This is a preview of "ANSI X9.69-2006". Click here to purchase the full version from the ANSI store.

American National Standard for Financial Services

ANSI X9.69–2006

Framework for Key Management Extensions

Accredited Standards Committee X9, Incorporated
Financial Industry Standards

Date Approved:

American National Standards Institute

© ASC X9, Inc. 2006 – All rights reserved

This is a preview of "ANSI X9.69-2006". Click here to purchase the full version from the ANSI store.

Contents

Page

© ASC X9, Inc. 2006 – All rights reserved

This is a preview of "ANSI X9.69-2006". Click here to purchase the full version from the ANSI store.

Figures

© ASC X9, Inc. 2006 – All rights reserved

This is a preview of "ANSI X9.69-2006". Click here to purchase the full version from the ANSI store.

Forword

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CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time.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
P.O. Box 4035
Annapolis, MD 21403 USA
X9 Online http://www.x9.org

Copyright © 2006 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. 2006 – All rights reserved

This is a preview of "ANSI X9.69-2006". Click here to purchase the full version from the ANSI store.

Introduction

This Standard is concerned with symmetric key systems in which the encrypting key and decrypting key are identical. The security and reliability of any process based on a symmetric cryptographic algorithm is directly dependent on the protection afforded to the secret quantity, called the key. Thus, no matter how strong the algorithm, the system is only as secure as its key management method.

This Standard defines two specific key management methods for controlling and handling keys, called (1) Constructive Key Management and (2) Key Usage Control. Each method can be used independently; or the methods can be used in combination. However, the combined use of the methods is highly recommended by the ASC X9 Subcommittee responsible for this Standard. Each method is described in a separate section of the Standard.

The section on CONSTRUCTIVE KEY MANAGEMENT, systematizes key creation, implementing “dual control” or “split knowledge” by using key components to construct the final working key. This working key may be used in several ways including as a session key, for a store-and-forward (i.e. e-mail) application, and for file encryption applications, such as archiving, or protecting filed information until needed again by the user. Other applications are also possible. Until now, this practice of split knowledge key creation has been used mainly to transport key parts into systems where “master keys” were used to protect keys in storage, and to recover the working keys for a current application. With the methodology of this Standard, a working key will be created as needed for a specific encryption process, and re-created when needed to decrypt the object. Depending on the application, the key may be saved or destroyed after each use. The working key is never transmitted; the application program only knows it while it is in use.

The section on KEY USAGE CONTROL, allows the creator of a key to specify the allowed uses of the key. For example, key usage control information can be used to distinguish key types (data, PIN, or key-encrypting). The type “data key” can be further sub-divided to distinguish data privacy keys—keys used to encrypt and decrypt data—from Message Authentication Code (MAC) keys---keys used to protect the integrity of data. The method attaches or binds a “key usage vector” to each generated key, for the life of the key, and is used by the system to ensure that keys are used properly. In short, the key usage vector prevents abuses and attacks against the key. The key usage vector can be used to protect keys stored within a single system, or to protect keys transmitted from one system to another.

This Standard is algorithm independent, and as new cryptographic algorithms with perhaps longer key lengths than currently in use are developed and adopted by the Financial Community this Standard will still apply.

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.

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, P.O. Box 4035, Annapolis, MD 21403 USA.

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. 2006 – All rights reserved

This is a preview of "ANSI X9.69-2006". Click here to purchase the full version from the ANSI store.

