American National Standard for Financial Services

ANSI X9.95-2016

Trusted Time Stamp Management and Security

Developed by
Accredited Standards Committee X9, Incorporated
Financial Industry Standards

Date Approved: December 16, 2016

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CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time.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

Accredited Standards Committee X9, Incorporated
Financial Industry Standards
275 West Street, Suite 107
Annapolis, MD 21401
http://x9.org/

Contents

Page

Figures

Tables

Flows

Introduction

As financial institutions increasingly conduct more business electronically, it is correspondingly becoming more important to ensure that there is a secure, standardize methodology to prove what and when digital data was created, transmitted, received, modified or stored. The duality of proving the “what” and the “when” necessitates that the methodology provides the ability to verify the integrity of the digital data and the time of the digital event. Such a time stamp must therefore be issued from a trustworthy authority, whose time originates from a trustworthy source, and whose time stamp is irrefutably verifiable. Such a methodology is applicable for financial institutions, their business partners, retailers and third party financial service providers.

There are numerous examples of financial applications where an electronic message (e.g., stock transaction, money transfers, document filing, clearing and settlement transaction) needs a time stamp that cannot be undetectably tampered with and offers an evidentiary trail of authenticity.

It is likewise essential from the standpoint of legal sufficiency, to provide the non- refutable time when a financial transaction has been digitally signed, that is there must be proof that the time of the digital signature is in fact the actual time when the document was signed.

This American National Standard defines the requirements to securely operate a Time Stamp Authority that issues time stamp tokens, provides recommendations to other Time Stamp Entities to manage time stamp tokens, describes time stamp token techniques, and offers a comprehensive set of control objectives and evaluation criteria to assess Time Stamp Entities that is suitable for use by a professional audit practitioner.

However, this Standard does not guarantee that a particular implementation is secure. It is the responsibility of the financial institution or integrator to put an overall process in place with the necessary controls to ensure that the process is securely implemented. Furthermore, the controls should include the application of appropriate audit tests in order to verify compliance with this Standard.

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 Accredited Standards Committee X9 Incorporated, 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
Claudia Swendseid, X9 Vice Chairman
Steve Stevens, Executive Director
Janet Busch, Program Manager

Organization Represented	*Representative*
ACI Worldwide	Doug Grote
ACI Worldwide	Dan Kinney
American Bankers Association	Diane Poole
American Express Company	David Moore
Bank of America	Daniel Welch
Bank of New York Mellon	Bryan Kirkpatrick
BlackBerry Limited	Daniel Brown
Blackhawk Network	Anthony Redondo
Bloomberg LP	Corby Dear
Capital One	Marie LaQuerre
Citigroup, Inc.	Karla McKenna
CLS Bank	Ram Komarraju
Conexxus, Inc.	Michael Davis
Conexxus, Inc.	Gray Taylor
Delap LLP	Darlene Kargel
Deluxe Corporation	Angela Hendershott
Diebold, Inc.	Bruce Chapa
Discover Financial Services	Michelle Zhang
eCurrency	David Wen
Federal Reserve Bank	Mary Hughes
Federal Reserve Bank	Janet LaFrence
Federal Reserve Bank	Claudia Swendseid
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	Susan Langford
IBM Corporation	Todd Arnold
Independent Community Bankers of America	Cary Whaley
Ingenico	Rob Martin
ISITC	Jason Brasile
J.P. Morgan Chase	Roy DeCicco
KPMG LLP	Mark Lundin
MagTek, Inc.	Roger Applewhite
MagTek, Inc.	Mimi Hart
MasterCard Europe Sprl	Mark Kamers
NACHA The Electronic Payments Association	Priscilla Holland
National Security Agency	Paul Timmel
NCR Corporation	David Norris
Office of Financial Research, U.S. Treasury Department	Justin Stekervetz
PCI Security Standards Council	Troy Leach
RouteOne	Chris Irving
RouteOne	Jenna Wolfe
State Street Corporation	Sharon Cournoyer

