This is a preview of "ANSI X9.69:1998". Click here to purchase the full version from the ANSI store.

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CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time.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

Copyright © 1998 by Accredited Standards Committee 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.

Printed in the United States of America

Table of Contents

1 SCOPE	
1.1 Aspects Not Covered	1
2 DEFINITION(S)	1
3 REFERENCES(S)	2
4 ABBREVIATION(S)	
4.1 Keywords	3
5 APPLICATION	4
5.1 General	
5.2 THE USE OF CONSTRUCTIVE KEY MANAGEMENT	4
5.3 THE USE OF KEY USAGE CONTROL VECTOR	4
5.4 System Algorithm and System Key	
6 CONSTRUCTIVE KEY MANAGMENT	4
6.1 Overview	
6.2 POLICY MANAGER	
6.2.1 Labels	
6.2.1.1 Fixed Labels	7
6.2.1.2 User Selectable Labels	7
6.2.2 Splits	
6.2.2.1 Fixed Splits	
6.2.2.2 Selectable Splits	
Random Split	
6.3 CREDENTIAL MANAGER.	8
0.3.1 Workstation	۰۰۰۰۰ ð
0.5.2 TOKEN	
6.4 L Kay Component Selection	
6.4.2 Key Component Selection	
6.4.3 Key Combinet	
0.4.5 Key Keconstruction	
7 KEY USAGE CONTROL	
7.1 Overview	
7.2 Key Binding Methods	
7.2.1 Binding Method 1	
7.2.2 Binding Method 2	
7.2.3 Binding Method 3	
7.2.4 Binding Method 4	
7.2.5 Binding Method 5	
7.2.6 Binding Method 6	
ANNEX A: EXAMPLE KEY USAGE VECTOR FORMATS	

Table of Figures

FIGURE 1 - OVERVIEW	5
FIGURE 2 – COMBINER FUNCTION	10
FIGURE 3: KEY USAGE VECTOR FIELDS	12

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 keyencrypting). 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

American Bankers Association

American Express Company Applied Communications

Automated Financial Services Banc One Services Corporation Bank of America Bankers Roundtable

Canadian Bankers Association

Chase Manhattan Bank

Citibank

Representative

Anne Livingston Kawika Daguio Bonnie Howard Douglas Grote Cindy Rink Tom Clute William Lyons Gretchen Breiling Kit Needlam Keviar Warner Christine Arjoonlal Mara Bakic Christopher Dowdell Francis Keenan Seymour Rosen Cybersafe Corporation Deluxe Corporation Ernst & Young, LLP

Federal Reserve Bank

Ferris & Associates, Inc. First Data Corporation IBM Corporation

Intel Corporation

KPMG Peat Marwick LLP

M. Blake Greenlee & Associates, Ltd. MARS Electronic International

MasterCard International Mellon Bank, N.A.

Merrill Lynch Moore Business Forms Inc. National Association of Convenience Stores National Security Agency NationsBanc NCR New York Clearing House NOVUS Services, Inc.

Pitney Bowes, Inc. Price Waterhouse Coopers Russell Technology Associates SPYRUS

Unisys Corporation

VeriFone, Inc.

Visa International Wells Fargo Bank Xcert International **Glenda Barnes** Maury Jansen **Geoffery** Turner **Richard Kastner** Ralph Poore Dexter Holt Susan Belisle Martin Ferris Gene Kathol Harry Hankla Donald Harman Pamela Warren Steve Ellis Jon Graff Jeff Stapleton Blake Greenlee E. E. Barnes Ron Bernardini Melinda Yee David Taddeo Genien Carlson John Dolan Thomas Oswald Robert Swanson Gerard Rainville Harold Deal Suzette Albert Vincent DeSantis Thomas Kossler Peggy Douds **David Pratscher** Leon Pintsov Jeff Zimmerman James Russell Peter Yee Karen Randall Thomas Hayosh James Graziano John Sheets Glenn Kramer Stuart Taylor Bill Chen Tim Silva Marc Branchaud Sandra Lambert

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

American Bankers AssociationKawika DaguioAmerican Express CompanyBonnie HowardApplied Communications Inc.Cindy RinkDouglas GroteDennis AbrahamBank of AmericaKathleen GibbonsBank of AmericaMartin JohnsonBank of CorpDuane BaldwinBankers RoundtableKeviar WarnerFrederick HonoldFrederick HonoldCertCo LLCRichard PhillipsCartCo LLCRichard AnkneyDaniel GeerDon B. JohnsonChase Manhattan BankGene RaoRichard YenRichard AnkneyCommunications Security EstablishmentMichael ChawrunAlan PoploveCybersafe CorporationCybersafe CorporationCony SurgesMaury JansenChuck BramDigital Equipment Corporation/CompaqDonald HoldenDigital Equipment Corporation/CompaqDonald HoldenErnst & Young, LLPRichard KastinerFirst Data CorporationGene KathleiFirst Data CorporationGene KathleiFirst Union CorporationGene KathleiFirst Union CorporationGene KathleiFirst Union CorporationGene KathleiFirst Union CorporationGene KathleiFirst Data CorporationGene KathleiFirst Union CorporationGene KathleiFirst Union CorporationJames RansaySandra LambertFod MasonFood Marketing InstituteTed MasonGilbarco Inc.Rena Smith	Organization Represented	Representative
American Express CompanyBonnie Howard Glem WeinerApplied Communications Inc.Cindy Rink Douglas Grote Dennis AbrahamBank of AmericaKathleen Gibbons Kathleen GibbonsBank of AmericaKathleen Gibbons Martin JohnsonBank One Corp Bankers RoundtableDuane Baldwin Frederick HonoldCertCo LLCRichard Ankney Daniel GeerCertCo LLCRichard Ankney Daniel GeerCertCo LLCRichard Yen Richard YenCommunications Security EstablishmentMichael Chawrun Alan PoploveCybersafe CorporationGlenda Barnes David OBrienCylink CorporationGlenda Barnes David OBrienCylink CorporationCory Surges Maury Jansen Lily Lidong Chen Digital Equipment Corporation/CompaqDigital Equipment Corporation/CompaqDonald Holden Entrust TechnologiesErnst & Young, LLPRichard Sastner Ralph Spencer Poore Federal Reserve BankFirst Data CorporationGene Kastner Ralph Spencer Poore First Data CorporationFirst Data CorporationGene Kathol First Union CorporationFirst Data CorporationGene Kathol First Union CorporationFirst Data CorporationGene Kathol First Data Corporation <t< td=""><td>American Bankers Association</td><td>Kawika Daguio</td></t<>	American Bankers Association	Kawika Daguio
Applied Communications Inc.Glenn Weiner Cindy Rink Douglas Grote Dennis AbrahamBank of AmericaKathleen Gibbons Mack Hicks Richard Phillips Martin JohnsonBank One CorpDuane Baldwin Steinard Phillips Martin JohnsonBank One CorpDuane Baldwin Frederick HonoldBankers RoundtableKeviar Warner Frederick HonoldCertico LLCRichard Ankney Daniel GeerCerticom CorporationDon B. JohnsonChase Manhattan BankGene Rao Richard YenCommunications Security EstablishmentMichael Chawrun Alan PoploveCybersafe CorporationGlenda Barnes David O'BrienCylink CorporationCory Surges Maury Jansen Chuck BramDigital Equipment Corporation/CompaqDonald Holden Tim MosesErnst & Young, LLPRichard Sweeney Michael Versace Gary ChaulklinFrederal Reserve BankRichard Sweeney Michael Versace Gary ChaulklinFirst Union CorporationGene Kathol Tim MosesFirst Union CorporationGene KatholFirst Union CorporationGene Kathol <td>American Express Company</td> <td>Bonnie Howard</td>	American Express Company	Bonnie Howard