The X9 committee had the following members:
Jim Schaffer, X9 Chairman
Vincent DeSantis, X9 Vice-Chairman
Cynthia Fuller, Executive Director
Susan Yashinskie, Managing Director

Organization Represented	Representative	
American Bankers Association	C. Diane	Poole
American Express Company	John	Allen
American Financial Services Association	Mark	Zalewski
Bank of America	Daniel	Welch
Certicom Corporation	Daniel	Brown
Citigroup, Inc.	Gary	Word
Clarke American Checks, Inc.	John	McCleary
CUSIP Service Bureau	James	Taylor
Deluxe Corporation	John	FitzPatrick
Diebold, Inc.	Bruce	Chapa
Discover Financial Services	Katie	Howser
Federal Reserve Bank	Dexter	Holt
First Data Corporation	Rick	Van Luvender
Fiserv	Skip	Smith
FSTC, Financial Services Technology Consortium	Daniel	Schutzer
Hewlett Packard	Larry	Hines
Hypercom	Scott	Spiker
IBM Corporation	Todd	Arnold
Ingenico	John	Spence
Intuit, Inc.	Jana	Hocker
J.P. Morgan Chase & Co	Jacqueline	Pagan
KPMG LLP	Mark	Lundin
MagTek, Inc.	Carlos	Morales
MasterCard International	William	Poletti
National Association of Convenience Stores	Michael	Davis
National Security Agency	Sheila	Brand
NCR Corporation	Steve	Stevens
Proofspace	Paul	Doyle
SWIFT/Pan Americas	James	Wills
U.S. Bank	Marc	Morrison
University Bank	Stephen	Ranzini
VECTORsgi	Ron	Schultz
VeriFone, Inc.	Brad	McGuinness
VISA	Richard	Sweeney
Wachovia Bank	Raymond	Gatland
Wells Fargo Bank	Ruven	Schwartz

© ASC X9, Inc. 2006 – All rights reserved

This is a preview of "ANSI X9.69-2006". Click here to purchase the full version from the ANSI store.

The X9F subcommittee on Information Security had the following members:

Dick Sweeney, X9F Chairman
Sandra Lambert, X9F Vice Chair

Organization Represented	Representative	
3PEA Technologies, Inc.	Mark	Newcomer
ACI Worldwide	Douglas	Grote
ACI Worldwide	Julie	Samson
ACI Worldwide	Jim	Shaffer
ACI Worldwide	Sid	Sidner
American Bankers Association	Tom	Judd
American Express Company	John	Allen
American Express Company	Richard	Rodriguez
American Express Company	Vicky	Sammons
American Financial Services Association	Mark	Zalewski
Bank of America	Daniel	Welch
Certicom Corporation	Daniel	Brown
Citigroup, Inc.	Paul	Gubiotti
Citigroup, Inc.	Susan	Rhodes
Citigroup, Inc.	Gary	Word
Clarke American Checks, Inc.	John	McCleary
Clarke American Checks, Inc.	John	Petrie
ClearWave Electronics	Mark	Ross
CUSIP Service Bureau	Scott	Preiss
CUSIP Service Bureau	James	Taylor
DeLap, White, Caldwell and Croy, LLP	Darlene	Kargel
Deluxe Corporation	John	FitzPatrick
Deluxe Corporation	Mike	Valiquet
Depository Trust and Clearing Corporation	Robert	Palatnick
Diebold, Inc.	Bruce	Chapa
Diebold, Inc.	Laura	Drozda
Discover Financial Services	Julie	Shaw
ECCHO	Phyllis	Meyerson
Federal Reserve Bank	Jeannine M.	DeLano
Federal Reserve Bank	Neil	Hersch
Federal Reserve Bank	Dexter	Holt
First Data Corporation	Tina	McGowan
First Data Corporation	Rick	Van Luvender
Fiserv	Bud	Beattie
Fiserv	Mary	Bland
Fiserv	Kevin	Finn
Fiserv	Dennis	Freiburg
FSTC, Financial Services Technology Consortium	Frank	Jaffe
FSTC, Financial Services Technology Consortium	Daniel	Schutzer
Futurex	Jason	Anderson
Futurex	Greg	Schmid
Hewlett Packard	Larry	Hines
Hewlett Packard	Susan	Langford
Hypercom	Scott	Spiker

© ASC X9, Inc. 2006 – All rights reserved

This is a preview of "ANSI X9.69-2006". Click here to purchase the full version from the ANSI store.

IBM Corporation	Todd	Arnold
InfoGard Laboratories	Tom	Caddy
Ingenico	John	Spence
Innove	Steven	Teppler
J.P. Morgan Chase & Co	Edward	Koslow
John H. Harland Company	Curt	Siroky
MagTek, Inc.	Terry	Benson
MagTek, Inc.	Jeff	Duncan
MagTek, Inc.	Carlos	Morales
MasterCard International	Jeanne	Moore
MasterCard International	Michael	Ward
National Institute of Standards and Technology	Elaine	Barker
National Institute of Standards and Technology	William	Burr
National Institute of Standards and Technology	David	Cooper
National Institute of Standards and Technology	Randall	Easter
National Institute of Standards and Technology	Sharon	Keller
National Institute of Standards and Technology	John	Kelsey
National Institute of Standards and Technology	Fernando	Podio
National Security Agency	Mike	Boyle
National Security Agency	Sheila	Brand
National Security Agency	Greg	Gilbert
National Security Agency	Tim	Havighurst
National Security Agency	Debby	Wallner
NCR Corporation	Ali	Lowden
NCR Corporation	David	Norris
NCR Corporation	Ron	Rogers
NCR Corporation	Ally	Whytock
NCR Corporation	Hui	Wu
NTRU Cryptosystems, Inc.	Nick	Howgrave-Graham
NTRU Cryptosystems, Inc.	William	Whyte
Pitney Bowes, Inc.	Leon	Pintsov
Proofspace	Paul	Doyle
Rosetta Technologies	Jim	Maher
Rosetta Technologies	Paul	Malinowski
RSA Security, Inc.	James	Randall
RSA Security, Inc.	Steve	Schmalz
Surety, Inc.	Dimitrios	Andivahis
TECSEC Incorporated	Ed	Scheidt
Thales e-Security, Inc.	Tim	Fox
Thales e-Security, Inc.	James	Torjussen
The Clearing House	Vincent	DeSantis
The Clearing House	Henry	Farrar
The Clearing House	Susan	Long
Triton Systems of Delaware, Inc.	Daryll	Cordeiro
U.S. Bank	Marc	Morrison
Unisys Corporation	David J.	Concannon
Unisys Corporation	Navnit	Shah
University Bank	Stephen	Ranzini
VECTORsgi	Ron	Schultz

© ASC X9, Inc. 2006 – All rights reserved

This is a preview of "ANSI X9.69-2006". Click here to purchase the full version from the ANSI store.

VeriFone, Inc.	John	Barrowman
VeriFone, Inc.	David	Ezell
VeriFone, Inc.	Dave	Faoro
VeriFone, Inc.	Brenda	Watlington
VISA	Chackan	Lai
VISA	Stoddard	Lambertson
Voltage Security, Inc.	Luther	Martin
Wachovia Bank	Raymond	Gatland
Wachovia Bank	David	Naelon
Wachovia Bank	Keith	Ross
Wells Fargo Bank	Mick	Bauer
Wells Fargo Bank	Jeff	Jacoby
Wells Fargo Bank	Eric	Lengvenis
Wells Fargo Bank	Farah	Moaven
Wells Fargo Bank	Chuck	Perry
Wells Fargo Bank	Ruven	Schwartz
Wells Fargo Bank	Craig	Shorter
Wells Fargo Bank	Tony	Stieber

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 X9F4 Cryptographic Protocol and Application Security working group which developed this standard had the following members:

Jeff Stapleton, X9F4 Chairman and Project Editor
Sandra Lambert, X9F4 Vice Chair

Organization Represented	**Representative**	
Bank of America	Andi	Coleman
Certicom Corporation	Scott	Vanstone
Clarke American Checks, Inc.	John	McCleary
Clarke American Checks, Inc.	John	Petrie
Clarke American Checks, Inc.	Steve	Smith
Comet Capital, LLC	Lawrence T.	Levine
Comet Capital, LLC	Miranda	Watson
DeLap, White, Caldwell and Croy, LLP	Steve	Case
DeLap, White, Caldwell and Croy, LLP	Darlene	Kargel
Diebold, Inc.	Bruce	Chapa
Diebold, Inc.	Anne	Doland
Diebold, Inc.	Scott	Harroff
Discover Financial Services	Julie	Shaw
Entrust, Inc.	Miles	Smid
Ernst and Young	Keith	Sollers
Federal Reserve Bank	Neil	Hersch

© ASC X9, Inc. 2006 – All rights reserved

This is a preview of "ANSI X9.69-2006". Click here to purchase the full version from the ANSI store.

Federal Reserve Bank	Deb	Hjortland
Federal Reserve Bank	Dexter	Holt
First Data Corporation	Lilik	Kazaryan
First Data Corporation	Todd	Nuzum
Fiserv	Dennis	Freiburg
Fiserv	Dan	Otten
FSTC, Financial Services Technology Consortium	Frank	Jaffe
FSTC, Financial Services Technology Consortium	Christine	Nautiyal
Futurex	Jason	Anderson
Futurex	Greg	Schmid
Griffin Consulting	Harriette	Griffin
Griffin Consulting	Phil	Griffin
Hewlett Packard	Larry	Hines
Hypercom	Scott	Spiker
Hypercom	Gary	Zempich
IBM Corporation	Todd	Arnold
IBM Corporation	Phil	Griffin
IBM Corporation	Michael	Kelly
InfoGard Laboratories	John	Attala
InfoGard Laboratories	Tom	Caddy
InfoGard Laboratories	Ken	Kolstad
Ingenico	Alexandre	Hellequin
Ingenico	John	Spence
Innove	Jarid	Cottrel
Innove	Brad	Morrison
Innove	Cindy	Morrison
Innove	Ralph	Poore
Innove	Steven	Teppler
KPMG LLP	Steven	Berhorst
KPMG LLP	Mark	Lundin
MagTek, Inc.	Terry	Benson
MasterCard International	William	Poletti
National Institute of Standards and Technology	Elaine	Barker
National Institute of Standards and Technology	Lily	Chen
National Security Agency	Sheila	Brand
National Security Agency	Greg	Gilbert
National Security Agency	Tim	Havighurst
National Security Agency	Paul	Timmel
nCipher Corporation Ltd.	Ron	Carter
NCR Corporation	Wayne	Doran
NCR Corporation	Charlie	Harrow
NCR Corporation	Steve	Stevens
NTRU Cryptosystems, Inc.	Ari	Singer
NTRU Cryptosystems, Inc.	William	Whyte
Proofspace	Paul	Doyle
Proofspace	Yuxin	Ruan
Proofspace	Bob	West
RSA Security, Inc.	Burt	Kaliski
RSA Security, Inc.	James	Randall
Sun Microsystems PS	Joel	Weise

© ASC X9, Inc. 2006 – All rights reserved

This is a preview of "ANSI X9.69-2006". Click here to purchase the full version from the ANSI store.

Surety, Inc.	Dimitrios	Andivahis
TECSEC Incorporated	Ed	Scheidt
TECSEC Incorporated	Dr. Wai	Tsang
Thales e-Security, Inc.	Tim	Fox
Thales e-Security, Inc.	James	Torjussen
Triton Systems of Delaware, Inc.	Daryll	Cordeiro
Triton Systems of Delaware, Inc.	Bob	Douglas
U.S. Bank	Peter	Skirvin
U.S. Bank	Rush	Wilson
Unisys Corporation	David J.	Concannon
University Bank	Stephen	Ranzini
University Bank	Michael	Talley
VECTORsgi	Jerry	Bowman
VECTORsgi	Ron	Schultz
VeriFone, Inc.	Dave	Faoro
VeriFone, Inc.	Doug	Manchester
VISA	Chackan	Lai
VISA	Richard	Sweeney
Voltage Security, Inc.	Luther	Martin
Wachovia Bank	David	Naelon
Wells Fargo Bank	Mick	Bauer
Wells Fargo Bank	Jeff	Jacoby
Wells Fargo Bank	Eric	Lengvenis
Wells Fargo Bank	Mike	McCormick
Wells Fargo Bank	Farah	Moaven
Wells Fargo Bank	Doug	Pelton
Wells Fargo Bank	Mike	Rudolph
Wells Fargo Bank	Ruven	Schwartz

