This is a preview of "ANSI X9.73-2010 (R20...". Click here to purchase the full version from the ANSI store.

American National Standard for Financial Services

ANSI X9.73-2010 (R2017)

Cryptographic Message Syntax — ASN.1 and XML

Accredited Standards Committee X9, Incorporated
Financial Industry Standards

Date Approved: April 22, 2010

Date Reaffirmed: March 4, 2017

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., 275 West Street, Suite 107, Annapolis, MD 21401.

This is a preview of "ANSI X9.73-2010 (R20...". Click here to purchase the full version from the ANSI store.

This page left intentionally blank

This is a preview of "ANSI X9.73-2010 (R20...". Click here to purchase the full version from the ANSI store.

Contents

Page

© ASC X9, Inc. 2017 – All rights reserved

This is a preview of "ANSI X9.73-2010 (R20...". Click here to purchase the full version from the ANSI store.

© ASC X9, Inc. 2017 – All rights reserved

This is a preview of "ANSI X9.73-2010 (R20...". Click here to purchase the full version from the ANSI store.

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

Copyright © 2017 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.

This is a preview of "ANSI X9.73-2010 (R20...". Click here to purchase the full version from the ANSI store.

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. And 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 which 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.

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 Chairman
Vincent DeSantis, X9 Vice-Chairman
Steve Stevens, Executive Director
Janet Busch, Program Manager

© ASC X9, Inc. 2017 – All rights reserved

This is a preview of "ANSI X9.73-2010 (R20...". Click here to purchase the full version from the ANSI store.

Organization Represented	*Representative*
ACI Worldwide	Doug Grote
ACI Worldwide	Cindy Rink
American Bankers Association	Tom Judd
American Bankers Association	Diane C. Poole
American Express Company	Ted Peirce
Apriva	Len Sutton
Bank of America	Andi Coleman
Bank of America	Daniel Welch
Certicom Corporation	Daniel Brown
Citigroup, Inc.	Mark Clancy
Citigroup, Inc.	Michael Knorr
Citigroup, Inc.	Karla McKenna
Citigroup, Inc.	Chii-Ren Tsai
Citigroup, Inc.	Gary Word
CUSIP Service Bureau	Gerard Faulkner
CUSIP Service Bureau	James Taylor
Deluxe Corporation	John FitzPatrick
Deluxe Corporation	Ralph Stolp
Diebold, Inc.	Anne Bayonnet
Diebold, Inc.	Bruce Chapa
Discover Financial Services	Dave Irwin
Discover Financial Services	Deana Morrow
Federal Reserve Bank	Deb Hjortland
Federal Reserve Bank	Claudia Swendseid
First Data Corporation	Todd Nuzum
First Data Corporation	Rick Van Luvender
Fiserv	Bud Beattie
Fiserv	Kevin Finn
Fiserv	Lori Hood
Fiserv	Dan Otten
Fiserv	Skip Smith
FIX Protocol Ltd	Jim Northey
FSTC, Financial Services Technology Consortium	Christine Nautiyal
FSTC, Financial Services Technology Consortium	Daniel Schutzer
FSTC, Financial Services Technology Consortium	Michael Versace
Harland Clarke	John McCleary
Hewlett Packard	Larry Hines
Hewlett Packard	Gary Lefkowitz
IBM Corporation	Todd Arnold
IFSA	Dexter Holt
IFSA	Dan Taylor
Ingenico	Alexandre Hellequin
Ingenico	Steve McKibben
Ingenico	John Spence
J.P. Morgan Chase & Co	Robert Blair
J.P. Morgan Chase & Co	Roy DeCicco
J.P. Morgan Chase & Co	Edward Koslow
J.P. Morgan Chase & Co	Jackie Pagan
J.P. Morgan Chase & Co	Charita Wamack
Key Innovations	Scott Spiker
Key Innovations	Paul Walters
KPMG LLP	Mark Lundin
MagTek, Inc.	Terry Benson

© ASC X9, Inc. 2017 – All rights reserved

This is a preview of "ANSI X9.73-2010 (R20...". Click here to purchase the full version from the ANSI store.

