X9/TG-4, 1993

Financial Services Technical Publication
Developed By Accredited
Standards Committee
X9 - Financial Services

RECOMMENDED NOTATION FOR DEA KEY MANAGEMENT IN RETAIL FINANCIAL NETWORKS

Developed by
Accredited Standards Committee
X9 - Financial Services

Recommended Notation for DEA Key Management in Retail Financial Networks

This guideline has been prepared to address the widespread use of cryptography to protect financial transactions from fraud that has led to a need for a standard set of terms, acronyms and notation conventions, with which to communicate among the parties involved in transaction processing.

Developed by the
Accredited Standards Committee on Financial Services, X9
operating under the procedures of the
American National Standards Institute

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

CONTENTS

Page

Foreword i

1 Scope and purpose 1

1.1 Scope 1

1.2 Purpose 1

2 References 1

3 Document Organization 1

4 Acronyms for cryptographic keys 1

4.1 General 1

4.2 First position 1

4.3 Second position 1

4.4 Third position 2

4.5 Fourth position 2

4.6 Specific use of a key-encrypting key 2

5 Notation 3

5.1 General 3

5.2 Double-length keys 3

5.3 Cryptogram notation 3

5.4 Cryptographic operations 3

5.5 Key qualifiers 3

5.6 Other key management terms 4

5.7 Identifiers 4

Foreword

The widespread use of cryptography to protect financial transactions from fraud has led to a need for a standard set of terms, acronyms and notation conventions, with which to communicate among the parties involved in transaction processing. This guideline has been prepared to address that need. The focus is on the most commonly used terms related to personal identification number (PIN) encryption and verification, data authentication and encryption, and the cryptographic keys used to perform those functions.

This guideline was prepared by Accredited Standards Committee X9 – Financial Services.

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.

At the time it approved this guideline, the X9 Committee had the following members:

Harold G. Deal, Chairman
Jack Kilhefner, Vice Chairman, Administration
Eileen Bell, Vice Chairman, Membership/Marketing
Cynthia L. Fuller, Manager, ABA Standards Division
Jennifer L. Shuey, Assistant Manager, ABA Standards Division

Organization Represented	*Name of Representative*
American Bankers Association	Andy Ernst
American Express Company	Eileen Bell
Applied Communications	Dale Ratliff
Bank of America	John Coombs
Canadian Bankers Association	Tom Anderson
Chase Manhattan Bank, N.A.	John McKessy
Chemical Bank, N.A.	Francis J. Keenan
Citicorp	Seymour R. Rosen
Continental Bank, N.A.	Joseph P. O'Toole
CoreStates Bank	Kent Seinfeld
Deluxe Corporation	James Gallup
Discover Card Services, Inc.	Bill Kabot
Federal Reserve Bank	Michael Garrett
First Interstate Bank of CA	Clarence Collins
IBAA	Viveca Ware
IBM Corporation	Daniel Sundberg
MasterCard International	Alice Droogan
Mellon Bank, N.A.	David P. Taddeo
National Security Clearing Corp.	Walter Cushman
National Security Agency	Gerard A. Rainville, Jr.
NationsBank Services, Inc.	Harold G. Deal
NCR Corporation	A.R. Daniels
New York Clearing House Assn.	Vincent De Santis
Nat'l Institute of Science & Technology	Miles Smid
PNC Financial Corporation	Kenneth Leckey
Sears Technology Services	Lori Eisenstaedt
Union Bank	Joseph Martino
UNISYS Corporation	Karl T. Sammons
U.S. Dept. of Treasury	Martin Ferris
VISA International	Patricia Greenhalgh
Wells Fargo Bank	Jack Kilhefner
XEROX Corporation	Frank Bov

Subcommittee X9A on Electronic Retail Financial Transactions, which developed this guideline, had the following members:

Honora A. Norton, Chair
Mark Zalewski, Vice Chair

Organization Represented	*Name of Representative*
American Bankers Association	Anne Livingston
American Express Company	Eileen Bell
Applied Communications	Kate Herse
AT&T	Priscilla Cronin
Bank of America	Paul Lohse
Canadian Bankers Association	Vas Alexiou
Citicorp	Bill Burnett
DataCard Corporation	Robert J. Leppke
Deluxe Corporation	James Gallup
Discover Card Services, Inc.	Bill Kabot
Electronic Data Systems Inc.	Daniel Twing
First Data Resources	Eugene Kathol
GTE Spacenet	Mark Zalewski
MagTek	Azita Amini
MasterCard International	Alice Droogan
National Data Corporation	George Wilcox
NationsBank Services Inc.	Harold G. Deal
Navy Federal Credit Union	Joan Wood
NCR Corporation	Phyllis Ashworth
Plus Systems, Inc.	Kirby Slunaker
Tyme Corporation	James H. Martin
UNISYS Corporation	Benjamin A. Dent
VISA International	Patricia Greenhalgh
Wells Fargo Bank	Loraine Boland

Working Group X9A3 on Security in Financial Networks, which developed this guideline, had the following participants:

Dennis Abraham, Chairman

Dennis Abraham
Caroline Archer
Joanne Barringer
Patty Bart
Mike Biskobing
Gerry Bordic
Thomas Britton
Carl Campbell
Bruce Carothers
William Cashel
Gary Chaulkin
Bill Chen
Tim Dickson
Alice Droogan
Lore Eisenstaedt
Steve Fisher
Cindy Fuller
Sally Graham
Peter Gregory
Charles Heckman
Sonia Hendrix
Larry Hines
Glenn Inouye
Jerry Johnson
Darlene Kargei
Rick Kastner
Timothy Knowlton
Beth Lynn
Hugh Mador
Lan Mai
Jerry McDaniel
Jean McWeeney
Kay Neumayer
Ramona Payne
Bob Pennington
Scott Petersen
Frank Pledad
Bob Propp
Bob Protheroe
James Ralah
Chas Randall
Karen Randall
Joan Rawlins
Pud Reaver
Sonia Reed
Barry Rhodes
Cheryl Rodi
Dan Sass
Steve Sherwood
Larry Siedentop
Miles Smid
Jeff Stapleton
Donald Sweet
Mark Wickham
Scott Wilson

Recommended Notation for DEA Key Management in Retail Financial Networks — Guideline

1 Scope and purpose

1.1 Scope

The aspects of transaction security covered include PIN encryption and verification, data authentication and encryption, and cryptographic key management, using the American National Standards Institute Data Encryption Algorithm (DEA).

This document does not address how the elements of this vocabulary are used in security techniques. See Section 2, References, for information on the use of the DEA in security techniques.

1.2 Purpose

It is the purpose of this document to establish a framework for a common vocabulary which can be used to describe retail financial transaction security, specifically cryptographic security, based on the use of secret keys.

2 References

The reader is referred to the following publications for information on the use of cryptography in financial transaction processing:

ANSI X3.92–1987, *Data Encryption Algorithm (DEA)*

ANSI X3.106–1983, *Modes of DEA Operation*

ANSI X9.8–1991, *Personal Identification Number (PIN) Management and Security*

ANSI X9.19–1986, *Financial Institution Retail Message Authentication*

ANSI X9.24–1992, *Financial Services Retail Key Management*

ANSI X9.17–1991, *Financial Institution Key Management (Wholesale)*

ANSI X9.9–1986, *Financial Institution Message Authentication (Wholesale)*

3 Document organization

The remainder of this document is divided into two sections:

- Section 4 defines a set of acronyms to represent different cryptographic key types.
- Section 5 defines notation conventions to use in the description of various cryptographic and key management processes.

4 Acronyms for cryptographic keys

4.1 General

Presented below is a system of acronyms for use in the representation of classes of cryptographic keys. The acronyms used for representing key types can be as few as two, and as many as four letters in length, depending on how broad or how specific the reference to the key type needs to be. Some users may never need more than a two-letter acronym, and some may require four-letter acronyms, depending on the complexity or level of detail desired.

Also included are hyphenated acronyms. This is a special class of acronyms used only with key-encrypting keys, for the purpose of specifying the type of key encrypted. Hyphenated acronyms can be greater than four letters in length.

4.2 First position

All cryptographic key acronyms begin with upper case "K" in the first position.

4.3 Second position

The second position classifies the key as follows:

K – key-encrypting
P – PIN-related
D – non-PIN data encryption
A – authentication

The following two-letter acronyms may be used to represent keys where only their broadest functional classification needs to be communicated:

KK – key-encrypting key
KP – PIN-related key
KD – non-PIN data encryption key
KA – authentication key