This document cancels and replaces X9.69-1999 Framework for Key Management Extensions in whole. X9.69-2006 was revised to address the industry transition from single DES to Triple DES, with the following changes:

A. Reference to the following documents were added:
   - X9.52 Triple Data Encryption Algorithms (3DEA) Modes of Operation
   - FIPS 197 Advanced Encryption Standard (AES)
   - IEEE Cryptography Transitions

B. References to the following withdrawn X9 standards were deleted:
   - X9.9 Financial Institution Message Authentication Codes (MAC) Wholesale; refer to Technical Guideline: Technical Guideline: Managing Risk and Migration Planning: Withdrawal of ANSI X9.9 (X9 TG-24-1999)
   - X9.17 Financial Institution Key Management (Wholesale); refer to Technical Guideline: Managing Risk and Migration Planning: Withdrawal of ANSI X9.17 (X9 TG-26 – 1999)

C. The follow terms were changed:
   - Policy Manager was changed to CKM Administration
   - Labels was changed to Credentials

© ASC X9, Inc. 2006 – All rights reserved

This is a preview of "ANSI X9.69-2006". Click here to purchase the full version from the ANSI store.

- Credential Manager was changed to Token Distribution

D. The document was converted to the current X9/ISO standards template.

At the time the original X9.69-1999 was approved, the X9 committee had the following members:

Harold Deal, X9 Chairman
William E. Lyons, X9 Vice Chairman
Cynthia Fuller, Managing Director

Organization Represented	Representative
American Bankers Association	Anne Livingston
	Kawika Daguio
American Express Company	Bonnie Howard
Applied Communications	Douglas Grote
	Cindy Rink
Automated Financial Services	Tom Clute
Banc One Services Corporation	William Lyons
Bank of America	Gretchen Breiling
Bankers Roundtable	Kit Needlam
	Keviar Warner
Canadian Bankers Association	Christine ArjoonLaL
	Mark Bakic
Chase Manhattan Bank	Christopher Dowdell
	Francis Keenan
Citibank	Seymour Rosen
Cybersafe Corp	Glenda Barnes
Deluxe Corporation	Maury Jansen
Ernst & Young, LLP	Geoffery Turner
	Richard Kastner
	Ralph Poore
Federal Reserve Bank	Dexter Holt
	Susan Belisle
Ferris & Associates, Inc.	Martin Ferris
First Data Corporation	Gene Kathol
Greenlee & Associates	Blake Greenlee
IBM Corporation	Harry Hankla
	Donald Harman
Intel Corporation	Pamela Warren
	Steve Ellis
KPMG Peat Marwick LLP	Jon Graff
	Jeff Stapleton
MARS Electronic International	E. E. Barnes
	Ron Bernardini
MasterCard International	Melinda Yee
Mellon Bank, N.A.	David Taddeo
	Genien Carlson
Merrill Lynch	John Dolan
Moore Business Forms Inc.	Thomas Oswald
National Association of Convenience Stores	Robert Swanson
National Security Agency	Gerard Rainville
NationsBanc	Harold Deal
NCR	Suzette Albert
New York Clearing House	Vincent DeSantis
NOVUS Services, Inc.	Thomas Kossler

© ASC X9, Inc. 2006 – All rights reserved

This is a preview of "ANSI X9.69-2006". Click here to purchase the full version from the ANSI store.