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 ..... Gary Zempich
VeriFone, Inc. ..... Dave Faoro
VISA ..... Kim Wagner
Wayne Fueling Systems ..... Steven Bowles
Wells Fargo Bank ..... Mark Schaffer

The X9F Subcommittee on Information Security had the following members:

Ed Scheidt, X9F Chairman
Sandra Lambert, X9F Vice Chairman

Organization Represented *Representative*

ACI Worldwide ..... Richard DuVall
ACI Worldwide ..... Doug Grote
ACI Worldwide ..... Dan Kinney
ACI Worldwide ..... Julie Samson
American Bankers Association ..... Tom Judd
American Express Company ..... David Armes
American Express Company ..... Eric Eldridge
American Express Company ..... William J. Gray
American Express Company ..... Farid Hatefi
American Express Company ..... Vicky Sammons
American Express Company ..... John Timar
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
BlackBerry Limited ..... Sandra Lambert
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 ..... David Buchanan
Delap LLP ..... Darlene Kargel
Deluxe Corporation ..... Angela Hendershott

Deluxe Corporation ..... Margiore Romay
Deluxe Corporation ..... Andy Vo
Diebold, Inc. ..... Bruce Chapa
Diebold, Inc. ..... Michael Ott
Diebold, Inc. ..... 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 ..... Cynthia Baxter
Federal Reserve Bank ..... Guy Berg
Federal Reserve Bank ..... Julia Cheney
Federal Reserve Bank ..... Marianne Crowe
Federal Reserve Bank ..... Sandeep Dhameja
Federal Reserve Bank ..... Amanda Dorphy
Federal Reserve Bank ..... Mary Hughes
Federal Reserve Bank ..... Heather Hultquist
Federal Reserve Bank ..... Janet LaFrence
Federal Reserve Bank ..... Jackie Nugent
Federal Reserve Bank ..... Jim O'Connell
Federal Reserve Bank ..... Susan Pandy
Federal Reserve Bank ..... Patti Ritter
Federal Reserve Bank ..... Daniel Rozycki
Federal Reserve Bank ..... Rick Sullivan
Federal Reserve Bank ..... Claudia Swendseid
First Data Corporation ..... Andrea Beatty
First Data Corporation ..... Lisa Curry
First National Bank of Omaha ..... Kristi White
Fiserv ..... Bud Beattie
Fiserv ..... Dan Otten
Futurex ..... Ryan Smith
GEOBRIDGE Corporation ..... Donna Gem
GEOBRIDGE Corporation ..... Jason Way
Gilbarco ..... Bruce Welch
Harland Clarke ..... Joseph Filer
Heartland Payment Systems ..... Scott Meeker
Hewlett Packard ..... Susan Langford
Hewlett Packard ..... Terence Spies
IBM Corporation ..... Todd Arnold
Independent Community Bankers of America ..... Cary Whaley
Ingenico ..... Rob Martin
ITS, Inc. (SHAZAM Networks) ..... Manish Nathwani
J.P. Morgan Chase ..... Bruce Geller
J.P. Morgan Chase ..... Kathleen Krupa
J.P. Morgan Chase ..... Jackie Pagán
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 Security Agency ..... Mike Boyle
National Security Agency ..... Paul Timmel
NCR Corporation ..... Charlie Harrow
NCR Corporation ..... David Norris
PCI Security Standards Council ..... Leon Fell
PCI Security Standards Council ..... Troy Leach
PCI Security Standards Council ..... Ralph Poore
Richard Sweeney ..... Richard Sweeney
RSA, The Security Division of EMC ..... Steve Schmalz
SafeNet, Inc. ..... Amit Sinha
Security Innovation ..... Mark Etzel
Security Innovation ..... William Whyte
Security Innovation ..... Lee Wilson
Security Innovation ..... Zhenfei Zhang
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 ..... Henry Farrar
Trustwave ..... John Amaral
Trustwave ..... Tim Hollebeek
U.S. Bank ..... Stephen Case
U.S. Bank ..... Peter Skirvin
Vantiv LLC ..... Dick Bloss
Vantiv LLC ..... Tom Humphrey
Vantiv LLC ..... Scott Mackelprang
Vantiv LLC ..... Bill Weingart
Vantiv LLC ..... Gary Zempich
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 ..... Mike McCormick
Wells Fargo Bank ..... Mark Schaffer
Wells Fargo Bank ..... Jeff Stapleton
Wincor Nixdorf Inc ..... Christoph Bruecher
Wincor Nixdorf Inc ..... Andrea Carozzi
Wincor Nixdorf Inc ..... Michael Nolte
XYPRO Technology ..... Steve Tcherchian

