American National Standard
for Financial Services

X9.73–October–2002

Cryptographic Message Syntax

Secretariat:
American Bankers Association

Approved:

American National Standards Institute

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CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time.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

American Bankers Association
1120 Connecticut Ave., NW
Washington, DC 20036 USA
Customer Service Center 1(800) 338-0626 or 1(202) 663-5087
Fax 1(202) 663-7543, E-mail custserv@aba.com
X9 Online http://www.x9.org

Contents

Foreword 1

Introduction 4

1 Scope 9

2 Normative references 9

3 Terms, definitions, symbols and abbreviated terms 10

4 Organization 14

5 Application 15

6 Message Structures 15
6.1 General 15
6.2 Signed Data 17
6.2.1 General 17
6.2.2 Signed Attributes 21
6.2.3 Unsigned Attributes 24
6.2.4 Certificate Formats 25
6.2.5 Detached Signatures 26
6.3 Enveloped Data 26
6.3.1 General 26
6.3.2 Detached Data 28
6.3.3 Certificate Formats 28
6.4 Authenticated Data 29
6.5 Digested Data 30
6.6 Encrypted Data 30
6.7 Named Key Encrypted Data 31
6.8 Nesting of Structures 31
6.9 Receipts 31
6.10 Aggregate Data Signing 31

7 Key Management Processing 31
7.1 General 31
7.2 Asymmetric Key Transport 32
7.3 Asymmetric Key Agreement 32
7.4 Pre-established Key Encryption Keys 33
7.5 External Mechanisms – Constructive Key Management 34
7.5.1 General 34
7.5.2 CKM Recipients 34
7.5.3 CKM Envelopes 35

8 S/MIME Formatting 38

9 Conformance Classes 38

Annex A (normative) **ASN.1 Module for Object Identifiers** 40

Annex B (normative) **X9.73 CMS Syntax** **43**
Annex C (informative) **Example Using CKM** **55**
Annex D (informative) **Example Using ANS X9.24 Key Management** **58**
Bibliography **59**

Introduction

NOTE: The user's attention is called to the possibility that compliance with this standard may require the 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 non-discriminatory 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, American Bankers Association, 1120 Connecticut Avenue, N.W., Washington, D.C. 20036.

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.
Secretariat will provide current text for the following:

The X9 committee had the following members:
Harold Deal, Chairman
Vincent DiSantis, Vice Chairman
Cynthia L. Fuller, Managing Director
Darlene J. Schubert, Program Manager

Organization Represented	Representative
ACI Worldwide	Cindy Rink
ACI Worldwide	Jim Shaffer
American Bankers Association	Stephen Schutze
American Bankers Association	Michael Scully
American Express Company	Mike Jones
American Express Company	Dick Schreiber
American Express Company	Gerry Smith
American Express Company	Barbara Wakefield
BB&T	Harold Deal
BancTec, Inc.	Christopher Dowdell
BancTec, Inc.	David Hunt
Bank One Corporation	Kimberly Ray
Bank of America	Mack Hicks
Bank of America	Richard Phillips
Bank of America	Daniel Welch
Caradas	John Gould
Caradas	Richard Kastner
Certicom Corporation	Donald Johnson