	Peggy Douds
	David Pratscher
Pitney Bowes, Inc.	Leon Pintsov
Price Waterhouse Coopers	Jeff Zimmerman
Russell Technology Associates	James Russell
SPYRUS	Peter Yee
	Karen Randall
Unisys Corporation	Thomas Hayosh
	James Graziano
VeriFone, Inc.	John Sheets
	Glenn Kramer
	Stuart Taylor
Visa International	Bill Chen
Wells Fargo Bank	Tim Silva
Xcert International	Marc Branchaud
	Sandra Lambert

At the time the original X9.69-1999 was approved, the X9F subcommittee on Information Security had the following members:

Glenda Barnes, X9F Chairman

Organization Represented	**Representative**
American Bankers Association	Kawika Daguio
American Express Company	Bonnie Howard
	Glenn Weiner
Applied Communications Inc.	Cindy Rink
	Douglas Grote
	Dennis Abraham
Bank of America	Kathleen Gibbons
	Mack Hicks
	Richard Phillips
	Martin Johnson
Bank One Corp	Duane Baldwin
Bankers Roundtable	Keviar Warner
	Frederick Honold
CertCo LLC	Richard Ankney
	Daniel Geer
Certicom Corporation	Don B. Johnson
Chase Manhattan Bank	Gene Rao
	Richard Yen
Communications Security Establishment	Michael Chawrun
	Alan Poplove
Cybersafe Corp.	Glenda Barnes
	David O'Brien
Cylink Corporation	Kamy Kavianian
	Lily Lidong Chen
Deluxe Corporation	Cory Surges
	Maury Jansen
	Chuck Bram
Digital Equipment corporation	Donald Holden
Entrust Technologies	Robert Zuccherato
	Tim Moses
Ernst & Young, LLP	Richard Kastner
	Ralph Spencer Poore

© ASC X9, Inc. 2006 – All rights reserved

This is a preview of "ANSI X9.69-2006". Click here to purchase the full version from the ANSI store.

Federal Reserve Bank	Richard Sweeney
	Michael Versace
	Gary Chaulklin
First Data Corporation	Gene Kathol
First Union Corporation	James Ramsay
	Sandra Lambert
Food Marketing Institute	Ted Mason
	Joy Nicholas
Fortress Technologies	Eva Bozoki
Gilbarco Inc.	Rena Smith
Griffin Consulting	Phillip Griffin
GTE Internetworking	Patrick Cain
Harmonic Systems Incorporated	Daniel Hunt
IBM Corporation	Mohammad Peyravian
	Harry Hankla
	Stephen Mike Matyas
Intel Corporation	Pamela Warren
	Steve Ellis
IIT Research Institute	Roger Westman
KPMG Peat Marwick LLP	Jeffrey Stapleton
M. Blake Greenlee Associates, Ltd.	Blake Greenlee
MasterCard International	R.O. Karlin
	William Poletti
Mellon Bank, N.A.	David Taddeo
Merrill Lynch	Lawrence LaBella
	John Dolan
	Ted Gerbracht
National Association of Convenience Stores	Robert Swanson
National Security Agency	Gerard Rainville
NCR	Mark Liddle
NIST	Donna Dodson
	Miles Smid
Northstar Technology Group, Inc.	John Bowman
Pitney bowes, Inc.	Andrei Obrea
Price Waterhouse Coopers	John Hunt
	David Oshman
	Jeffrey Zimmerman
Pulse EFT Association	Karen Gardstein
	Leslie Hendrix
Racal Guardata, Inc.	Scott Petersen
	Emile Soueid
	Samuel Epstein
SAIC	Wanda Gamble-Braggs
Security Dynamics	Burt Kaliski
SPYRUS	Karen Randall
	Peter Yee
Technical Communications Corporation	John Gill
TECSEC Incorporated	Edward Scheidt
	Pud Reaver
	Jay Wack
VeriFone, Inc.	John Sheets
	Stuart Taylor
	Trong Nguyen
VISA International	Willaim Chen
Wells Fargo Bank	Azita Amini
	Terry Leahy

© ASC X9, Inc. 2006 – All rights reserved

This is a preview of "ANSI X9.69-2006". Click here to purchase the full version from the ANSI store.