Applied Communications Inc.Cindy Rink Douglas Grote Dennis AbrahamBank of AmericaKathleen Gibbons Mack Hicks Richard Phillips Martin JohnsonBank One CorpDuane BaldwinBankers RoundtableKeviar Warner Frederick HonoldCertCo LLCRichard Ankney Daniel GeerCerticom CorporationDon B. JohnsonChase Manhattan BankGene Rao Richard YenCommunications Security EstablishmentMichael Chawrun Alan PoploveCybersafe CorporationGlenda Barnes David OBrienCylink CorporationCorporation Bariel GeerCylink CorporationCorporation CorporationDeluxe CorporationCory Surges Maury Jansen Chuck BramDigital Equipment Corporation/CompaqDonald Holden Entrust TechnologiesErnst & Young, LLPRichard Kastner Ralph Spencer Poore Federal Reserve BankFrederick Tunion CorporationGene Kathol Tim MosesFirst Data CorporationGene Kathol First Union CorporationFrist Data CorporationGene Kathol First Union CorporationFrist Data CorporationGene Kathol First Data CorporationFrist Data CorporationGene Kathol First Union CorporationFrist Data CorporationGene Kathol First Data CorporationFrist Data CorporationGene Kathol First Data CorporationFirst Data CorporationGene Kathol First Data CorporationFirst Data CorporationGene Kathol First Data CorporationFirst Data CorporationGene Kathol First Data CorporationFir		Glenn Weiner
bank of America Douglas Grote Dennis Abraham Kathleen Gibbons Mack Hicks Richard Phillips Martin Johnson Bank One Corp Bankers Roundtable Keviar Warner Frederick Honold CertCo LLC Richard Ankney Daniel Geer Certicom Corporation Communications Security Establishment Michael Chawrun Alan Poplove Cybersafe Corporation Glenda Barnes David O'Brien Cylink Corporation Glenda Barnes David O'Brien Cylink Corporation Kamy Kavianian Lily Lidong Chen Deluxe Corporation Corporation/Compaq Digital Equipment Corporation/Compaq Entrust Technologies Frederal Reserve Bank First Data Corporation First Data Corporation First Data Corporation First Union Corporation First Union Corporation First Union Corporation Fortress Technologies Fortress Technologies Eva Bozoki Gilbarco Inc. Rena Smith	Applied Communications Inc.	Cindy Rink
Bank of AmericaDennis Abraham Kathleen Gibbons Mack Hicks Mack Hicks Martin JohnsonBank One CorpDuane BaldwinBank One CorpDuane BaldwinBank One CorpDuane BaldwinBankers RoundtableKeviar WarnerFrederick HonoldFrederick HonoldCertCo LLCRichard AnkneyDaniel GeerDaniel GeerCerticom CorporationDon B. JohnsonChase Manhattan BankGene RaoRichard YenRichard YenCommunications Security EstablishmentMichael Chawrun Ala PoploveCybersafe CorporationGlenda Barnes David O'BrienCylink CorporationKamy Kavianian Lily Lidong Chen Maury JansenDeluxe CorporationCory Surges Maury JansenDigital Equipment Corporation/CompaqDonal Holden Entrust TechnologiesErnst & Young, LLPRichard Kastner Ralph Spencer PooreFederal Reserve BankGene Kathol First Data CorporationFirst Data CorporationGene Kathol First D	**	Douglas Grote
Bank of America Kathleen Gibbons Mack Hicks Nack Hicks Richard Phillips Martin Johnson Bank One Corp Duane Baldwin Bankers Roundtable Keviar Warner Frederick Honold Frederick Honold CerrCo LLC Richard Ankney Daniel Geer Daniel Geer Certicom Corporation Don B. Johnson Chase Manhattan Bank Gene Rao Richard Yen Alan Poplove Cybersafe Corporation Glenda Barnes David O'Brien David O'Brien Cylink Corporation Cory Surges Palue Equipment Corporation/Compaq Donald Holden Entrust Technologies Robert Zuccherato First Data Corporation Gary Chaulklin First Data Corporation Gare Rating First Data Corporation Gare Rating First Data Corporation <		Dennis Abraham
Mack Hicks Richard Phillips Martin JohnsonBank One Corp Bankers RoundtableDuane BaldwinBankers RoundtableKeviar Warner Frederick HonoldCertiCo LLCRichard Ankney Daniel GeerCerticom CorporationDon B. JohnsonChase Manhattan BankGene Rao Richard YenCommunications Security EstablishmentMichael Chawrun Alan PoploveCybersafe CorporationGlenda Barnes David O'BrienCylink CorporationKamy Kavianian Lily Lidong ChenDeluxe CorporationCorporation Chuck BramDigital Equipment Corporation/CompaqDonald HoldenErnst & Young, LLPRichard Sweeney Michael Versace Gary ChaulklinFirst Data CorporationGare Rain Ralph Spencer PooreFirst Data CorporationGarey Chaulklin Gary ChaulklinFirst Data CorporationJames Ramsay Sandra LambertFord Marketing InstituteTed Mason Joy NicholasFord Marketing InstituteTed Mason Joy NicholasFortress TechnologiesEva BozokiGilbarco Inc.Kena Smith	Bank of America	Kathleen Gibbons
