American National Standard for Financial Services

ANSI X9.143-2022

Retail Financial Services

Interoperable Secure Key Block Specification

Accredited Standards Committee X9, Incorporated

Financial Industry Standards

Date Approved: May 6, 2022

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 page intentionally left blank

Contents **Page**

Foreword viii
Introduction ix
1 Scope 1
2 Normative references 1
3 Terms and definitions 2
3.1 AES 2
3.2 ASCII 2
3.3 Authentication Value 2
3.4 CAPI 2
3.5 CBC 2
3.6 Crypto-agility 2
3.7 Cryptographic Domain 2
3.8 DEA 2
3.9 ECC 2
3.10 EMV 2
3.11 hex-ASCII 2
3.12 ID 3
3.13 Initialization Vector (IV) 3
3.14 KBH 3
3.15 Key Block 3
3.16 Key Block Encryption Key (KBEK) 3
3.17 Key Block Authentication Key (KBAK) 3
3.18 Key Block Protection Key (KBPK) 3
3.19 Key Encrypting Key (KEK) 3
3.20 Key Export 3
3.21 Key Import 3
3.22 Key Wrapping Key 3
3.23 Key Wrapping Mechanism 4
3.24 Master File Key (MFK) 4
3.25 Message Authentication Code (MAC) 4
3.26 PIN 4
3.27 Pseudorandom Function 4
3.28 Secure Cryptographic Device (SCD) 4
3.29 Subkey 4
3.30 TCBC 4
3.31 TDEA 4
3.32 Unwrapping 4
3.33 Wrapping 4
4 Notations and Symbols 5
5 Key Block Elements 6
6 Key Block Format 6
6.1 Introduction 6
6.2 Key Block Header (KBH) 7
6.2.1 Changing Key Headers 11
6.3 Defined values for Key Block Headers 12
6.3.1 Key Usage 12
6.3.2 Algorithm 18
6.3.3 Mode of Use 19
6.3.4 Key Version Number 20
6.3.5 Exportability 20
6.3.6 Optional Block ID 21
6.4 Encoding 46
6.4.1 RSA Key Pairs 47
6.4.2 Elliptic Curve Cryptography (ECC) Key Pairs 48

7 Key Block Binding and Validation Methods 48
7.1 General 48
7.2 Key Block Binding Method Using Key Derivation (Preferred) 49
7.2.1 Key Block Binding Method – AES 49
7.2.2 Key Block Binding Method – TDEA 54
7.3 Key Block Binding Method Using Variants (TDEA only) 58
7.3.1 Key Variant Binding Method 58
7.3.2 Key Variant Binding Validation Method 59
8 Examples 60
8.1 AES Key Block Example 60
8.1.1 Introduction 60
8.1.2 Constructing the Key Block Header 60
8.2 AES Key Block with Optional Blocks 68
8.2.1 Using AES Key Derivation Binding Method for CBC mode 68
8.3 TDEA Key Block Examples 71
8.3.1 Notation Used 71
8.3.2 Example 1: TDEA Key Block without Optional Blocks 71
8.4 TDEA Key Block with Optional Block 80
8.4.1 Example 2a: Using Key Variant Binding Method 80
8.4.2 Example 2b: Using Key Derivation Binding Method 83
8.5 RSA Key Block Example with CT Optional Block 91
8.5.1 Keys used in the example 91
8.5.2 Constructing the Key Block Header 93
8.5.3 Constructing the Binary Key Data 95
8.5.4 Constructing the complete Key Block 97
8.6 ECC Key Block Example with CT Certificate Chain Optional Block 99
8.6.1 Keys used in the example 99
8.6.2 Constructing the Key Block Header 100
8.6.3 Constructing the Binary Key Data 103
8.6.4 Constructing the complete Key Block 103
Annex A. (Informative) Operational Challenges and Examples with Exportability 105