Certicom Corporation	Daniel Brown
Check Solutions	Harry Hankla
Check Solutions	Don Harman
Check Solutions	Ron Schultz
Check Solutions	Jerry Bowman
Citibank	Bill Burnett
Citibank	David Budinger
Citibank	Dan Schutzer
Compaq Computer Corporation	Larry Hines
Compaq Computer Corporation	Gary Lefkowitz
Deluxe Corporation	Maury Jansen
Diebold, Inc.	Bruce Chapa
Diebold, Inc.	Judy Edwards
Discover Financial Services Inc.	Masood Mirza
Discover Financial Services Inc.	Pam Ellington
eFunds Corporation	Chuck Bram
eFunds Corporation	Forrest Martin
eFunds Corporation	Cory Surges
Federal Reserve Bank	Dexter Holt
First Data Corporation	Gene Kathol
Food Marketing Institute	Ted Mason
Food Marketing Institute	Stacy Fitzgerald-Redd
Griffin Consulting	Phillip H. Griffin
Griffin Consulting	Harriette Griffin
HW & W Inc.	Martin Ferris
JP Morgan Chase &Co	Robert Blair
JP Morgan Chase & Co	Richard Yen
KPMG LLP	Jeff Stapleton
KPMG LLP	Al Van Ranst, Jr.
Mag-Tek, Inc.	Carlos Morales
Mag-Tek, Inc.	Jeff Duncan
Mag-Tek, Inc.	Mimi Hart
Mag-Tek, Inc.	Terry Benson
MasterCard International	Ron Karlin
MasterCard International	Naiyre Foster
Mellon Bank, N.A.	Richard Adams
Mellon Bank, N.A.	David Taddeo
Merrill Lynch	John Roy
Merrill Lynch	Jennifer Smith
National Association of Convenience Stores	John Hervey
National Association of Convenience Stores	Teri Richmond
National Security Agency	Greg Bergren
National Security Agency	Sheila Brand
NCR Corporation	David Norris
NCR Corporation	Steve Stevens
New York Clearing House	Vincent DeSantis
New York Clearing House	John Dunn

PricewaterhouseCoopers	Jeff Zimmerman
Silas Technologies	Andrew Garner
Silas Technologies	Ray Gatland
SPYRUS	Karen Randall
SPYRUS	James Randall
Star Systems, Inc.	Elizabeth Lynn
Star Systems, Inc.	Michael Wade
Sun Microsystems PS	Yvonne Humphery
Sun Microsystems PS	Joel Weise
Unisys Corporation	Thomas Hayosh
Unisys Corporation	Navnit Shah
VeriFone	Brad McGuinness
VeriFone.	John Sheets
VeriFone	Brenda Watlington
VISA International	Patricia Greenhalgh
Wells Fargo Bank	Terry Leahy
Wells Fargo Bank	Ruven Schwartz

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

Richard Sweeney, Chair, Inovant

Organization	**Representative**
ACI Worldwide	Jim Shaffer
American Bankers Association	Stephen Schutze
American Bankers Association	Michael Scully
American Express Company	Mark Merkow
American Express Company	Gerry Smith
American Express Company	Mike Jones
BancTec, Inc.	Christopher Dowdell
Bank of America	Mack Hicks
Bank of America	Craig Worstell
Bank One Corporation	Mark Ryding
BB&T	Harold Deal
Caradas	Richard Kastner
Certicom Corporation	Don Johnson
Check Solutions	Harry Hankla
Check Solutions	Ron Schultz
Check Solutions	Jerry Bowman
Chrysalis-ITS	Terry Fletcher
Communications Security Establishment	Alan Poplove
Communications Security Establishment	Mike Chawrun
Datum, Inc	Sandra Lambert
Deluxe Corporation	Maury Jansen
Diebold, Inc.	Bruce Chapa
Diebold, Inc.	Judy Edwards
Digital Signature Trust	Brandon Brown
Digital Signature Trust	Trent Henry
Diversinet Corporation	Michael Crerar
eFunds Corporation	Chuck Bram