Richard Phillips Martin JohnsonBank One CorpDuane BaldwinBankers RoundtableKeviar WarnerFrederick HonoldFrederick HonoldCertCo LLCRichard Ankney Daniel GeerCerticom CorporationDon B. JohnsonChase Manhattan BankGene Rao Richard YenCommunications Security EstablishmentMichael Chawrun Alan PoploveCybersafe CorporationGene Rao Richard YenCybersafe CorporationGene Rao Richard YenCylink CorporationCory Surges Maruy Jansen Lily Lidong ChenDeluxe CorporationCory Surges Maruy JansenDigital Equipment Corporation/CompaqDonald HoldenErnst & Young, LLPRichard Kastner Ralph Spencer Poore Federal Reserve BankRichard Sweeney Michael Versace Gary ChaulklinFirst Data CorporationGene Kathol First Union CorporationJames Ramsay Sandra LambertFood Marketing InstituteTed Mason Jay NicholasYa BozokiFortress TechnologiesFred Mason Jay NicholasYa Bozoki		Mack Hicks
Martin JohnsonBank One CorpDuane BaldwinBankers RoundtableKeviar WarnerFrederick HonoldFrederick HonoldCertCo LLCRichard AnkneyDaniel GeerCerticom CorporationConse Manhattan BankGene RaoRichard YenRichard YenCommunications Security EstablishmentMichael ChawrunAlan PoploveGlenda BarnesCybersafe CorporationGlenda BarnesDavid O'BrienLily Lidong ChenCylink CorporationCory SurgesMaury JansenChuck BramDigital Equipment Corporation/CompaqDonald HoldenErnst & Young, LLPRichard KastnerRalph Spencer PooreFrederick MasonFirst Data CorporationGene KatholFirst Data CorporationGene KatholFirst Union CorporationGene KatholFirst Union CorporationGene KatholFirst Union CorporationJames RamsaySandra LambertFod MasonJoy NicholasFortress TechnologiesFortress TechnologiesEva BozokiGilbarco Inc.Rena Smith		Richard Phillips
Bank One Corp Duane Baldwin Bankers Roundtable Keviar Warner Frederick Honold CertCo LLC Richard Ankney Daniel Geer Don B. Johnson Chase Manhattan Bank Gene Rao Communications Security Establishment Michael Chawrun Alan Poplove Olytenda Barnes Cybersafe Corporation Glenda Barnes David O'Brien Lily Lidong Chen Cylink Corporation Kamy Kavianian Lily Lidong Chen Donald Holden Deluxe Corporation/Compaq Donald Holden Entrust Technologies Richard Kastner Richard Sweeney Michael Versace Gary Chaulklin Gary Chaulklin First Data Corporation Gene Kathol First Union Corporation James Ramsay First Union Corporation Gene Kathol First Union Corporation James Ramsay Sandra Lambert Fod Mason Joy Nicholas Joy Nicholas Fortress Technologies Eva Bozoki		Martin Johnson
Bankers RoundtableKeviar Warner Frederick HonoldCertCo LLCRichard Ankney Daniel GeerCerticom CorporationDon B. JohnsonChase Manhattan BankGene Rao Richard YenCommunications Security EstablishmentMichael Chawrun Alan PoploveCybersafe CorporationGlenda Barnes David O'BrienCylink CorporationKamy Kavianian Lily Lidong ChenDeluxe CorporationCory Surges Maury Jansen Chuck BramDigital Equipment Corporation/CompaqDonald HoldenErnst & Young, LLPRichard Kastner Ralph Spencer PooreFederal Reserve BankRichard Sweeney Michael Versace Gary ChaulklinFirst Data CorporationGene KatholFirst Union CorporationJames Ramsay Sandra LambertFood Marketing InstituteTed Mason Joy NicholasFortress TechnologiesEva Bozoki Gilbarco Inc.	Bank One Corp	Duane Baldwin