MagTek, Inc. ..... Jeff Duncan
MagTek, Inc. ..... Mimi Hart
MasterCard International ..... Mark Kamers
Merchant Advisory Group ..... Dodd Roberts
Metavante Image Solutions ..... Stephen Gibson-Saxty
NACHA The Electronic Payments Association ..... Nancy Grant
National Association of Convenience Stores ..... Michael Davis
National Association of Convenience Stores ..... Alan Thiemann
National Security Agency ..... Paul Timmel
NCR Corporation ..... David Norris
NCR Corporation ..... Steve Stevens
RMG-SWIFT ..... Jamie Shay
RouteOne ..... Mark Leonard
SWIFT/Pan Americas ..... Jean-Marie Eloy
SWIFT/Pan Americas ..... James Wills
The Clearing House ..... Vincent DeSantis
U.S. Bank ..... Brian Fickling
U.S. Bank ..... Gregg Walker
University Bank ..... Stephen Ranzini
University Bank ..... Michael Talley
VeriFone, Inc. ..... David Ezell
VeriFone, Inc. ..... Dave Faoro
VeriFone, Inc. ..... Allison Holland
VeriFone, Inc. ..... Doug Manchester
VeriFone, Inc. ..... Brad McGuinness
VeriFone, Inc. ..... Brenda Watlington
VISA ..... Brian Hamilton
VISA ..... John Sheets
VISA ..... Richard Sweeney
Wells Fargo Bank ..... Andrew Garner
Wells Fargo Bank ..... Mike McCormick
Wells Fargo Bank ..... Mike Rudolph
Wells Fargo Bank ..... Mark Tiggas
Wincor Nixdorf Inc. ..... Ramesh Arunashalam
XBRL US, Inc. ..... Mark Bolgiano

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

Richard Sweeney, X9F Chair
Sandra Lambert, X9F Vice Chair

Organization Represented *Representative*

ACI Worldwide ..... Doug Grote
ACI Worldwide ..... Julie Samson
ACI Worldwide ..... Sid Sidner
American Bankers Association ..... Tom Judd
American Express Company ..... William J. Gray
American Express Company ..... Vicky Sammons
Bank of America ..... Dion Bellamy
Bank of America ..... Terrelle Carswell

 © ASC X9, Inc. 2017 – All rights reserved

This is a preview of "ANSI X9.73-2010 (R20...". Click here to purchase the full version from the ANSI store.

Bank of America ..... Andi Coleman
Bank of America ..... Todd Inskeep
Bank of America ..... John McGraw
Bank of America ..... Chris Schrick
Bank of America ..... Daniel Welch
Certicom Corporation ..... Daniel Brown
Certicom Corporation ..... John O. Goyo
Certicom Corporation ..... Sandra Lambert
Certicom Corporation ..... Scott Vanstone
Citigroup, Inc. ..... Mark Clancy
Citigroup, Inc. ..... Susan Rhodes
Citigroup, Inc. ..... Gary Word
Communications Security Establishment ..... Alan Poplove
Communications Security Establishment ..... Bridget Walshe
Cryptographic Assurance Services LLC ..... Ralph Poore
Cryptographic Assurance Services LLC ..... Jeff Stapleton
CUSIP Service Bureau ..... Scott Preiss
CUSIP Service Bureau ..... James Taylor
DeLap LLP ..... Steve Case
DeLap LLP ..... Darlene Kargel
Deluxe Corporation ..... John FitzPatrick
Deluxe Corporation ..... Ralph Stolp
Depository Trust and Clearing Corporation ..... Robert Palatnick
Diebold, Inc. ..... Anne Bayonnet
Diebold, Inc. ..... Bruce Chapa
Diebold, Inc. ..... Laura Drozda
Diebold, Inc. ..... Scott Harroff
Diebold, Inc. ..... Jessica Wapole
Discover Financial Services ..... Julie Shaw
Entrust, Inc. ..... Sharon Boeyen
Entrust, Inc. ..... Miles Smid
Federal Reserve Bank ..... Darin Contini
Federal Reserve Bank ..... Pieralberto Deganello
Federal Reserve Bank ..... Deb Hjortland
Federal Reserve Bank ..... Mike Ram
Ferris and Associates, Inc. ..... J. Martin Ferris
First Data Corporation ..... Lisa Curry
First Data Corporation ..... Lilik Kazaryan
First Data Corporation ..... Todd Nuzum
First Data Corporation ..... Scott Quinn
First Data Corporation ..... Andrea Stallings
First Data Corporation ..... Rick Van Luvender
Fiserv ..... Bud Beattie
Fiserv ..... Mary Bland
Fiserv ..... Kevin Finn
Fiserv ..... Dennis Freiburg
Fiserv ..... Dan Otten

© ASC X9, Inc. 2017 – All rights reserved

This is a preview of "ANSI X9.73-2010 (R20...". Click here to purchase the full version from the ANSI store.

FSTC, Financial Services Technology Consortium ..... Christine Nautiyal
FSTC, Financial Services Technology Consortium ..... Daniel Schutzer
FSTC, Financial Services Technology Consortium ..... Michael Versace
Futurex ..... Greg Schmid
GEOBRIDGE Corporation ..... Jason Way
Harland Clarke ..... Joseph Filer
Harland Clarke ..... John McCleary
Harland Clarke ..... John Petrie
Heartland Payment Systems ..... Roger Cody
Heartland Payment Systems ..... Glenda Preen
Hewlett Packard ..... Larry Hines
Hewlett Packard ..... Susan Langford
Hewlett Packard ..... Gary Lefkowitz
Hypercom ..... Mohammed Arif
Hypercom ..... Gary Zempich
IBM Corporation ..... Todd Arnold
IBM Corporation ..... Michael Kelly
IFSA ..... Dexter Holt
InfoGard Laboratories ..... Doug Biggs
InfoGard Laboratories ..... Ken Kolstad
Ingenico ..... Alexandre Hellequin
Ingenico ..... John Spence
J.P. Morgan Chase & Co ..... Robert Blair
J.P. Morgan Chase & Co ..... Edward Koslow
J.P. Morgan Chase & Co ..... Kathleen Krupa
J.P. Morgan Chase & Co ..... Donna Meagher
J.P. Morgan Chase & Co ..... Jackie Pagan
J.P. Morgan Chase & Co ..... Shawn Shifflett
Key Innovations ..... Scott Spiker
KPMG LLP ..... Mark Lundin
MagTek, Inc. ..... Terry Benson
MagTek, Inc. ..... Jeff Duncan
MagTek, Inc. ..... Mimi Hart
MasterCard International ..... Jeanne Moore
MasterCard International ..... Michael Ward
Merchant Advisory Group ..... Dodd Roberts
Metavante Image Solutions ..... Ron Schultz
National Institute of Standards and Technology ..... Elaine Barker
National Institute of Standards and Technology ..... Lawrence Bassham III
National Institute of Standards and Technology ..... William Burr
National Institute of Standards and Technology ..... Lily Chen
National Institute of Standards and Technology ..... David Cooper
National Institute of Standards and Technology ..... Morris Dworkin
National Institute of Standards and Technology ..... Randall Easter
National Institute of Standards and Technology ..... Sharon Keller
National Institute of Standards and Technology ..... John Kelsey
National Institute of Standards and Technology ..... Annabelle Lee

© ASC X9, Inc. 2017 – All rights reserved

This is a preview of "ANSI X9.73-2010 (R20...". Click here to purchase the full version from the ANSI store.

National Institute of Standards and Technology.....Fernando Podio
National Security Agency ..... Mike Boyle
National Security Agency ..... Greg Gilbert
National Security Agency .....Tim Havighurst
National Security Agency ..... Paul Timmel
National Security Agency ..... Debby Wallner
NCR Corporation .....Charlie Harrow
NCR Corporation ..... Ali Lowden
NCR Corporation ..... David Norris
NCR Corporation .....Ron Rogers
NCR Corporation .....Steve Stevens
NCR Corporation ..... Ally Whytock
NTRU Cryptosystems, Inc. .....Nick Howgrave-Graham
NTRU Cryptosystems, Inc. .....Ari Singer
NTRU Cryptosystems, Inc. ..... William Whyte
Pitney Bowes, Inc. .....Andrei Obrea
Pitney Bowes, Inc. .....Leon Pintsov
Pitney Bowes, Inc. .....Rick Ryan
Rosetta Technologies ..... Jim Maher
Rosetta Technologies .....Paul Malinowski
RSA, The Security Division of EMC ..... James Randall
RSA, The Security Division of EMC ..... Steve Schmalz
Surety, Inc.....Dimitrios Andivahis
Surety, Inc.....Tom Klaff
Thales e-Security, Inc..... Colette Broadway
Thales e-Security, Inc.....Jose Diaz
Thales e-Security, Inc.....Tim Fox
Thales e-Security, Inc.....James Torjussen
The Clearing House .....Vincent DeSantis
The Clearing House .....Henry Farrar
The Clearing House ..... Susan Long
U.S. Bank .....Glenn Marshall
U.S. Bank .....Peter Skirvin
U.S. Bank .....Robert Thomas
Unisys Corporation.....David J. Concannon
Unisys Corporation.....Navnit Shah
University Bank..... Stephen Ranzini
University Bank.....Michael Talley
VeriFone, Inc. .....John Barrowman
VeriFone, Inc. .....David Ezell
VeriFone, Inc. .....Dave Faoro
VeriFone, Inc. ..... Doug Manchester
VeriFone, Inc. .....Brad McGuinness
VeriFone, Inc. .....Brenda Watlington
VISA .....Leon Fell
VISA .....Tara Kissoon
VISA ..... Chackan Lai

© ASC X9, Inc. 2017 – All rights reserved

This is a preview of "ANSI X9.73-2010 (R20...". Click here to purchase the full version from the ANSI store.

VISA ..... Stoddard Lambertson
VISA ..... Chris McDaniel
VISA ..... John Sheets
VISA ..... Richard Sweeney
VISA ..... Johan (Hans) Van Tilburg
Voltage Security, Inc. ..... Luther Martin
Voltage Security, Inc. ..... Terence Spies
Wells Fargo Bank ..... Mick Bauer
Wells Fargo Bank ..... Jason Buck
Wells Fargo Bank ..... Andrew Garner
Wells Fargo Bank ..... Jeff Jacoby
Wells Fargo Bank ..... Brian Keltner
Wells Fargo Bank ..... Israel Laracuente
Wells Fargo Bank ..... Eric Lengvenis
Wells Fargo Bank ..... Mike McCormick
Wells Fargo Bank ..... David Naelon
Wells Fargo Bank ..... Doug Pelton
Wells Fargo Bank ..... Chuck Perry
Wells Fargo Bank ..... Keith Ross
Wells Fargo Bank ..... Mike Rudolph
Wells Fargo Bank ..... Ruven Schwartz
Wells Fargo Bank ..... Craig Shorter
Wells Fargo Bank ..... Tony Stieber
Wincor Nixdorf Inc ..... Ramesh Arunashalam
Wincor Nixdorf Inc ..... Saul Caprio
Wincor Nixdorf Inc ..... Joerg-Peter Dohrs
Wincor Nixdorf Inc ..... Matthias Runowski
Wincor Nixdorf Inc ..... Adam Sandoval
Wincor Nixdorf Inc ..... Michael Waechter

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
Phillip H. Griffin, X9.73 Editor

Organization Represented ..... *Representative*

Bank of America ..... Andi Coleman
Certicom Corporation ..... Sandra Lambert

© ASC X9, Inc. 2017 – All rights reserved

This is a preview of "ANSI X9.73-2010 (R20...". Click here to purchase the full version from the ANSI store.