Xcert International, Inc.	Marcus Branchaud Sandra Lambert

At the time the original X9.69-1999 was approved, the X9F3 working group that developed this Standard had the following members:

Gary Chaulklin, Chair X9F3

Organization Represented	Representative
Abraham & Associates	Dennis G. Abraham
AT&T	Bill Oeschger
Certco LLC	Richard Ankney
Certicom	Don B. Johnson
Chase Manhattan Bank	Richard Yen
Citigroup	Perry Gleason
Communications Devices Inc	Tadgh Kelly
Compaq	Don Holden
Coopers & Lybrand	Victor Blanchard
CyberSafe	Glenda Barnes
Cylink Corporation	Kamy Kavianian
Delap, White, Caldwell & Croy, LLP	Darlene Kargel
Diebold	Sandra Morgan
Dresser Industries	Mike Biskobing
Ernst & Young	Ralph Poore
	Rick Kastner
EXXON Company	John Pratt
Federal Reserve Bank	Richard Sweeney
	Gary Chaulklin
First Union Bank	Jim Ramsay
Gilbarco Inc	Rena Smith
	Tim Dickson
GTE Internetworking	Pat Cain
Hitachi Data Systems	Bill Cox
IBM	Stephen M. Matyas
	Mohammad Peyravian
InfoGard Labs	Les Biggs
IRE	Doug Kozlay
IVI Checkmate	John Spence
JL Information Solutions	Jan Lovorn
Jones Futurex	Gerry Scott
KPMG Peat Marwick	Eric Ashdown
MasterCard	Carl Campbell
NIST	Elaine Barker
	Jim Foti
NSA	Gerard Rainville
PNC Bank	Tim Garland
PULSE	Vivian M. Banki
Schlumberger Ind	Richard Carpenter
Spyrus	Karen Randall
	Peter Yee
TECSEC	Ed Scheidt
	Jay Wack
	Clarence Reaver
U. S. Bancorp	Jeanne Fagan
Verifone	John Sheets

© ASC X9, Inc. 2006 – All rights reserved

This is a preview of "ANSI X9.69-2006". Click here to purchase the full version from the ANSI store.

	Ken Gillman
VISA International	Rick Hite
Wells Fargo Bank	Azita Amini

© ASC X9, Inc. 2006 – All rights reserved

This is a preview of "ANSI X9.69-2006". Click here to purchase the full version from the ANSI store.

Framework for Key Management Extensions

1 Scope

This Standard defines methods for the generation and control of keys used in symmetric cryptographic algorithms. The Standard defines a *constructive method* for the creation of symmetric keys, by combining two or more secret key components. The Standard also defines a method for attaching a *key usage vector* to each generated key that prevents abuses and attacks against the key. The two defined methods can be used separately or in combination.

The Standard does not cover aspects of key management, such as:

- Key establishment mechanisms;

  See for example ANSI X9.24 Financial Institution Key Management (Retail), or ISO/IEC 11770-2, Key Management, Part 2: Mechanisms using symmetric techniques.

- Mechanisms to store, archive, delete, destroy, etc. keys;

- Mechanisms for key recovery in the event of the failure or loss of keys.

The Standard also does not define the implementation of key management mechanisms; there may be different products that comply with this Standard and yet are not interoperable.

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.

ANS X3.92-1981 Data Encryption Algorithm

ANS X3.106-1983 Data Encryption Algorithm - Modes of Operation

ANS X9.19 Financial Institution Retail Message Authentication

ANS X9.52 Triple Data Encryption Algorithms (3DEA) Modes of Operation

FIPS 197 Advanced Encryption Standard (AES)

3 Terms, symbols and abbreviated terms

For the purposes of this document, the following terms and definitions apply.

© ASC X9, Inc. 2006 – All rights reserved