Frederick HonoldCertCo LLCRichard Ankney Daniel GeerCerticom CorporationDon B. JohnsonChase Manhattan BankGene Rao Richard YenCommunications Security EstablishmentMichaelCommunications Security EstablishmentMichaelCommunications Security EstablishmentMichaelCybersafe CorporationGlenda Barnes David O'BrienCylink CorporationKamy Kavianian Lily Lidong ChenDeluxe CorporationCory Surges Maury Jansen Chuck BramDigital Equipment Corporation/CompaqDonald HoldenEntrust TechnologiesRobert Zuccherato Tim MosesFrnst & Young, LLPRichard Kastner Ralph Spencer PooreFederal Reserve BankRichard Sweeney Gary ChaulklinFirst Data CorporationGene Kathol James Ramsay Sandra LambertFood Marketing InstituteTed Mason Joy NicholasFoot Marketing InstituteEva BozokiFootress TechnologiesEva Bozoki	Bankers Roundtable	Keviar Warner
CertCo LLCRichard Ankney Daniel GeerCerticom CorporationDon B. JohnsonChase Manhattan BankGene Rao Richard YenCommunications Security EstablishmentMichael Chawrun Alan PoploveCybersafe CorporationGlenda Barnes David O'BrienCylink CorporationKamy Kavianian Lily Lidong ChenDeluxe CorporationCory Surges Maury Jansen Chuck BramDigital Equipment Corporation/CompaqDonald HoldenErnst & Young, LLPRichard Kastner Ralph Spencer Poore Federal Reserve BankRichard Sweeney Michael Versace Gary ChauklinFirst Data CorporationGene KatholFirst Union CorporationJames Ramsay Sandra LambertFood Marketing InstituteTed Mason Joy NicholasFortress TechnologiesEva BozokiFortress TechnologiesFea Bozoki		Frederick Honold
Daniel GeerCerticom CorporationDon B. JohnsonChase Manhattan BankGene Rao Richard YenCommunications Security EstablishmentMichael Chawrun Alan PoploveCybersafe CorporationGlenda Barnes David O'BrienCylink CorporationKamy Kavianian Lily Lidong ChenDeluxe CorporationCory Surges Maury Jansen Chuck BramDigital Equipment Corporation/CompaqDonald Holden Robert Zuccherato Tim MosesErnst & Young, LLPRichard Kastner Ralph Spencer PooreFederal Reserve BankRichard Sweeney Michael Versace Gary ChaulklinFirst Data CorporationGene Kathol First Union CorporationFood Marketing InstituteTed Mason Joy NicholasFootress TechnologiesEva Bozoki Gilbarco Inc.	CertCo LLC	Richard Ankney
Certicom CorporationDon B. JohnsonChase Manhattan BankGene Rao Richard YenCommunications Security EstablishmentMichael Chawrun Alan PoploveCybersafe CorporationGlenda Barnes David O'BrienCylink CorporationKamy Kavianian Lily Lidong ChenDeluxe CorporationCory Surges Maury Jansen Chuck BramDigital Equipment Corporation/CompaqDonald HoldenErnst & Young, LLPRichard Kastner Ralph Spencer PooreFederal Reserve BankRichard Sweeney Michael Versace Gary ChaulklinFirst Data CorporationGene Kathol James Ramsay Sandra LambertFood Marketing InstituteTed Mason Joy NicholasFortress TechnologiesTed Mason Joy NicholasFortress TechnologiesEva Bozoki		Daniel Geer
Chase Manhattan BankGene Rao Richard YenCommunications Security EstablishmentMichael Chawrun Alan PoploveCybersafe CorporationGlenda Barnes David O'BrienCylink CorporationKamy Kavianian Lily Lidong ChenDeluxe CorporationCorp Surges Maury Jansen Chuck BramDigital Equipment Corporation/CompaqDonald HoldenEntrust TechnologiesRobert Zuccherato Tim MosesErnst & Young, LLPRichard Kastner Ralph Spencer PooreFederal Reserve BankRichard Sweeney Michael Versace Gary ChaulklinFirst Data CorporationGene KatholFirst Union CorporationJames Ramsay Sandra LambertFood Marketing InstituteTed Mason Joy NicholasFortress TechnologiesEva BozokiGilbarco Inc.Rena Smith	Certicom Corporation	Don B. Johnson
Richard YenCommunications Security EstablishmentMichael Chawrun Alan PoploveCybersafe CorporationGlenda Barnes David O'BrienCylink CorporationKamy Kavianian Lily Lidong ChenDeluxe CorporationCory Surges Maury Jansen Chuck BramDigital Equipment Corporation/CompaqDonald HoldenEntrust TechnologiesRobert Zuccherato Tim MosesErnst & Young, LLPRichard Kastner Ralph Spencer PooreFederal Reserve BankRichard Sweeney Michael Versace Gary ChaulklinFirst Data CorporationGene Kathol James Ramsay Sandra LambertFood Marketing InstituteTed Mason Joy NicholasFortress TechnologiesEva Bozoki	Chase Manhattan Bank	Gene Rao