© ASC X9, Inc. 2022 – All rights reserved

Tables

Table 1 – Key Block Header 8
Table 2 - Defined Key Usage Values 12
Table 3 - Defined Algorithm Values 18
Table 4 - Defined Mode of Use Values 19
Table 5 - Key Version Number definition 20
Table 6 - Defined Values for Exportability Byte 21
Table 7 - Defined Values for Optional Block ID 22
Table 8 - Key Derivation Input Data 24
Table 9 - Base Derivation Key identifier for DUKPT Optional Block Format 24
Table 10 - Public Key Certificate Optional Block Format - Single Certificate 25
Table 11 - Public Key Certificate Optional Block Format - Certificate Chain 26
Table 12 - Derivation(s) Allowed Optional Block Format 36
Table 13 - HMAC Optional Block Format 38
Table 14 - Initial Key identifier for AES DUKPT Optional Block Format 39
Table 15 - KCV Optional Block Format 39
Table 16 - Initial Key Serial Number for DUKPT Optional Block Format 40
Table 17 - Key Block Values Version IDs Optional Block 40
Table 18 - Label Optional Block 41
Table 20 - Proprietary Algorithm Optional Block 41
Table 19 - Padding Block Optional Block 42
Table 20 - Protection Key Check Value Optional Block 43
Table 21 - Time of Creation Optional Block 43
Table 22 - Time Stamp Optional Block 45
Table 23 - Wrapping Pedigree Optional Block 46
Table 24 - Key Derivation Input Data 49
Table 25 - Key Derivation Input Data 54
Table 26 - Example of confidential data for a double-length TDEA key 59
Table 27 - AES Key Block Example Header 61
Table 28 - Values for Example 65
Table 29 - AES Key Block with Optional Blocks Example Header 69
Table 30 - TDEA Key Block without Optional Blocks Example Header 72
Table 31 - TDEA Key Block 'B' without Optional Blocks Example Header 74
Table 32 - Values for Example 78
Table 33 - TDEA Key Block 'C' with Optional Blocks Example Header 81
Table 34 - TDEA Key Block 'B' with Optional Blocks Example Header 83
Table 35 - Values for Example 88
Table 36 - AES Key Block with Optional Blocks Example Header 94
Table 37 - AES Key Block with Optional Blocks Example Header 100

© ASC X9, Inc. 2022 – All rights reserved

Figures

Figure 1 - Key Block 6
Figure 2 - Key Block 7
Figure 3 - Examples of KBH and Optional Blocks 22
Figure 4 - Deriving an AES-128 KBEK and KBAK 50
Figure 5 - Deriving an AES-192 Encryption and Authentication key 51
Figure 6 - Deriving an AES-256 Encryption and Authentication key 52
Figure 7 - AES Key Block Binding Method 53
Figure 8 - Deriving a 2-Key TDEA MAC and Encryption Key 55
Figure 9 - Deriving a 3-Key TDEA Authentication (MAC) and Encryption Key 56
Figure 10 - Key Block Binding Method 57
Figure 11 - Key Variant Binding Method 58
Figure 12 - Deriving the Key Block Encryption Key from the Key Block Protection Key 64
Figure 13 - Derivation of the Key Block Authentication key from the Key Block Protection Key 65
Figure 14 - CMAC Subkey Derivation from the Key Block Authentication key 67
Figure 15 - CMAC Subkey Derivation from the Key Block Protection Key 76
Figure 16 - Deriving the Key Block Encryption Key from the Key Block Protection Key 77
Figure 17 - Derivation of the Key Block Authentication key from the Key Block Protection Key 78
Figure 18 - CMAC Subkey Derivation from the Key Block Authentication key 79
Figure 19 - CMAC Subkey Derivation from the Key Block Protection Key 86
Figure 20 - Deriving the Key Block Encryption Key from the Key Block Protection Key 87
Figure 21 - Derivation of the Key Block Authentication key from the Key Block Protection Key 88
Figure 22 - CMAC Subkey Derivation from the KBAK 90
Figure 28 - Key export control for transfer between HSMs with different MFKs 108
Figure 29 - Key export control in a multi-node environment with a Key Management System 109
Figure 30 - KMS Distribution to Two Nodes 110
Figure 31 - MFK Translation 111
Figure 32 - Key Export Control for DUKPT Initial Keys 113

© ASC X9, Inc. 2022 – All rights reserved

Foreword

Approval of an American National Standard requires verification by ANSI that the requirements for due process, consensus, and other criteria for approval have been met by the standards developer.

Consensus is established when, in the judgment of the ANSI Board of Standards Review, substantial agreement has been reached by directly and materially affected interests. Substantial agreement means much more than a simple majority, but not necessarily unanimity. Consensus requires that all views and objections be considered, and that a concerted effort be made toward their resolution.

The use of American National Standards is completely voluntary; their existence does not in any respect preclude anyone, whether he has approved the standards or not from manufacturing, marketing, purchasing, or using products, processes, or procedures not conforming to the standards.

