



American National Standard for Financial Services

ANSI X9.102

Symmetric Key Cryptography For the Financial Services Industry— Wrapping of Keys and Associated Data—

June 2008



Accredited Standards Committee X9, Incorporated
Financial Industry Standards

Date Approved:

American National Standards Institute

American National Standards, Technical Reports and Guides developed through the Accredited Standards Committee X9, Inc., are copyrighted. Copying these documents for personal or commercial use outside X9 membership agreements is prohibited without express written permission of the Accredited Standards Committee X9, Inc. For additional information please contact ASC X9, Inc., 1212 West Street, Suite 200, Annapolis, Maryland 21401.

This is a preview of "X9.102-2008". [Click here to purchase the full version from the ANSI store.](#)

Contents	Page
Foreword	v
Introduction.....	vi
1 Scope	1
2 Conformance.....	1
3 Normative references	1
4 Terms and definitions	2
5 Symbols and abbreviated terms	3
6 Preliminaries	5
6.1 Key wrapping	5
6.2 Summary of the four key wrap mechanisms and the underlying block ciphers	5
6.3 Overview and comparison of data elements	6
6.4 Integrity protection.....	6
6.4.1 Overview	6
6.4.2 Default ICVs for AESKW and TDKW.....	7
6.4.3 Extending the scope of the data integrity for AESKW and TDKW	7
6.4.4 Generation of the ICV for AKW1	7
7 Specifications of key wrap mechanisms	8
7.1 AESKW	8
7.1.1 Overview and organization.....	8
7.1.2 AESKW data requirements	8
7.1.3 AESKW plaintext formatting function	9
7.1.4 AESKW integrity check function.....	9
7.1.5 AESKW wrapping function	10
7.1.6 AESKW unwrapping function.....	11
7.2 TDKW	12
7.2.1 Overview and organization.....	12
7.2.2 TDKW data requirements.....	13
7.2.3 TDKW plaintext formatting function	13
7.2.4 TDKW integrity check function	13
7.2.5 TDKW wrapping function.....	14
7.2.6 TDKW unwrapping function	15
7.3 AKW1	16
7.3.1 Overview and organization.....	16
7.3.2 AKW1 data requirements.....	16
7.3.3 AKW1 wrapping function.....	17
7.3.4 AKW1 unwrapping function	18
7.4 AKW2	19
7.4.1 Overview	19
7.4.2 AKW2 data requirements.....	19
7.4.3 AKW2 wrapping function.....	20
7.4.4 AKW2 unwrapping function	21
Annex A (Informative) Security considerations.....	23

ANS X9.102-2008

A.1	Overview	23
A.2	Security levels.....	23
A.2.1	Key wrap mechanisms	23
A.2.2	The wrapped key in a consuming application	23
A.3	Assurance of Confidentiality	24
A.3.1	Bit Dependencies.....	24
A.3.2	Concealing the Equality of Plaintexts	24
A.4	Assurance of Integrity	25
A.4.1	General integrity assurance	25
A.4.2	When the associated data string is a representative for the actual message string	25
A.4.3	Relying Party Integrity.....	26
A.5	Summary of Security Against Generic Attacks.....	26
Annex B (Informative)	Alternative descriptions for software implementations	27
B.1	Overview	27
B.2	AESKW wrapping function	27
B.3	AESKW unwrapping function.....	28
B.4	TDKW wrapping function.....	28
B.5	TDKW unwrapping function	29

Figures

Figure 1	— The AESKW wrapping function	11
Figure 2	— The AESKW unwrapping function.....	12
Figure 3	— The AKW1 wrapping function.....	18
Figure 4	— The AKW1 unwrapping function	19
Figure 5	— The AKW2 wrapping function.....	21
Figure 6	— The AKW2 unwrapping function	22

Tables

Table 1	— Security Against Generic Attacks.....	26
---------	---	----

Foreword

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
1212 West Street, Suite 200
Annapolis, MD 21401 USA
X9 Online <http://www.x9.org>

Copyright © 2007 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.

ANS X9.102-2008

Introduction

The protection of the integrity/authenticity of confidential data is often important and sometimes crucial to the security of an information system. However, the interaction of an encryption algorithm with a separate authentication algorithm can lead to unexpected vulnerabilities; see Ref. [5], for example. Therefore, recent years have seen the development of dedicated, single mechanisms for authenticated encryption. This Standard specifies several such mechanisms, called key wraps, that are intended for the protection of cryptographic keys and other specialized data, whether in storage or in transport.

For general use, this Standard specifies a particularly robust mechanism that is based on the AES algorithm; an analogue based on the Triple Data Encryption Algorithm (TDEA) is also specified. The conservative security of these mechanisms comes with a corresponding cost in performance. The rationale for this design choice is that the protection of keys is paramount, and in many systems the extra overhead for their management can be tolerated.

In addition, this Standard specifies two other key wrap mechanisms that are based on TDEA. One of them is specified to support the S/MIME protocol of the IETF. The other is tailored to the needs of particular legacy systems in the financial services industry.

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, 1212 West Street, Suite 200, Annapolis, MD 21401 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.

The X9 committee had the following members:

James Shaffer, X9 Chairman
Vincent DeSantis, X9 Vice-Chairman
Cynthia Fuller, Executive Director

<i>Organization Represented</i>	<i>Representative</i>
ACI Worldwide	James Shaffer
American Bankers Association	C. Diane Poole
American Express Company	Mark Merkow
American Financial Services Association	Mark Zalewski
Bank of America	Daniel Welch
Certicom Corporation	Daniel Brown
Citigroup, Inc.	Gary Word

CUSIP Service Bureau	James Taylor
Deluxe Corporation	John Fitzpatrick
Diebold, Inc.	Bruce Chapa
Discover Financial Services	Deana Morrow
Federal Reserve Bank	Dexter Holt
First Data Corporation	Rick Van Luvender
Fiserv	Skip Smith
FSTC, Financial Services Technology Consortium.....	Daniel Schutzer
Harland Clarke.....	John McCleary
Hewlett Packard	Larry Hines
Hypercom	Scott Spiker
IBM Corporation.....	Todd Arnold
Ingenico	John Spence
Intuit, Inc.	Jana Hocker
JP Morgan Chase & Co	Jacqueline Pagan
KPMG LLP	Mark Lundin
Mag-Tek, Inc.	Carlos Morales
Metavante Image Solutions	Ron Schultz
NACHA The Electronic Payments Association	Nancy Grant
National Association of Convenience Stores	Michael Davis
National Security Agency	Paul Timmel
NCR Corporation	Steve Stevens
SWIFT/Pan Americas	James Wills
The Clearing House	Vincent DeSantis
U.S. Bank	Brian Fickling
University Bank	Stephen Ranzini
VeriFone, Inc.	Brad McGuinness
VISA	Richard Sweeney
Wachovia Bank	Raymond Gatland
Wells Fargo Bank	Ruven Schwartz

ANS X9.102-2008

The X9F subcommittee on Data and Information Security had the following members:

Richard J. Sweeney, X9F Chairman
 Sandra Lambert, X9F Vice Chairman

<i>Organization Represented</i>	<i>Representative</i>
[3PEA Technologies, Inc.	Mark Newcomer
ACI Worldwide	Jim Shaffer
American Express Company	Mark Merkow
American Financial Services Association	Mark Zalewski
Bank of America	Daniel Welch
Certicom Corporation	Daniel Brown
Citigroup, Inc.	Gary Word
ClearWave Electronics	Mark Ross
Communications Security Establishment	Alan Poplove
CUSIP Service Bureau	Scott Preiss
DeLap, White, Caldwell and Croy, LLP	Darlene Kargel
Deluxe Corporation	John Fitzpatrick
Depository Trust and Clearing Corporation	Robert Palatnik
Diebold, Inc.	Bruce Chapa
Discover Financial Services	Julie Shaw
Entrust, Inc.	Miles Smid
Federal Reserve Bank	Dexter Holt
Ferris and Associates, Inc.	J. Martin Ferris
First Data Corporation	Rick Van Luvender
Fiserv	Bud Beattie
FSTC, Financial Services Technology Consortium	Daniel Schutzer
Futurex	Jason Anderson
Geobridge	Jeff Stapleton
Harland Clarke	John McCleary
Hewlett Packard	Larry Hines
Hypercom	Scott Spiker
IBM Corporation	Todd Arnold
InfoGuard Laboratories	Tom Caddy
Ingenico	John Spence
Innové, LLC.....	Steven Teppler
Intel Massachusetts, Inc.	Paul Posco
JP Morgan Chase & Co	Edward Koslow
KPMG LLP	Mark Lundin
Mag-Tek, Inc.	Carlos Morales
MasterCard International	Michael Ward
Metavante Image Solutions	Ron Schultz
National Institute of Standards and Technology	Elaine Barker
National Security Agency	Paul Timmel
NCR Corporation	David Norris
NTRU Cryptosystems	William Whyte
Pitney Bowes Inc.	Leon Pintsov
Rosetta Technologies	Jim Maher
RSA, The Security Division of EMC.....	James Randall
Surety, Inc.	Dimitrios Andivahis
Thales e-Security, Inc.	James Torjussen
The Clearing House.....	Vincent DeSantis

Triton Systems of Delaware, Inc.	Daryll Cordeiro
U.S. Bank.....	Robert Thomas
Unisys Corporation	David J. Concannon
University Bank	Stephen Ranzini
VeriFone	Dave Faoro
VISA	John Sheets
Voltage Security, Inc.....	Luther Martin
Wachovia Bank	Raymond Gatland
Wells Fargo Bank	Ruven Schwartz

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 X9F1 Cryptographic Tool Standards and Guidelines group which developed this standard had the following members:

Miles Smid, Chairman and Morris Dworkin, Project Editor

<i>Organization Represented</i>	<i>Representative</i>
Certicom Corporation	Dan Brown
.....	Scott Vanstone
Communications Security Establishment of Canada	Bridget Walshe
Entrust	Don Johnson
.....	Robert Zuccherato
HP	Susan Langford
Innové, LLC	Ralph Poore
National Institute of Standards and Technology	Morris Dworkin
.....	Elaine Barker
.....	John Kelsey
.....	Lily Chen
National Security Agency	Paul Timmel
.....	Michael Boyle
NTRU	William Whyte
ORION	Miles Smid
Pitney Bowes, Inc	Matt Compagna
RSA Security	James Randall
.....	Burt Kaliski
.....	Steve Schmalz
University Bank.....	Mick Talley

This is a preview of "X9.102-2008". [Click here to purchase the full version from the ANSI store.](#)

Symmetric Key Cryptography for the Financial Services Industry —Wrapping of Keys and Associated Data

1 Scope

This Standard specifies four key wrap mechanisms based on ASC X9-approved symmetric key block ciphers whose block size is either 64 bits or 128 bits. The key wrap mechanisms can provide assurance of the confidentiality and the integrity of data, especially cryptographic keys or other specialized data.

2 Conformance

An implementation of the following mechanisms for authenticated encryption may claim conformance with this Standard:

- AESKW (Clause 7.1)
- TDKW (Clause 7.2)
- AKW1 (Clause 7.3)
- AKW2 (Clause 7.4)
- CCM (normative reference [3.6] below).

An implementation of AKW2 may only claim conformance with this Standard in conjunction with TR-31 [3.1].

3 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.

[3.1] Accredited Standards Committee X9, Incorporated, TR-31—2005: Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms.

[3.2] ANS X9.24 Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques: 2004.

[3.3] FIPS Publication 197, Advanced Encryption Standard (AES), U.S. DoC/NIST, November 26, 2001; ASC X9 Registry 00002.