

ENGINE REFERENCE
DO NOT TAKE FROM THIS ROOM

ANSI X9.17
1995

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

**FINANCIAL INSTITUTION KEY
MANAGEMENT (WHOLESALE)**



Developed by
Accredited Standards Committee
X9 - Financial Services

PUBLISHED BY
X9 - SECRETARIAT
AMERICAN BANKERS ASSOCIATION

11/11/2016 10:00:00 AM



ANSI®
X9.17-1995

American National Standard
for Financial Services

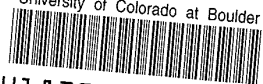
Financial Institution Key Management
(Wholesale)

Secretariat

American Bankers Association

Approved: October 6, 1995

American National Standards Institute, Inc.

University of Colorado at Boulder

U18304 9002201

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CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time.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

EDI Support Services, Inc.
P.O. Box 203, Chardon, OH 44024
Order Desk: 800-334-4912
International Orders: 216-974-7650

Copyright © 1995 by American Bankers Association, Standards Division
All rights reserved.

No part of this publication may be reproduced in any form, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without prior written permission from the X9 Secretariat, c/o American Bankers Association.

Printed in the United States of America

Contents

	Page
Foreword	vii
1 Scope	1
2 Definitions and common abbreviations	1
2.1 Definitions	1
2.2 Common abbreviations	4
3 Key management facility protection	7
3.1 General	7
3.2 Facility requirements	7
3.3 Key entry	7
3.4 Transportation and storage	7
3.5 Cryptographic module operational integrity	8
3.6 Destruction of keys	8
4 Key management requirements	9
4.1 General requirements	9
4.2 Automated key management architecture	9
4.3 Automated key management architecture	11
5 Key and initialization vector generation	11
5.1 General requirements	11
5.2 Generation of keys and IVs for manual distribution	11
5.3 Generation of keys and IVs for automated distribution	11
6 Key and IV distribution	12
6.1 General	12
6.2 Automated key distribution environments	12
6.3 Manual key distribution	13
6.4 Automated key distribution	13
7 Key and IV encryption and decryption	14
7.1 Notation	14
7.2 Encryption, decryption, authentication and error detection	15
7.3 Counters	19
7.4 Offsetting of keys	21
7.5 Notarization of keys	22
8 Cryptographic service messages	25
8.1 General	25
8.2 Cryptographic service message classes	25

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts



Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research



With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips



Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.