The American National Standards Institute does not develop standards and will in no circumstances give an interpretation of any American National Standard. Moreover, no person **SHALL** have the right or authority to issue an interpretation of an American National Standard in the name of the American National Standards Institute. Requests for interpretation **SHOULD** be addressed to the secretariat or sponsor whose name appears on the title page of this standard.

CAUTION NOTICE: This American National Standard 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 standard no later than five years from the date of approval.

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 © 2022 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.

© ASC X9, Inc. 2022 – All rights reserved

Introduction

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

By publication of this standard, 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.

ANSI X9.143 is intended to give the reader an implementation that meets the requirements for secure key management as set forth in ANSI X9.24 Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques. This standard updates and formalizes the methods published in ASC X9 TR 31-2018. This enhances the support for compatibility requirements for exchange of keys according to the requirements as set forth in ANSI X9.24.

Cryptographic Sunset

The Financial Services industry is migrating to AES. References to TDEA in this standard, are included for backward compatibility. But a sunset date of TDEA may be announced prior to the release of the next version of this standard. New applications should use AES. Migration away from TDEA is currently recommended. TDEA should not be used for new implementations.

Migration considerations and impacts related to the sunset of TDEA should include the concept of creating crypto-agility within your environment to enable adoption of new algorithms.

Quantum Readiness

Large-scale Quantum Computers are a threat to the security of asymmetric algorithms. New Post Quantum Cryptography methods are being investigated and vetted for use within the Financial Services industry. At the time of publication of this version of this standard, the methods remain undecided. It should be assumed that any key protected by asymmetric techniques, will need to be changed for security if a large-scale Quantum Computer becomes a reality.

While this standard focuses on symmetric key wrapping, it is important to remember that the Key Block Protection Key may have been exchanged by asymmetric techniques and is subject to risk of compromise due to Quantum Computing. Compromise would require changing the Key Block Protection Key and all keys protected by it.

The cryptographic systems most at risk from attack by a quantum computer are those based on asymmetric algorithms. Symmetric algorithms, such as AES, are not immune from attack from quantum computing. But in the best known symmetric key attack (Grover's algorithm) the security of symmetric key algorithms can be preserved by doubling the length of the key. For example, an AES 256-bit symmetric key will have at least as much security against a Quantum Computer as an AES 128-bit symmetric key has against a classical computer and is hence believed to be intractable to attack. Currently, due to the understanding that large-scale quantum computers cannot parallelize or quickly run Grover's algorithm, quantum computing is not expected to provide a significant advantage in attacking symmetric algorithms. NIST guidance is that AES 128-bit is expected to remain secure from quantum attack and that key doubling to protect against quantum computing is unnecessary at this time. See: https://csrc.nist.gov/Projects/post-quantum-cryptography/faqs#xisl

For further information, see ASCX9 IR 01-2019, Quantum Computing Risks to the Financial Services Industry.

Suggestions for the improvement or revision of this Standard are welcome. They should be sent to the X9 Committee Secretariat, Accredited Standards Committee X9, Inc., Financial Industry Standards, 275 West Street, Suite 200, Annapolis, MD 21401 USA.

© ASC X9, Inc. 2022 – All rights reserved

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

© ASC X9, Inc. 2022 – All rights reserved

The X9 committee had the following members:

Corby Dear, X9 Chairman

Michelle Wright, X9 Vice Chairman

Steve Stevens, X9 Executive Director

Janet Busch, Program Manager

Ambria Frazier, Program Manager

Organization Represented	*Representative*
ACI Worldwide	Julie Samson
Amazon	Tyler Messa
American Bankers Association	Tab Stewart
American Express Company	Marshall Williams
Arvest Bank	Yurik Paroubek
Bank of America	Daniel Welch
Bank of New York Mellon	Kevin Barnes
BankVOD	Sean Dunlea
Bloomberg LP	Corby Dear
Capital One	Valerie Hodge
Citigroup, Inc.	David Edelman
Conexxus, Inc.	Alan Thiemann
CUSIP Global Services	Gerard Faulkner
Delap LLP	Andrea Beatty
Deluxe Corporation	Andy Vo
Diebold Nixdorf	Bruce Chapa
Digicert	Dean Coclin
Discover Financial Services	Susan Pandy
Dover Fueling Solutions	Simon Siew
Federal Reserve Bank	Ainsley Hargest
FirstBank	Ryan Buerger
FIS	Stephen Gibson-Saxty
Fiserv	Lisa Curry
FIX Protocol Ltd - FPL	James Northey
Futurex	Ryan Smith
Gilbarco	Bruce Welch
Harland Clarke/Vericast	Jonathan Lee
Hyosung TNS Inc.	Joe Militello
IBM Corporation	Richard Kisley

© ASC X9, Inc. 2022 – All rights reserved

Ingenico	Steven Bowles
ISITC	Lisa Iagatta
ITS, Inc. (SHAZAM Networks)	Manish Nathwani
J.P. Morgan Chase	Ted Rothschild
MasterCard Europe Sprl	Mark Kamers
NACHA The Electronic Payments Association	George Throckmorton
National Security Agency	Mike Boyle
NCR Corporation	Charlie Harrow
Office of Financial Research, U.S. Treasury Department	Thomas Brown Jr.
PCI Security Standards Council	Ralph Poore
PNC Bank	David Bliss
SWIFT/Pan Americas	Anne Suprenant
TECSEC Incorporated	Ed Scheidt
Thales DIS CPL USA Inc	James Torjussen
The Clearing House	Sharon Jablon
U.S. Bank	Michelle Wright
U.S. Commodity Futures Trading Commission (CFTC)	Robert Stowsky
University Bank	Stephen Ranzini
USDA Food and Nutrition Service	Lisa Gifaldi
Valley Bank	Michael Duffner
VeriFone, Inc.	Joachim Vance
Viewpointe	Richard Luchak
VISA	Kristina Breen
Wells Fargo Bank	Sotos Barkas
Wolters Kluwer	Colleen Knuff
Zions Bank	Kay Hall

© ASC X9, Inc. 2022 – All rights reserved

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

Steven Bowles, Chairman
Richard Kisley, Vice Chairman
Ed Scheidt, Vice Chairman

Organization Represented	*Representative*
ACI Worldwide	Julie Samson
Amazon	Sean Estrada
Amazon	Sandra Lambert
American Bankers Association	Tab Stewart
American Express Company	Gail Chapman
American Express Company	Farid Hatefi
American Express Company	Peter Markall
American Express Company	John Timar
American Express Company	Kevin Welsh
Bank of America	Amanda Adams
Bank of America	Andi Coleman
Bank of America	Terry McKinney
Bank of America	Matt Sharp
Bank of America	Michael Smith
Bank of America	Daniel Welch
BDO	Tim Crawford
Bloomberg LP	Erik Anderson
Bloomberg LP	Corby Dear
Capital One	Johnny Lee
Citigroup, Inc.	Sudha Iyer
comforte AG	Thomas Gloerfeld
comforte AG	Henning Horst
Communications Security Establishment	Jonathan Hammell
Conexxus, Inc.	David Ezell
Conexxus, Inc.	Alan Thiemann
Consultant	David Cooper
CUSIP Global Services	Scott Preiss
Delap LLP	Andrea Beatty
Delap LLP	Diane Bishop
Delap LLP	David Buchanan

© ASC X9, Inc. 2022 – All rights reserved

Deluxe Corporation	Andy Vo
Diebold Nixdorf	Christoph Bruecher
Diebold Nixdorf	Bruce Chapa
Digicert	Tim Hollebeek
Discover Financial Services	Susan Pandy
Discover Financial Services	Jordan Schaefer
Discover Financial Services	Jorge Vargas
Federal Reserve Bank	Guy Berg
Federal Reserve Bank	Marianne Crowe
Federal Reserve Bank	Ainsley Hargest
Federal Reserve Bank	Patti Ritter
First National Bank of Omaha	Robert Lamagna-Reiter
First National Bank of Omaha	Sherry Rewolinski
First National Bank of Omaha	Kristi White
Fiserv	Bud Beattie
Fiserv	Lisa Curry
Fiserv	Vinayak Kagalkar
Fiserv	Dan Otten
Futurex	Comron Moeni
Futurex	Ryan Smith
Futurex	Tim Weston
GEOBRIDGE Corporation	Jason Way
Gilbarco	Scott Turner
Gilbarco	Bruce Welch
Hyosung TNS Inc.	Joe Militello
Hyosung TNS Inc.	JaeWhan Shin
IBM Corporation	Richard Kisley
Ingenico	Steven Bowles
Ingenico	Wayne Burgess
ISARA Corporation	Philip Lafrance
ITS, Inc. (SHAZAM Networks)	Manish Nathwani
J.P. Morgan Chase	Kathleen Krupa
J.P. Morgan Chase	Darryl Scott
K3DES LLC	Mukul Gupta
MagTek, Inc.	Jeff Duncan
MagTek, Inc.	Mimi Hart
MasterCard Europe Sprl	Mark Kamers

© ASC X9, Inc. 2022 – All rights reserved

MasterCard Europe Sprl	Michael Ward
Micro Focus LLC - USSM	John Ivie
Micro Focus LLC - USSM	Luther Martin
Micro Focus LLC - USSM	Timothy Roake
Micro Focus LLC - USSM	Phil Smith III
Microsoft	Paul Adare
Microsoft	Karina Sirota
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	Nick Gajcowski
National Security Agency	Paul Timmel
NCR Corporation	Charlie Harrow
NCR Corporation	Bradford Loewy
P97 Networks, Inc.	Steve Moses
PCI Security Standards Council	Leon Fell
PCI Security Standards Council	Ralph Poore
PCI Security Standards Council	Joel Weisz
PNC Bank	Omar Jarrar
SteinTech LLC	Clay Epstein
TECSEC Incorporated	Ed Scheidt
TECSEC Incorporated	Jay Wack
Thales DIS CPL USA Inc	Amit Sinha
Thales DIS CPL USA Inc	Devesh Tewari
Thales DIS CPL USA Inc	James Torjussen
The Clearing House	Mark Fitlin
The Clearing House	Sharon Jablon
The Clearing House	Hirak Patel
U.S. Bank	Stephen Case
University Bank	Stephen Ranzini
University Bank	Michael Talley
Utimaco Inc.	Susan Langford
Valley Bank	Mike Livni
VeriFone, Inc.	John Barrowman
VeriFone, Inc.	Christophe Devaux
VeriFone, Inc.	Indra Fitzgerald
VeriFone, Inc.	Joachim Vance

© ASC X9, Inc. 2022 – All rights reserved

Viewpointe ..... Richard Luchak
VISA ..... Adam Clark
VISA ..... Eric Le Saint
VISA ..... Kim Wagner
Wells Fargo Bank ..... Sotos Barkas
Wells Fargo Bank ..... Jason Buck
Wells Fargo Bank ..... Goriola Dawodu
Wells Fargo Bank ..... Garrett Ellis
Wells Fargo Bank ..... Rameshchandra Ketharaju
Wells Fargo Bank ..... Antoinette McCarthy
Wells Fargo Bank ..... Kelly O'Donnell
Wells Fargo Bank ..... James Satterlee
Wells Fargo Bank ..... Jeff Stapleton
Wells Fargo Bank ..... Srinivas Voora
Whitebox Advisors ..... Heinrich Smit

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:

Stephen Case, Chairman
Andrea Beatty, Vice Chairman
Richard Kisley, Project Editor

Organization Represented ***Representative***

ACI Worldwide ..... Julie Samson
Amazon ..... Sean Estrada
Amazon ..... Sandra Lambert
American Express Company ..... Gail Chapman
American Express Company ..... Alan Fong
American Express Company ..... Michael Hyzer
American Express Company ..... Peter Markall

© ASC X9, Inc. 2022 – All rights reserved

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	Terrelle Carswell
Bank of America	Andi Coleman
Bank of America	Sean Fitzpatrick
Bank of America	Chuck Gruesbeck
Bank of America	Terry McKinney
Bank of America	Chris Schrick
Bank of America	Michael Shanzer
Bank of America	Matt Sharp
Bank of America	Michael Smith
Bank of America	Daniel Welch
Bank of America	Terri Willis
BetterBuyDesign	Steve Mott
Bloomberg LP	Erik Anderson
Capital One	Johnny Lee
Citigroup, Inc.	Sudha Iyer
comforte AG	Henning Horst
comforte AG	Michael Horst
Conexxus, Inc.	David Ezell
Conexxus, Inc.	Alan Thiemann
Conexxus, Inc.	Linda Toth
CUSIP Global Services	Scott Preiss
Delap LLP	Andrea Beatty
Delap LLP	Diane Bishop
Delap LLP	David Buchanan
Delap LLP	Spencer Giles
Diebold Nixdorf	Christoph Bruecher
Diebold Nixdorf	Rick Brunt
Diebold Nixdorf	Bruce Chapa
Diebold Nixdorf	B Scott Harroff
Diebold Nixdorf	Anne Konecny
Diebold Nixdorf	Alexander Lindemeier
Diebold Nixdorf	Michael Nolte

© ASC X9, Inc. 2022 – All rights reserved

Diebold Nixdorf ..... Matthias Runowski
Digicert ..... Corey Bonnell
Digicert ..... Tim Hollebeek
Discover Financial Services ..... Debbie Holfeld
Discover Financial Services ..... Susan Pandy
Discover Financial Services ..... Julie Quandt
Discover Financial Services ..... Lakshmi Ramanathan
Discover Financial Services ..... Jordan Schaefer
Discover Financial Services ..... Jorge Vargas
Dover Fueling Solutions ..... Rohith Chinnaswamy
Dover Fueling Solutions ..... Simon Siew
Dover Fueling Solutions ..... Harish Veeravalli
Federal Reserve Bank ..... Guy Berg
Federal Reserve Bank ..... Ainsley Hargest
Federal Reserve Bank ..... Bob Hunt
Federal Reserve Bank ..... Paul Nunnally
Federal Reserve Bank ..... Patti Ritter
First National Bank of Omaha ..... Robert Lamagna-Reiter
First National Bank of Omaha ..... Sherry Rewolinski
First National Bank of Omaha ..... Kristi White
FIS ..... Chris Doyle
FIS ..... Tami Harris
FIS ..... Ian Lumsden
Fiserv ..... Bud Beattie
Fiserv ..... Scott Carpenter
Fiserv ..... Lisa Curry
Fiserv ..... Jacqueline Dill
Fiserv ..... Riquet Dominico
Fiserv ..... Angela Ghetu
Fiserv ..... Vinayak Kagalkar
Fiserv ..... Brian Kean
Fiserv ..... Michelle Matthews
Fiserv ..... Andres Mendoza
Fiserv ..... Dan Otten
Fiserv ..... Anthony Ringer
Fiserv ..... Bambi Tsui
Fiserv ..... Allisa Walker

© ASC X9, Inc. 2022 – All rights reserved

Futurex.....Comron Moeni
Futurex.....Ryan Smith
Futurex.....Tim Weston
GEOBRIDGE Corporation.....Dean Macinskas
GEOBRIDGE Corporation.....Jason Way
Georgetown University.....Shin'ichiro Matsuo
Gilbarco.....Scott Spiker
Gilbarco.....Scott Turner
Gilbarco.....Bruce Welch
Hyosung TNS Inc.....Joe Militello
Hyosung TNS Inc.....JaeWhan Shin
Hyosung TNS Inc.....Nancy Walker
IBM Corporation.....Wai Choi
IBM Corporation.....Richard Kisley
ID TECH.....Lewis Lin
Ingenico.....Steven Bowles
Ingenico.....Wayne Burgess
Ingenico.....Vanessa Terrade
ISARA Corporation.....Philip Lafrance
ITS, Inc. (SHAZAM Networks).....Janet LaFrence
ITS, Inc. (SHAZAM Networks).....Manish Nathwani
J.P. Morgan Chase.....Kathleen Krupa
J.P. Morgan Chase.....Darryl Scott
K3DES LLC.....James Richardson
MagTek, Inc.....Jeff Duncan
MagTek, Inc.....Mimi Hart
MasterCard Europe Sprl.....Robert Gallagher
MasterCard Europe Sprl.....Mark Kamers
MasterCard Europe Sprl.....Michael Ward
Member Emeritus.....Todd Arnold
Member Emeritus.....Dave Faoro
Member Emeritus.....Larry Hines
Member Emeritus.....Darlene Kargel
Member Emeritus.....Lawrence LaBella
Member Emeritus.....Richard Sweeney
National Institute of Standards and Technology (NIST).....Elaine Barker
National Institute of Standards and Technology (NIST).....Lily Chen

© ASC X9, Inc. 2022 – All rights reserved

National Institute of Standards and Technology (NIST) ..... Morris Dworkin
National Security Agency..... Paul Timmel
NCR Corporation ..... Charlie Harrow
NCR Corporation ..... Bradford Loewy
NCR Corporation ..... Brian Wotherspoon
PAX Technology, Inc. ..... LeAnn Hostetler
PCI Security Standards Council ..... Leon Fell
PCI Security Standards Council ..... Doug Manchester
PCI Security Standards Council ..... Ralph Poore
PCI Security Standards Council ..... Randall Rieth
PNC Bank ..... Omar Jarrar
PNC Bank ..... Melinda Tobolewski
Publix Super Markets, Inc. ..... Jonathan Carter
Publix Super Markets, Inc. ..... Mark Clements
Publix Super Markets, Inc. ..... Joshua Peak
TECSEC Incorporated ..... Ed Scheidt
TECSEC Incorporated ..... Jay Wack
Thales DIS CPL USA Inc ..... Amit Sinha
Thales DIS CPL USA Inc ..... Devesh Tewari
Thales DIS CPL USA Inc ..... James Torjussen
The Clearing House ..... Sharon Jablon
The Clearing House ..... Jackie Pagán
U.S. Bank ..... Stephen Case
U.S. Bank ..... Dave Esmond
U.S. Bank ..... Victoria Evans
U.S. Bank ..... Stephanie Lane
University Bank ..... Stephen Ranzini
University Bank ..... Michael Talley
Utimaco Inc. ..... Jillian Benedick
Utimaco Inc. ..... Susan Langford
Utimaco Inc. ..... Manish Upasani
VeriFone, Inc. ..... John Barrowman
VeriFone, Inc. ..... Christophe Devaux
VeriFone, Inc. ..... Indra Fitzgerald
VeriFone, Inc. ..... Joachim Vance
VISA ..... Adam Clark
VISA ..... Kim Wagner

© ASC X9, Inc. 2022 – All rights reserved

Wells Fargo Bank .....Troy Anderson
Wells Fargo Bank .....Sotos Barkas
Wells Fargo Bank .....Goriola Dawodu
Wells Fargo Bank .....Ankur Desai
Wells Fargo Bank .....Garrett Ellis
Wells Fargo Bank .....Matthew Greenwell
Wells Fargo Bank .....Ryan Hegland
Wells Fargo Bank .....Jeff Jacoby
Wells Fargo Bank .....Rameshchandra Ketharaju
Wells Fargo Bank .....Jan Kohl
Wells Fargo Bank .....Eric Lengvenis
Wells Fargo Bank .....Brian Parks
Wells Fargo Bank .....Tim Plantand
Wells Fargo Bank .....Abhijit Rao
Wells Fargo Bank .....James Satterlee
Wells Fargo Bank .....Jeff Stapleton
Wells Fargo Bank .....Tony Stieber
Wells Fargo Bank .....Richard Toohey
Wells Fargo Bank .....Srinivas Voora
Wells Fargo Bank .....David Walgamotte
Whitebox Advisors .....Heinrich Smit

© ASC X9, Inc. 2022 – All rights reserved

Retail Financial Services - Interoperable Secure Key Block Specification

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 between SCDs that share a symmetric key to wrap keys and other relevant data. This could be host to host or host to transaction-originating SCD. This method may also be used for the storage of keys under a symmetric key. Interoperability may be less of a factor when storing keys for use with a given implementation. The symmetric key used for storage need not be shared when using this method for key storage.

This document establishes the security requirements for an interoperable Key Block, which is a structure containing the encrypted key and its attributes wrapped together.

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. ANSI X9.24, Retail Financial Services Symmetric Key Management: All Parts
2. ANSI X3.92, Data Encryption Algorithm (DEA)
3. NIST SP 800-67 Rev. 2, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher
4. ISO/IEC 9797.1:1999, Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 1: Mechanisms using a block cipher
5. ISO/IEC 9797.1:2011, Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 1: Mechanisms using a block cipher
6. ANSI X9.102-2008 (R2017), Symmetric Key Cryptography For the Financial Services Industry – Wrapping of Keys and Associated Data
7. ISO 16609:2016, Banking – Requirements for message authentication using symmetric techniques
8. NIST SP 800-38B, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication
9. NIST SP 800-108, Recommendation for Key Derivation Using Pseudorandom Functions
10. FIPS 197, Advanced Encryption Standard (AES), November 2001
11. FIPS 198-1, The Keyed-Hash Message Authentication Code (HMAC), July 2008
12. ISO 13491:2016, Financial Services – Secure Cryptographic Devices (Retail), All parts
13. IETF RFC 5915, Elliptic Curve Private Key Structure, June 2010
14. IETF RFC 4648, The Base16, Base32, and Base64 Data Encodings, October 2006

© ASC X9, Inc. 2022 – All rights reserved