eFunds Corporation	Cory Surges
Entrust Technologies	Santosh Chokhani
Entrust Technologies	Miles Smid
Entrust Technologies	Mike Just
Federal Reserve Bank	Dexter Holt
First Data Corporation	Gene Kathol
First Data Corporation	Lisa Curry
First Data Corporation	Michael Hodges
Food Marketing Institute	Ted Mason
Food Marketing Instittute	Stacy Fitzgerald-Redd
Griffin Consulting	Phillip H. Griffin
Griffin Consulting	Harriette Griffin
IBM Corporation	Todd Arnold
InnoVentry	Anita Jimenez
Inovant	Richard Sweeney
Jones Futurex, Inc.	Steve Junod
JP Morgan Chase & Co	Richard Yen
KPMG LLP	Jeff Stapleton
KPMG LLP	Al Van Ranst, Jr.
KPMG LLP	Azita Amini
Mag-Tek, Inc.	Mimi Hart
Mag-Tek, Inc.	Terry Benson
MasterCard International	Ron Karlin
MasterCard International	William Poletti
Mellon Bank, N.A.	David Taddeo
Mellon Bank, N.A.	Genien Carlson
Merrill Lynch	Lawrence LaBella
Merril Lynch	Jennifer Smith
National Association of Convenience Stores	John Hervey
National Security Agency	Gregory Bergren
National Security Agency	Sheila Brand
NCR Corporation	Adrian Shields
NCR Corporation	Steve Stevens
NEC Zefer	Michael Versace
NIST	Elaine Barker
NIST	Morris Dworkin
Pitney Bowes, Inc.	Andrei Obrea
Pitney Bowes, Inc.	Leon Pintsov
PricewaterhouseCoopers	Jeff Zimmerman
Rainbow Technologies	Paul Blomgren
Rainbow Technologies	Georgina Schroder
Rainbow Technologies	Vic Sundararajan
RSA Securities	Russ Housley
RSA Securities	Burt Kaliski
SPYRUS	Karen Randall
SPYRUS	James Randall
Star Systems, Inc.	Elizabeth Lynn

Star Systems, Inc.	Michael Wade
Star Systems, Inc.	Carol Fazzone
Sun Microsystems PS	Joel Weise
TECSEC Incorporated	Ed Scheidt
TECSEC Incorporated	Jay Wack
Datum, Inc	Sandra Lambert
VeriFone	John Sheets
Verisign, Inc.	Warwick Ford
VISA International	Richard Hite
Wells Fargo Bank	Ruven Schwartz
Wells Fargo Bank	Terry Leahy
Zaxus, Inc.	Samuel Epstein

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. (Note: Per X9 policy, company names of non-member participants are listed only if, at time of publication, the X9 Secretariat received an original signed release permitting such company names to appear in print.)

The X9F3 Working Group, which developed this standard had the following members:

C. L. Reaver, Chair

Ersin Domangue, Technical Editor

Rich Ankney, Technical Editor

Special thanks to Phil Griffin for his work with the ASN.1

Organization	**Representative**
TBD	

Cryptographic Message Syntax (CMS)

1 Scope

This Standard specifies a cryptographic message syntax that can be used to protect financial transactions and other documents from unauthorized disclosure and modification. The message syntax has the following characteristics:

1) Messages are protected independently. There is no cryptographic sequencing (e.g., cipher block chaining) between messages. There need not be any real-time connection between the sender and recipient of the message. This makes the syntax suitable for use over store-and-forward systems, e.g. Automated Clearing House (ACH). Standard attributes are defined to allow applications to maintain relationships between messages, if desired.

2) The syntax is algorithm independent. It supports confidentiality, integrity, origin authentication, and non-repudiation services. Only ANSI X9-approved algorithm(s) may be used for message encryption, digital signature, message authentication, and key management.

3) Support for biometric security (ANS X9.84), enhanced certificate techniques such as domain certificates (ANS X9.68) and key management extensions such as constructive key management (ANS X9.69) are provided.

4) Selective field protection can be provided by combining multiple instances of this syntax into a composite message.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. Nevertheless, parties to agreements based on this document are encouraged to consider applying the most recent edition of the referenced documents indicated below. For undated references, the latest edition of the referenced document (including any amendments) applies.

[1] ANS X9.42-2001, Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography.

[2] ANS X9.45-1997, Enhanced Management Controls Using Digital Signatures and Attribute Certificates.

[3] ANS X9.63-2001, Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography.