# American National Standard for Financial Services

# ANSI X9.73-2017

# Cryptographic Message Syntax — ASN.1 and XML

Accredited Standards Committee X9, Incorporated
Financial Industry Standards

**Date Approved: September 28, 2017**

American National Standards Institute

**This page left intentionally blank**

# Contents

Page

# 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CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time.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
275 West Street, Suite 107
Annapolis, MD 21401 USA
X9 Online http://www.x9.org

# Introduction

Financial business practices have changed with the introduction of computer and network-based technologies. Increased reliance on electronic transactions has heightened the need to manage the security of information and communications technology. Huge amounts in funds and securities are transferred daily by electronic communication mechanisms controlled by security practices based on business policies.

The high value or sheer volume of such transactions within an open environment exposes the financial community to the risk of potentially severe consequences from accidental or deliberate disclosure, alteration, substitution, or destruction of data. This risk is compounded by interconnected networks, and the increased number and sophistication of malicious adversaries. When financial transactions involve systemically important payment systems, these consequences may adversely affect national and global financial markets.

This standard defines a cryptographic message syntax that can be used to protect financial transactions and other information from the threats described above. The syntax is easily extensible in design to allow the use of any cryptographic algorithm defined in current or future standards appropriate for use by the financial services. The cryptographic syntax is suitable for the protection of the identity and rights management information critical for secure access control.

The syntax provides support for data confidentiality, data integrity, data origin authentication, and non-repudiation services needed to provide strong, mutual authentication. These services can be applied to prevent innovative types of fraud such as 'phishing' that are aimed at identity impersonation and theft, and which threaten the interests of financial institutions and their customers, the merchants, consumers and other actors of commerce.

Flexibility of key management techniques is provided through support for a variety of key establishment mechanisms, including key exchange, key agreement, password-based encryption and constructive key management. These techniques can be employed to mitigate risks, and to help financial institutions meet the legal and regulatory requirements of protecting sensitive business information, and the personal information of their customers and employees.

Use of this widely deployed syntax will lead to quick market acceptance in the financial community, lower costs due to economy of scale, and interoperability with a large number of existing standards and applications.

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, 275 West Street, Suite 107, 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.

At the time this standard was approved, the X9 committee had the following members:

Roy DeCicco, X9 Chair
Angela Hendershott, X9 Vice Chair
Steve Stevens, Executive Director
Janet Busch, Program Manager

| *Organization Represented* | *Representative* |
|---|---|
| ACI Worldwide | Doug Grote |
| American Bankers Association | Diane Poole |
| American Express Company | David Moore |
| Bank of America | Daniel Welch |
| Bank of New York Mellon | Arthur Sutton |
| Blackhawk Network | Anthony Redondo |
| Bloomberg LP | Corby Dear |
| Capital One | Marie LaQuerre |
| Citigroup, Inc. | Karla McKenna |
| CLS Bank | Ram Komarraju |
| Conexxus, Inc. | Gray Taylor |
| CUSIP Service Bureau | Gerard Faulkner |
| Delap LLP | Andrea Beatty |
| Delap LLP | Darlene Kargel |
| Deluxe Corporation | Angela Hendershott |
| Diebold Nixdorf | Bruce Chapa |
| Discover Financial Services | Michelle Zhang |
| eCurrency | David Wen |
| Federal Reserve Bank | Mary Hughes |
| First Data Corporation | Lisa Curry |
| FIS | Stephen Gibson-Saxty |
| Fiserv | Dan Otten |
| FIX Protocol Ltd - FPL | Jim Northey |
| Futurex | Ryan Smith |
| Gilbarco | Bruce Welch |
| Harland Clarke | John McCleary |
| Hewlett Packard | Terence Spies |
| IBM Corporation | Todd Arnold |
| Independent Community Bankers of America | Cary Whaley |
| Ingenico | Rob Martin |
| ISARA Corporation | Alexander Truskovsky |
| ISITC | Jason Brasile |
| ITS, Inc. (SHAZAM Networks) | Manish Nathwani |
| J.P. Morgan Chase | Roy DeCicco |
| KPMG LLP | Mark Lundin |
| MagTek, Inc. | Mimi Hart |
| MasterCard Europe Sprl | Mark Kamers |
| NACHA The Electronic Payments Association | Priscilla Holland |
| National Security Agency | Paul Timmel |
| Nautilus Hyosung | Joe Militello |
| NCR Corporation | David Norris |
| Office of Financial Research, U.S. Treasury Department | Thomas Brown Jr. |
| PCI Security Standards Council | Troy Leach |
| RouteOne | Chris Irving |
| RouteOne | Jenna Wolfe |
| SWIFT/Pan Americas | Karin DeRidder |
| SWIFT/Pan Americas | Frank Vandriessche |

Symcor Inc. ..... Debbi Fitzpatrick
TECSEC Incorporated ..... Ed Scheidt
The Clearing House ..... Sharon Jablon
U.S. Bank ..... John King
U.S. Commodity Futures Trading Commission (CFTC) ..... Robert Stowsky
USDA Food and Nutrition Service ..... Kathy Ottobre
Vantiv LLC ..... John Hall
VeriFone, Inc. ..... Dave Faoro
VISA ..... Kim Wagner
Wayne Fueling Systems ..... Steven Bowles
Wells Fargo Bank ..... Mark Schaffer

At the time this standard was approved, the X9F subcommittee on Data and Information Security had the following members:

Dave Faoro, X9F Chair
Steven Bowles, X9F Vice Chair

*Organization Represented* *Representative*

ACI Worldwide ..... Doug Grote
ACI Worldwide ..... Dan Kinney
ACI Worldwide ..... Julie Samson
American Bankers Association ..... Tom Judd
American Express Company ..... Farid Hatefi
American Express Company ..... John Timar
American Express Company ..... Kevin Welsh
Bank of America ..... Amanda Adams
Bank of America ..... Peter Capraro
Bank of America ..... Andi Coleman
Bank of America ..... Lawrence LaBella
Bank of America ..... Will Robinson
Bank of America ..... Michael Smith
Bank of America ..... Daniel Welch
BlackBerry Limited ..... Daniel Brown
Blackhawk Network ..... Vijay Bolina
Blackhawk Network ..... Anthony Redondo
Bloomberg LP ..... Erik Anderson
Bloomberg LP ..... Corby Dear
Capital One ..... Marie LaQuerre
Capital One ..... Johnny Lee
Cipherithm ..... Scott Spiker
comForte 21 GmbH ..... Thomas Gloerfeld
comForte 21 GmbH ..... Henning Horst
Communications Security Establishment ..... Jonathan Hammell
Communications Security Establishment ..... David Smith
Conexxus, Inc. ..... Alan Thiemann
CUSIP Service Bureau ..... Scott Preiss
Delap LLP ..... Andrea Beatty

Delap LLP ..... David Buchanan
Delap LLP ..... Darlene Kargel
Deluxe Corporation ..... Angela Hendershott
Deluxe Corporation ..... Margiore Romay
Deluxe Corporation ..... Andy Vo
Diebold Nixdorf ..... Christoph Bruecher
Diebold Nixdorf ..... Andrea Carozzi
Diebold Nixdorf ..... Bruce Chapa
Diebold Nixdorf ..... Michael Nolte
Diebold Nixdorf ..... Michael Ott
Diebold Nixdorf ..... Dave Phister
Discover Financial Services ..... Cheryl Mish
Discover Financial Services ..... Diana Pauliks
Discover Financial Services ..... Jordan Schaefer
eCurrency ..... David Wen
Federal Reserve Bank ..... Patrick Adler
Federal Reserve Bank ..... Guy Berg
Federal Reserve Bank ..... Marianne Crowe
Federal Reserve Bank ..... Amanda Dorphy
Federal Reserve Bank ..... Mary Hughes
Federal Reserve Bank ..... Heather Hultquist
Federal Reserve Bank ..... Janet LaFrence
Federal Reserve Bank ..... Susan Pandy
Federal Reserve Bank ..... Patti Ritter
Federal Reserve Bank ..... Daniel Rozycki
First Data Corporation ..... Annmarie Corrigan
First Data Corporation ..... Lisa Curry
First National Bank of Omaha ..... Kristi White
FIS ..... Chelsea Lopez
FIS ..... John Soares
FIS ..... Sunny Wear
Fiserv ..... Bud Beattie
Fiserv ..... Dan Otten
Futurex ..... Ryan Smith
GEOBRIDGE Corporation ..... Donna Gem
GEOBRIDGE Corporation ..... Jason Way
Gilbarco ..... Scott Turner
Gilbarco ..... Bruce Welch
Harland Clarke ..... Joseph Filer
Heartland Payment Systems ..... Scott Meeker
Hewlett Packard ..... Luther Martin
Hewlett Packard ..... Terence Spies
IBM Corporation ..... Todd Arnold
Independent Community Bankers of America ..... Cary Whaley
Ingenico ..... Rob Martin
ISARA Corporation ..... Mike Brown
ISARA Corporation ..... Alexander Truskovsky

ITS, Inc. (SHAZAM Networks) ..... Manish Nathwani
J.P. Morgan Chase ..... Bruce Geller
J.P. Morgan Chase ..... Kathleen Krupa
J.P. Morgan Chase ..... Jackie Pagán
J.P. Morgan Chase ..... Darryl Scott
K3DES LLC ..... Azie Amini
KPMG LLP ..... Mark Lundin
MagTek, Inc. ..... Jeff Duncan
MagTek, Inc. ..... Mimi Hart
MasterCard Europe Sprl ..... Mark Kamers
MasterCard Europe Sprl ..... Joshua Knopp
MasterCard Europe Sprl ..... Larry Newell
MasterCard Europe Sprl ..... Adam Sommer
MasterCard Europe Sprl ..... Michael Ward
National Institute of Standards and Technology (NIST) ..... Elaine Barker
National Institute of Standards and Technology (NIST) ..... Lily Chen
National Institute of Standards and Technology (NIST) ..... Paul Grassi
National Security Agency ..... Mike Boyle
National Security Agency ..... Paul Timmel
Nautilus Hyosung ..... Joe Militello
Nautilus Hyosung ..... Jay Shin
NCR Corporation ..... Tanika Eng
NCR Corporation ..... Charlie Harrow
NCR Corporation ..... David Norris
Onboard Security ..... Mark Etzel
Onboard Security ..... Virendra Kumar
Onboard Security ..... William Whyte
Onboard Security ..... Lee Wilson
Onboard Security ..... Zhenfei Zhang
PCI Security Standards Council ..... Leon Fell
PCI Security Standards Council ..... Troy Leach
PCI Security Standards Council ..... Ralph Poore
RSA, The Security Division of EMC ..... Steve Schmalz
SafeNet Infotech Pvt. Ltd. ..... Amit Sinha
Safeway ..... Gary Zempich
TECSEC Incorporated ..... Ed Scheidt
TECSEC Incorporated ..... Dr. Wai Tsang
TECSEC Incorporated ..... Jay Wack
Thales UK Limited ..... Larry Hines
Thales UK Limited ..... James Torjussen
The Clearing House ..... Mark Fitlin
The Clearing House ..... Sharon Jablon
The Clearing House ..... Hirak Patel
The Clearing House ..... Miguel Sanchez
Trustwave ..... John Amaral
Trustwave ..... Tim Hollebeek
U.S. Bank ..... Stephen Case

U.S. Bank ..... Peter Skirvin
Vantiv LLC ..... john hall
Vantiv LLC ..... Jeffrey Singleton
Vantiv LLC ..... Bill Weingart
Vantiv LLC ..... James Zerfas
VeriFone, Inc. ..... John Barrowman
VeriFone, Inc. ..... David Ezell
VeriFone, Inc. ..... Dave Faoro
VeriFone, Inc. ..... Doug Manchester
VeriFone, Inc. ..... Brad McGuinness
VeriFone, Inc. ..... Joachim Vance
VISA ..... Shahzad Khan
VISA ..... Kim Wagner
Wayne Fueling Systems ..... Steven Bowles
Wells Fargo Bank ..... William Felts, IV
Wells Fargo Bank ..... Phillip Griffin
Wells Fargo Bank ..... Jan Kohl
Wells Fargo Bank ..... Garrett Macey
Wells Fargo Bank ..... Kelly O'Donnell
Wells Fargo Bank ..... Mark Schaffer
Wells Fargo Bank ..... Jeff Stapleton
XYPRO Technology ..... Steve Tcherchian

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.)

At the time this standard was approved, the X9F4 Cryptographic Protocol and Application Security working group which developed this standard had the following active members:

Jeff Stapleton, X9F4 Chair
Sandra Lambert, X9F4 Vice Chair
Janet LaFrence, Project Manager
Phillip H. Griffin, Technical Editor

*Organization Represented* *Representative*

Bank of America ..... Amanda Adams
Bank of America ..... Peter Capraro
Bank of America ..... Andi Coleman
Bank of America ..... David Freeman
Bank of America ..... Lawrence LaBella
Bank of America ..... Daniel Welch
Member Emeritus ..... Bill Poletti
BlackBerry Limited ..... Daniel Brown

Bloomberg LP ..... Erik Anderson
Capital One ..... Johnny Lee
Cipherithm ..... Scott Spiker
comForte 21 GmbH ..... Henning Horst
Conexxus, Inc. ..... Alan Thiemann
Conexxus, Inc. ..... Linda Toth
Delap LLP ..... Andrea Beatty
Delap LLP ..... Darlene Kargel
Diebold Nixdorf ..... Christoph Bruecher
Diebold Nixdorf ..... Rick Brunt
Diebold Nixdorf ..... Andrea Carozzi
Diebold Nixdorf ..... Bruce Chapa
Diebold Nixdorf ..... Scott Harroff
Diebold Nixdorf ..... Anne Konecny
Diebold Nixdorf ..... Michael Nolte
Diebold Nixdorf ..... Michael Ott
Diebold Nixdorf ..... Dave Phister
Diebold Nixdorf ..... Matthias Runowski
Discover Financial Services ..... Cheryl Mish
Discover Financial Services ..... Diana Pauliks
Discover Financial Services ..... Lakshmi Ramanathan
Discover Financial Services ..... Jordan Schaefer
Discover Financial Services ..... Michelle Zhang
Federal Reserve Bank ..... Patrick Adler
Federal Reserve Bank ..... Guy Berg
Federal Reserve Bank ..... Marianne Crowe
Federal Reserve Bank ..... Pieralberto Deganello
Federal Reserve Bank ..... Amanda Dorphy
Federal Reserve Bank ..... Mary Hughes
Federal Reserve Bank ..... Heather Hultquist
Federal Reserve Bank ..... Janet LaFrence
Federal Reserve Bank ..... Paul Nunnally
Federal Reserve Bank ..... Susan Pandy
Federal Reserve Bank ..... Patti Ritter
Federal Reserve Bank ..... Daniel Rozycki
Federal Reserve Bank ..... Charles Tsai
First Data Corporation ..... Lisa Curry
First Data Corporation ..... Brian Kean
First Data Corporation ..... Brian Murray
First Data Corporation ..... Randall Rieth
FIS ..... Chelsea Lopez
FIS ..... Ian Lumsden
FIS ..... Sunny Wear
Fiserv ..... Dan Otten
FIX Protocol Ltd - FPL ..... Jim Northey
Member Emeritus ..... Gene Kathol
GEOBRIDGE Corporation ..... Donna Gem

GEOBRIDGE Corporation ..... Dean Macinskas
GEOBRIDGE Corporation ..... Jason Way
Gilbarco ..... Bruce Welch
Harland Clarke ..... John McCleary
Hewlett Packard ..... Terence Spies
IBM Corporation ..... Todd Arnold
Independent Community Bankers of America ..... Cary Whaley
ISARA Corporation ..... Mike Brown
ISARA Corporation ..... Alexander Truskovsky
ITS, Inc. (SHAZAM Networks) ..... Manish Nathwani
J.P. Morgan Chase ..... Robin Doyle
J.P. Morgan Chase ..... Darryl Scott
K3DES LLC ..... Davi Ottenheimer
KPMG LLP ..... Mark Lundin
MagTek, Inc. ..... Mimi Hart
Mark Tiggas ..... Mark Tiggas
MasterCard Europe Sprl ..... Mark Kamers
Merchant Advisory Group ..... Brad Andrews
National Institute of Standards and Technology (NIST) ..... Elaine Barker
National Institute of Standards and Technology (NIST) ..... Lily Chen
National Institute of Standards and Technology (NIST) ..... Elaine Newton
National Institute of Standards and Technology (NIST) ..... Burak Sahin
National Security Agency ..... Greg Gilbert
National Security Agency ..... Tim Havighurst
National Security Agency ..... Paul Timmel
NCR Corporation ..... Charlie Harrow
NCR Corporation ..... Brian Wotherspoon
Onboard Security ..... Mark Etzel
Onboard Security ..... Jeff Hoffstein
Onboard Security ..... William Whyte
PCI Security Standards Council ..... Leon Fell
PCI Security Standards Council ..... Troy Leach
PCI Security Standards Council ..... Ralph Poore
PCI Security Standards Council ..... Elizabeth Terry
Member Emeritus ..... Richard Sweeney
RSA, The Security Division of EMC ..... Steve Schmalz
SafeNet Infotech Pvt. Ltd ..... Amit Sinha
TECSEC Incorporated ..... Ed Scheidt
TECSEC Incorporated ..... Dr. Wai Tsang
TECSEC Incorporated ..... Jay Wack
Thales UK Limited ..... Colette Broadway
Thales UK Limited ..... Larry Hines
Thales UK Limited ..... James Torjussen
The Clearing House ..... Ken Friedman
The Clearing House ..... Sharon Jablon
Trustwave ..... Tim Hollebeek
U.S. Bank ..... Stephen Case

U.S. Bank ..... Peter Skirvin
Vantiv LLC ..... John Hall
VeriFone, Inc. ..... David Ezell
VeriFone, Inc. ..... Dave Faoro
VeriFone, Inc. ..... LeAnn Hostetler
VeriFone, Inc. ..... Doug Manchester
VeriFone, Inc. ..... Joachim Vance
VISA ..... Geoff Brookman
VISA ..... Hap Huynh
VISA ..... Shahzad Khan
VISA ..... Chackan Lai
VISA ..... Johan Van Tilburg
VISA ..... Kim Wagner
Wells Fargo Bank ..... Sotos Barkas
Wells Fargo Bank ..... Tony Bautts
Wells Fargo Bank ..... William Felts, IV
Wells Fargo Bank ..... Phillip Griffin
Wells Fargo Bank ..... Sam Grosby
Wells Fargo Bank ..... Jeff Jacoby
Wells Fargo Bank ..... Joseph Kaluzny
Wells Fargo Bank ..... Brian Keltner
Wells Fargo Bank ..... Jan Kohl
Wells Fargo Bank ..... Eric Lengvenis
Wells Fargo Bank ..... Doug Pelton
Wells Fargo Bank ..... Mike Rudolph
Wells Fargo Bank ..... Jeff Stapleton
Wells Fargo Bank ..... Tony Stieber
Wells Fargo Bank ..... Nathan Suri

This document cancels and replaces previous versions of X9.73.

# Cryptographic Message Syntax - ASN.1 and XML

## 1 Scope

This standard specifies a cryptographic syntax scheme that can be used to protect financial transactions, files and other messages from unauthorized disclosure and modification. The cryptographic syntax scheme is based on an abstract Cryptographic Message Syntax (CMS) schema whose concrete values can be represented using either a compact, efficient, binary encoding, or as a flexible, human-readable, XML markup format. The syntax scheme has the following characteristics:

1) Protected messages are represented as XML markup using the Canonical XML Encoding Rules (cXER), or represented in a binary format that is backward compatible with existing deployed systems. These systems rely on cryptographic message syntax, using the Basic Encoding Rules (BER) or the canonical subset of BER, the Distinguished Encoding Rules (DER).

2) 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) or Society for Worldwide Interbank Financial Telecommunication (SWIFT).

3) Standard attributes are defined using an extensible design to allow any organization with a need to define additional attributes for any purpose. Attributes are defined that allow Security Assertion Markup Language (SAML) and Extensible Markup Language (XML) Key Management Specification (XKMS) content to be carried in each of the cryptographic types defined in X9.73.

4) The syntax is cryptographic algorithm independent and extensible. It supports provision of data confidentiality using encryption and tokenization techniques, data integrity, data origin authentication, and non-repudiation services. Any algorithm may be used for message encryption, digital signature, signcryption, MAC, and key management. A variety of key management techniques are supported, including key exchange, key agreement, password-based encryption and constructive key management.

5) Selective field protection can be provided in two ways. First, they can be protected by combining multiple instances of this syntax into a composite message. Second, they can be protected in a single message by using identifier and markup tag names and content specific manifests that are cryptographically bound to content to select message components. This approach allows reusable message components to be moved between documents without affecting the validity of the signature.

6) Precise message encoding and detailed cryptographic processing requirements of binary and XML markup message representations are provided.

Simple Object Application Protocol (SOAP) message extensions are defined for each of the cryptographic types defined in X9.73 to enable protection of financial services information in Web Services environments.