Communications Security EstablishmentMichael ChawrunAlan PoploveAlan PoploveCybersafe CorporationGlenda BarnesDavid O'BrienDavid O'BrienCylink CorporationKamy KavianianLily Lidong ChenLily Lidong ChenDeluxe CorporationCory SurgesMaury JansenChuck BramDigital Equipment Corporation/CompaqDonald HoldenEntrust TechnologiesRobert ZuccheratoTim MosesTim MosesErnst & Young, LLPRichard KastnerFederal Reserve BankRichard SweeneyMichael VersaceGary ChaulklinFirst Data CorporationGene KatholFirst Union CorporationJames RamsaySandra LambertFood Marketing InstituteFoot Marketing InstituteEva BozokiGilbarco Inc.Rena Smith		Richard Yen
Alan PoploveCybersafe CorporationGlenda Barnes David O'BrienCylink CorporationKamy Kavianian Lily Lidong ChenDeluxe CorporationCory Surges Maury Jansen Chuck BramDigital Equipment Corporation/CompaqDonald HoldenEntrust TechnologiesRobert Zuccherato Tim MosesErnst & Young, LLPRichard Kastner Ralph Spencer PooreFederal Reserve BankRichard Sweeney Michael Versace Gary ChaulklinFirst Data CorporationGene KatholFirst Union CorporationJames Ramsay Sandra LambertFood Marketing InstituteTed Mason Joy NicholasFortress TechnologiesEva Bozoki Gilbarco Inc.	Communications Security Establishment	Michael Chawrun
Cybersafe CorporationGlenda Barnes David O'BrienCylink CorporationKamy Kavianian Lily Lidong ChenDeluxe CorporationCory Surges Maury Jansen Chuck BramDigital Equipment Corporation/CompaqDonald HoldenEntrust TechnologiesRobert Zuccherato Tim MosesErnst & Young, LLPRichard Kastner Ralph Spencer PooreFederal Reserve BankRichard Sweeney Michael Versace Gary ChaulklinFirst Data CorporationGene KatholFirst Union CorporationJames Ramsay Sandra LambertFood Marketing InstituteTed Mason Joy NicholasFortress TechnologiesEva Bozoki Gilbarco Inc.	2	Alan Poplove
David O'BrienCylink CorporationKamy KavianianLily Lidong ChenLily Lidong ChenDeluxe CorporationCory SurgesMaury JansenChuck BramDigital Equipment Corporation/CompaqDonald HoldenEntrust TechnologiesRobert ZuccheratoTim MosesTim MosesErnst & Young, LLPRichard KastnerFederal Reserve BankRichard SweeneyMichael VersaceGary ChaulklinFirst Data CorporationGene KatholFirst Union CorporationJames RamsaySandra LambertTed MasonFood Marketing InstituteTed MasonJoy NicholasJoy NicholasFortress TechnologiesEva BozokiGilbarco Inc.Rena Smith	Cybersafe Corporation	Glenda Barnes
Cylink CorporationKamy Kavianian Lily Lidong ChenDeluxe CorporationCory Surges Maury Jansen Chuck BramDigital Equipment Corporation/CompaqDonald HoldenEntrust TechnologiesRobert Zuccherato Tim MosesErnst & Young, LLPRichard Kastner Ralph Spencer PooreFederal Reserve BankRichard Sweeney Michael Versace Gary ChaulklinFirst Data CorporationGene KatholFirst Union CorporationJames Ramsay Sandra LambertFood Marketing InstituteTed Mason Joy NicholasFortress TechnologiesEva BozokiGilbarco Inc.Rena Smith		David O'Brien
Lily Lidong Chen Cory Surges Maury Jansen Chuck Bram Digital Equipment Corporation/Compaq Entrust Technologies Ernst & Young, LLP Federal Reserve Bank First Data Corporation First Union Corporation Food Marketing Institute Food Marketing Institute Foot marketing Institute Fortress Technologies Fortress Technologies Fortress Technologies Fortress Technologies Fortress Technologies Fortress Technologies Corporation Corporatio	Cylink Corporation	Kamy Kavianian
Deluxe CorporationCory Surges Maury Jansen Chuck BramDigital Equipment Corporation/CompaqDonald HoldenEntrust TechnologiesRobert Zuccherato Tim MosesErnst & Young, LLPRichard Kastner Ralph Spencer PooreFederal Reserve BankRichard Sweeney Michael Versace Gary ChaulklinFirst Data CorporationGene KatholFirst Union CorporationJames Ramsay Sandra LambertFood Marketing InstituteTed Mason Joy NicholasFortress TechnologiesEva BozokiGilbarco Inc.Rena Smith	5 1	Lily Lidong Chen
Image: Addition of the second secon	Deluxe Corporation	Cory Surges
Digital Equipment Corporation/CompaqChuck BramDigital Equipment Corporation/CompaqDonald HoldenEntrust TechnologiesRobert ZuccheratoTim MosesTim MosesErnst & Young, LLPRichard KastnerRalph Spencer PooreRalph Spencer PooreFederal Reserve BankRichard SweeneyMichael VersaceGary ChaulklinFirst Data CorporationGene KatholFirst Union CorporationJames RamsaySandra LambertSandra LambertFood Marketing InstituteTed MasonJoy NicholasFortress TechnologiesFortress TechnologiesEva BozokiGilbarco Inc.Rena Smith	1	Maury Jansen
Digital Equipment Corporation/CompaqDonald HoldenEntrust TechnologiesRobert Zuccherato Tim MosesErnst & Young, LLPRichard Kastner Ralph Spencer PooreFederal Reserve BankRichard Sweeney Michael Versace Gary ChaulklinFirst Data CorporationGene KatholFirst Union CorporationJames Ramsay Sandra LambertFood Marketing InstituteTed Mason Joy NicholasFortress TechnologiesEva BozokiGilbarco Inc.Rena Smith		Chuck Bram
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	Digital Equipment Corporation/Compag	Donald Holden
Ernst & Young, LLP Richard Kastner Ernst & Young, LLP Richard Kastner 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	Entrust Technologies	Robert Zuccherato
Ernst & Young, LLPRichard Kastner Ralph Spencer Poore Richard Sweeney Michael Versace Gary ChaulklinFederal Reserve BankRichard Sweeney Michael Versace Gary ChaulklinFirst Data CorporationGene KatholFirst Union CorporationJames Ramsay Sandra LambertFood Marketing InstituteTed Mason Joy NicholasFortress TechnologiesEva BozokiGilbarco Inc.Rena Smith		Tim Moses
Federal Reserve Bank 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	Ernst & Young, LLP	Richard Kastner
Federal Reserve BankRichard Sweeney Michael Versace Gary ChaulklinFirst Data CorporationGene KatholFirst Union CorporationJames Ramsay Sandra LambertFood Marketing InstituteTed Mason Joy NicholasFortress TechnologiesEva BozokiGilbarco Inc.Rena Smith		Ralph Spencer Poore
Michael Versace Gary ChaulklinFirst Data CorporationGene KatholFirst Union CorporationJames Ramsay Sandra LambertFood Marketing InstituteTed Mason Joy NicholasFortress TechnologiesEva BozokiGilbarco Inc.Rena Smith	Federal Reserve Bank	Richard Sweeney
First Data CorporationGary ChaulklinFirst Data CorporationGene KatholFirst Union CorporationJames RamsaySandra LambertSandra LambertFood Marketing InstituteTed MasonJoy NicholasJoy NicholasFortress TechnologiesEva BozokiGilbarco Inc.Rena Smith		Michael Versace
First Data CorporationGene KatholFirst Union CorporationJames RamsaySandra LambertSandra LambertFood Marketing InstituteTed MasonJoy NicholasJoy NicholasFortress TechnologiesEva BozokiGilbarco Inc.Rena Smith		Gary Chaulklin
First Union Corporation James Ramsay Sandra Lambert Food Marketing Institute Ted Mason Joy Nicholas Fortress Technologies Eva Bozoki Gilbarco Inc. Rena Smith	First Data Corporation	Gene Kathol
Food Marketing Institute Sandra Lambert Food Marketing Institute Ted Mason Joy Nicholas Fortress Technologies Eva Bozoki Gilbarco Inc. Rena Smith	First Union Corporation	James Ramsay
Food Marketing InstituteTed Mason Joy NicholasFortress TechnologiesEva BozokiGilbarco Inc.Rena Smith		Sandra Lambert
Joy NicholasFortress TechnologiesEva BozokiGilbarco Inc.Rena Smith	Food Marketing Institute	Ted Mason
Fortress TechnologiesEva BozokiGilbarco Inc.Rena Smith		Joy Nicholas
Gilbarco Inc. Rena Smith	Fortress Technologies	Eva Bozoki
	Gilbarco Inc.	Rena Smith
Griffin Consulting Phillip Griffin	Griffin Consulting	Phillip Griffin

GTE Internetworking Harmonic Systems Incorporated IBM Corporation

Intel Corporation

IIT Research Institute KPMG Peat Marwick LLP M. Blake Greenlee Associates, Ltd. MasterCard International

Mellon Bank, N.A. Merrill Lynch

National Association of Convenience Stores National Security Agency NCR NIST

Northstar Technology Group, Inc. Pitney bowes, Inc. Price Waterhouse Coopers

Pulse EFT Association

Racal Guardata, Inc.

SAIC Security Dynamics SPYRUS

Technical Communications Corporation TECSEC Incorporated

VeriFone, Inc.

VISA International Wells Fargo Bank

Xcert International, Inc.

Patrick Cain Daniel Hunt Mohammad Peyravian Harry Hankla Stephen Mike Matyas Pamela Warren Steve Ellis Roger Westman Jeffrey Stapleton Blake Greenlee Ron Karlin William Poletti David Taddeo Lawrence LaBella John Dolan Ted Gerbracht Robert Swanson Gerard Rainville Mark Liddle Donna Dodson Miles Smid John Bowman Andrei Obrea John Hunt David Oshman Jeffrey Zimmerman Karen Gardstein Leslie Hendrix Scott Petersen Emile Soueid Samuel Epstein Wanda Gamble-Braggs Burt Kaliski Karen Randall Peter Yee John Gill Edward Scheidt Pud Reaver Jay Wack John Sheets Stuart Taylor Trong Nguyen William Chen Azita Amini Terry Leahy 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 PULSE EFT Association Schlumberger Ind SPYRUS

TECSEC Incorporated

U. S. Bancorp Verifone, Inc.

VISA International Wells Fargo Bank Tim Garland Vivian M. Banki Richard Carpenter Karen Randall Peter Yee Ed Scheidt Jay Wack Clarence Reaver Jeanne Fagan John Sheets Ken Gillman Rick Hite 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.