Certicom Corporation.....Scott Vanstone
Cryptographic Assurance Services LLC.....Ralph Poore
Cryptographic Assurance Services LLC.....Jeff Stapleton
DeLap LLP.....Steve Case
DeLap LLP.....Darlene Kargel
Diebold, Inc.....Anne Bayonnet
Diebold, Inc.....Bruce Chapa
Diebold, Inc.....Scott Harroff
Diebold, Inc.....Jessica Wapole
Discover Financial Services.....Julie Shaw
Entrust, Inc.....Sharon Boeyen
Entrust, Inc.....Sheila Brand
Entrust, Inc.....Miles Smid
Ernst and Young.....Keith Sollers
Federal Reserve Bank.....Darin Contini
Federal Reserve Bank.....Pieralberto Deganello
Federal Reserve Bank.....Deb Hjortland
Federal Reserve Bank.....Mike Ram
First Data Corporation.....Lilik Kazaryan
First Data Corporation.....Brian Kean
First Data Corporation.....Todd Nuzum
Fiserv.....Dennis Freiburg
Fiserv.....Dan Otten
FSTC, Financial Services Technology Consortium.....Christine Nautiyal
FSTC, Financial Services Technology Consortium.....Michael Versace
Futurex.....Greg Schmid
GEOBRIDGE Corporation.....Jason Way
Harland Clarke.....John McCleary
Harland Clarke.....John Petrie
Hewlett Packard.....Larry Hines
Hypercom.....Mohammed Arif
Hypercom.....Gary Zempich
IBM Corporation.....Todd Arnold
IBM Corporation.....Phillip H. Griffin
IBM Corporation.....Michael Kelly
IFSA.....Dexter Holt
InfoGard Laboratories.....Doug Biggs
InfoGard Laboratories.....Ken Kolstad
Ingenico.....Alexandre Hellequin
Ingenico.....John Spence
J.P. Morgan Chase & Co.....Sean Croston
J.P. Morgan Chase & Co.....Leonid Vayner
KPMG LLP.....Mark Lundin
MagTek, Inc.....Terry Benson
Merchant Advisory Group.....Dodd Roberts
National Institute of Standards and Technology.....Elaine Barker
National Institute of Standards and Technology.....Lily Chen

© ASC X9, Inc. 2017 – All rights reserved

This is a preview of "ANSI X9.73-2010 (R20...". Click here to purchase the full version from the ANSI store.

National Security Agency ..... Greg Gilbert
National Security Agency ..... Tim Havighurst
National Security Agency ..... Paul Timmel
NCR Corporation ..... Charlie Harrow
NCR Corporation ..... Steve Stevens
NTRU Cryptosystems, Inc. ..... Ari Singer
NTRU Cryptosystems, Inc. ..... William Whyte
RSA, The Security Division of EMC ..... James Randall
Sun Microsystems PS ..... Joel Weise
Surety, Inc. ..... Dimitrios Andivahis
Thales e-Security, Inc. ..... Tim Fox
Thales e-Security, Inc. ..... James Torjussen
Transaction Network Services, Inc. ..... Kevin Gateman
Transaction Network Services, Inc. ..... Luc Saaka
Transaction Network Services, Inc. ..... Travis Lee
U.S. Bank ..... Peter Skirvin
U.S. Bank ..... Rush Wilson
Unisys Corporation ..... David J. Concannon
University Bank ..... Stephen Ranzini
University Bank ..... Michael Talley
VeriFone, Inc. ..... Dave Faoro
VeriFone, Inc. ..... Doug Manchester
VISA ..... Leon Fell
VISA ..... Tara Kissoon
VISA ..... Chackan Lai
VISA ..... Chris McDaniel
VISA ..... Richard Sweeney
VISA ..... Johan (Hans) Van Tilburg
Voltage Security, Inc. ..... Luther Martin
Wells Fargo Bank ..... Mick Bauer
Wells Fargo Bank ..... Jeff Jacoby
Wells Fargo Bank ..... Brian Keltner
Wells Fargo Bank ..... Eric Lengvenis
Wells Fargo Bank ..... Mike McCormick
Wells Fargo Bank ..... David Naelon
Wells Fargo Bank ..... Doug Pelton
Wells Fargo Bank ..... Mike Rudolph
Wells Fargo Bank ..... Ruven Schwartz
Wincor Nixdorf Inc ..... Matthias Runowski

This document cancels and replaces previous versions of X9,73 and X9.96 in whole.

This document merges together into a single national standard previous versions of the X9,73 and X9.96 standards, and provides a common, abstract, cryptographic messaging schema that supports both a compact binary and a verbose textual format of its messages.

© ASC X9, Inc. 2017 – All rights reserved

This is a preview of "ANSI X9.73-2010 (R20...". Click here to purchase the full version from the ANSI store.

Cryptographic Message Syntax - ASN.1 and XML

1 Scope

This Standard specifies a cryptographic syntax scheme which 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 that 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 realtime 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, data integrity, data origin authentication, and non-repudiation services. Any algorithm may be used for message encryption, digital signature, 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 by combining multiple instances of this syntax into a composite message. And second by using identifier and type markup tag names to select message components to be protected in a single message. 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.

2 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.

© ASC X9, Inc. 2017 – All rights reserved