDGE Corporation	Dean Macinskas
GEOBRIDGE Corporation	Jason Way

© ASC X9, Inc. 2018 – All rights reserved

This is a preview of "ASC X9 TR 31-2018". Click here to purchase the full version from the ANSI store.

Gilbarco	Scott Turner
Gilbarco	Bruce Welch
Harland Clarke	John McCleary
Heartland Payment Systems	Kevin Halliburton
Heartland Payment Systems	Randy Ison
Heartland Payment Systems	John Masden
Heartland Payment Systems	Scott Meeker
IBM Corporation	Todd Arnold
IBM Corporation	Richard Kisley
ID TECH	Eric Lecesne
Ingenico	Rob Martin
Ingenico	Steve McKibben
ISARA Corporation	Mike Brown
ISARA Corporation	Philip Lafrance
ISARA Corporation	Alexander Truskovsky
ITS, Inc. (SHAZAM Networks)	Manish Nathwani
J.P. Morgan Chase	Kathleen Krupa
J.P. Morgan Chase	Jackie Pagán
J.P. Morgan Chase	Darryl Scott
K3DES LLC	Azie Amini
K3DES LLC	James Richardson
MagTek, Inc.	Jeff Duncan
MagTek, Inc.	Mimi Hart
Mainsail Trim, Inc.	Norman Cecil
MasterCard Europe Sprl	Mark Kamers
MasterCard Europe Sprl	Joshua Knopp
MasterCard Europe Sprl	Susie Thompson
MasterCard Europe Sprl	Michael Ward
MasterCard Europe Sprl	Gregory Williamson
Micro Focus	Priyank Kumar
Micro Focus	Susan Langford
National Institute of Standards and Technology (NIST)	Elaine Barker
National Institute of Standards and Technology (NIST)	Lawrence Bassham III
National Institute of Standards and Technology (NIST)	Lily Chen
National Institute of Standards and Technology (NIST)	David Cooper
National Institute of Standards and Technology (NIST)	Morris Dworkin
National Institute of Standards and Technology (NIST)	Randall Easter
National Institute of Standards and Technology (NIST)	Sharon Keller
National Institute of Standards and Technology (NIST)	Annabelle Lee
National Institute of Standards and Technology (NIST)	Fernando Podio
National Security Agency	Paul Timmel
Nautilus Hyosung	Joe Militello
Nautilus Hyosung	Jay Shin
NCR Corporation	Tanika Eng
NCR Corporation	Charlie Harrow
NCR Corporation	David Norris
NCR Corporation	Brian Wotherspoon
Onboard Security	Mark Etzel
Onboard Security	Jeff Hoffstein
Onboard Security	William Whyte
PCI Security Standards Council	Leon Fell
PCI Security Standards Council	Troy Leach
PCI Security Standards Council	Ralph Poore
Richard Sweeney	Richard Sweeney
RSA, The Security Division of EMC	Steve Schmalz

© ASC X9, Inc. 2018 – All rights reserved

This is a preview of "ASC X9 TR 31-2018". Click here to purchase the full version from the ANSI store.

SafeNet Infotech Pvt. Ltd.	Amit Sinha
SafeNet Infotech Pvt. Ltd.	Devesh Tewari
Safeway	Gary Zempich
TECSEC Incorporated	Ed Scheidt
TECSEC Incorporated	Dr. Wai Tsang
TECSEC Incorporated	Jay Wack
Thales UK Limited	Colette Broadway
Thales UK Limited	Larry Hines
Thales UK Limited	James Torjussen
The Clearing House	Sharon Jablon
Trustwave	John Amaral
U.S. Bank	Stephen Case
U.S. Bank	Dave Esmond
U.S. Bank	Peter Skirvin
USDA Food and Nutrition Service	Erin McBride
USDA Food and Nutrition Service	Kathy Ottobre
Vantiv LLC	Chris Doyle
Vantiv LLC	John Hall
Vantiv LLC	Jeffrey Singleton
Vantiv LLC	Bill Weingart
VeriFone, Inc.	John Barrowman
VeriFone, Inc.	David Ezell
VeriFone, Inc.	Dave Faoro
VeriFone, Inc.	LeAnn Hostetler
VeriFone, Inc.	Chris Madden
VeriFone, Inc.	Doug Manchester
VeriFone, Inc.	Brad McGuinness
VeriFone, Inc.	Joachim Vance
VISA	Adam Clark
VISA	Hap Huynh
VISA	Shahzad Khan
VISA	Chackan Lai
VISA	Stoddard Lambertson
VISA	Sekhar Nagasundaram
VISA	Michael Stefanich
VISA	Johan ("Hans") Van Tilburg
VISA	Kim Wagner
Wells Fargo Bank	Sotos Barkas
Wells Fargo Bank	William Felts, IV
Wells Fargo Bank	Andrew Garner
Wells Fargo Bank	Matthew Greenwell
Wells Fargo Bank	Phillip Griffin
Wells Fargo Bank	Sam Grosby
Wells Fargo Bank	Ryan Hegland
Wells Fargo Bank	Jeff Jacoby
Wells Fargo Bank	Brian Keltner
Wells Fargo Bank	Jan Kohl
Wells Fargo Bank	Eric Lengvenis
Wells Fargo Bank	Garrett Macey
Wells Fargo Bank	Brian Parks
Wells Fargo Bank	Doug Pelton
Wells Fargo Bank	Jeff Stapleton
Wells Fargo Bank	Tony Stieber
XYPRO Technology	Steve Tcherchian

© ASC X9, Inc. 2018 – All rights reserved

This is a preview of "ASC X9 TR 31-2018". Click here to purchase the full version from the ANSI store.

This document cancels and replaces TR-31 2010 Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms in whole and includes support for AES key management and public key distribution. This document represents an implementation method that is consistent with requirements in X9.24 parts 1 & 2.

© ASC X9, Inc. 2018 – All rights reserved

This is a preview of "ASC X9 TR 31-2018". Click here to purchase the full version from the ANSI store.

This is a preview of "ASC X9 TR 31-2018". Click here to purchase the full version from the ANSI store.

Interoperable Secure Key Exchange Key Block Specification

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 Normative 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: 1999 Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 1: Mechanisms using a block cipher
6. ISO 9797: 2011 Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 1: Mechanisms using a block cipher
7. ANS X9 TR-39: TG 3 PIN Security Compliance Guideline
8. ANS X9 TG 7 Initial DEA Key Distribution for PIN Entry and Transaction Originating Devices Guideline
9. ISO 16609-2004, Banking – Requirements for message authentication using symmetric techniques
10. NIST SP 800-38B, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication
11. NIST SP 800-108, Recommendation for Key Derivation Using Pseudorandom Functions.
12. FIPS 197 Advanced Encryption Standard (AES), November 26, 2001
13. FIPS 198-1 The Keyed-Hash Message Authentication Code (HMAC), July 2008

© ASC X9, Inc. 2018 – All rights reserved