ANS

X9.69 - 1998

American National Standard
For Financial Services

X9.69 – 1998

Framework for Key Management Extensions

Secretariat
Accredited Standards Committee X9, Inc.

Approved January 28, 1999
American National Standards Institute

American National Standard

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 interpretations 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CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time.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, Inc.
P.O. Box 4035
Annapolis, Maryland 21403 USA
Phone: 410-267-7707 or 301-879-7988
Fax: 301-879-5124
Email: Cindy.Fuller@X9.org
Isabel.Bailey@X9.org
X9 Online: http://www.x9.org

Printed in the United States of America

Table of Contents

Table of Figures

FOREWORD

This foreword is not part of American National Standard X9.69-1998.

Financial institutions are making increased use of symmetric cryptographic algorithms to protect financial messages and other sensitive information. Specific examples of this include message encryption and funds transfer message authentication.

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.

Section 6, 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.

Section 7, 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.

While the techniques specified in this Standard are designed to maintain the security of keys, and to prevent abuses and attacks on keys, the Standard in no way guarantees that a particular implementation of the techniques is secure. It is the responsibility of the financial institution to put an overall process in place with the necessary controls to ensure the process is securely implemented. Furthermore, the controls should include the application of appropriate audit tests in order to verify compliance with this Standard. Suggestions for the improvement or revision of this Standard are welcome. They should be sent to Accredited Standards Committee X9, Inc., P.O. Box 4035, Annapolis, Maryland 21403 USA. This Standard was processed and approved for submittal to ASC X9 by the Accredited Standards Committee on Financial Services, X9. Committee approval of the Standard does not necessarily imply that all committee members voted for its approval.

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 publisher.

At the time that this Standard was approved, the X9 Committee had the following members:

Harold Deal, X9 Chairman
William E. Lyons, X9 Vice Chairman
Cynthia Fuller, Managing Director
Darlene J. Schubert, Program Manager

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
	Mara Bakic
Chase Manhattan Bank	Christopher Dowdell
	Francis Keenan
Citibank	Seymour Rosen

Cybersafe Corporation	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
IBM Corporation	Harry Hankla
	Donald Harman
Intel Corporation	Pamela Warren
	Steve Ellis
KPMG Peat Marwick LLP	Jon Graff
	Jeff Stapleton
M. Blake Greenlee & Associates, Ltd.	Blake Greenlee
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
	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

The X9F subcommittee on Data and Information Security had the following members:
Glenda Barnes, Chairperson X9F

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 Corporation	Glenda Barnes
	David O'Brien
Cylink Corporation	Kamy Kavianian
	Lily Lidong Chen
Deluxe Corporation	Cory Surges
	Maury Jansen
	Chuck Bram
Digital Equipment Corporation/Compaq	Donald Holden
Entrust Technologies	Robert Zuccherato
	Tim Moses
Ernst & Young, LLP	Richard Kastner
	Ralph Spencer Poore
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	Ron 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	William Chen
Wells Fargo Bank	Azita Amini
	Terry Leahy
Xcert International, Inc.	Marcus Branchaud
	Sandra Lambert

Under ASC X9 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.

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
Coopers & Lybrand	Victor Blanchard
CyberSafe Corporation	Glenda Barnes
Cylink Corporation	Kamy Kavianian
Delap, White, Caldwell & Croy, LLP	Darlene Kargel
Diebold, Inc.	Sandra Morgan
Digital Equipment Corporation/Compaq	Don Holden
Dresser Industries	Mike Biskobing
Ernst & Young, LLP	Ralph Poore
	Rick Kastner
EXXON Company	John Pratt
Federal Reserve Bank	Richard Sweeney
	Gary Chaulklin
First Union Corporation	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 International	Carl Campbell
National Security Association	Gerard Rainville
NIST	Elaine Barker
	Jim Foti

PNC Bank	Tim Garland
PULSE EFT Association	Vivian M. Banki
Schlumberger Ind	Richard Carpenter
SPYRUS	Karen Randall
	Peter Yee
TECSEC Incorporated	Ed Scheidt
	Jay Wack
	Clarence Reaver
U. S. Bancorp	Jeanne Fagan
Verifone, Inc.	John Sheets
	Ken Gillman
VISA International	Rick Hite
Wells Fargo Bank	Azita Amini

X9.69 – 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.

1.1 Aspects Not Covered

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

- Key establishment mechanisms, see for example ANSI X9.17 Financial Institution Key Management (Wholesale), 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 Definition(s)

Dual Control - A process of utilizing two or more separate entities (usually persons), operating in concert, to protect sensitive functions or information whereby no single entity is able to access or utilize the materials, e.g. cryptographic key.

Credential - A set of access permissions.

Data Separation - Using encryption as a means of access control.

Fixed Split - Secret key(s) used in all encryption/decryption operations; this split is unique to a particular organization or group.

Header – Contains Labels, Random Split, Identity of author, Identity of Credential Manager, Date/time when encrypted, and other information deemed appropriate by Policy Manager.

Key usage vector - Specifies cryptographic services, modes and key values, in which the associated key may be used.