The X9F4 Working Group on Applications Security had the following members:

Jeff Stapleton, X9F4 Chair
Sandra Lambert, X9F4 Vice Chairman

Philip Griffin, X9F4 Vice Chairman
Dimitri Andivahis and Philip Griffin, Editor

Organization Represented	*Representative*
Bank of America	Andi Coleman
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
Bill Poletti	Bill Poletti
BlackBerry Limited	Daniel Brown
BlackBerry Limited	Sandra Lambert
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	Darlene Kargel
Diebold, Inc.	Rick Brunt
Diebold, Inc.	Bruce Chapa
Diebold, Inc.	Scott Harroff
Diebold, Inc.	Anne Konecny
Diebold, Inc.	Michael Ott
Diebold, Inc.	Dave Phister
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	Billy Boykin
Federal Reserve Bank	Jeremy Brotherton
Federal Reserve Bank	Marianne Crowe
Federal Reserve Bank	Pieralberto Deganello
Federal Reserve Bank	Sandeep Dhameja
Federal Reserve Bank	Amanda Dorphy
Federal Reserve Bank	Mary Hughes
Federal Reserve Bank	Heather Hultquist
Federal Reserve Bank	Janet LaFrence
Federal Reserve Bank	Joonho Lee
Federal Reserve Bank	Jackie Nugent
Federal Reserve Bank	Paul Nunnally
Federal Reserve Bank	Jim O'Connell
Federal Reserve Bank	Susan Pandy
Federal Reserve Bank	Michael Ram
Federal Reserve Bank	Patti Ritter
Federal Reserve Bank	Daniel Rozycki
Federal Reserve Bank	Rick Sullivan
Federal Reserve Bank	Claudia Swendseid
Federal Reserve Bank	Charles Tsai
Federal Reserve Bank	Adam Webb

First Data Corporation ..... Andrea Beatty
First Data Corporation ..... Lisa Curry
First Data Corporation ..... Brian Kean
First Data Corporation ..... Randall Rieth
Fiserv ..... Dan Otten
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
ITS, Inc. (SHAZAM Networks) ..... Manish Nathwani
J.P. Morgan Chase ..... Darryl Scott
K3DES LLC ..... Davi Ottenheimer
KPMG LLP ..... Mark Lundin
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 Security Agency ..... Greg Gilbert
National Security Agency ..... Tim Havighurst
National Security Agency ..... Paul Timmel
NCR Corporation ..... Charlie Harrow
NCR Corporation ..... Brian Wotherspoon
PCI Security Standards Council ..... Leon Fell
PCI Security Standards Council ..... Troy Leach
PCI Security Standards Council ..... Ralph Poore
PCI Security Standards Council ..... Elizabeth Terry
Richard Sweeney ..... Richard Sweeney
RSA, The Security Division of EMC ..... Steve Schmalz
SafeNet, Inc. ..... Amit Sinha
Security Innovation ..... Mark Etzel
Security Innovation ..... Jeff Hoffstein
Security Innovation ..... William Whyte
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 ..... Gary Zempich
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 ("Hans") Van Tilburg
VISA ..... Kim Wagner
VISA ..... Sue Zloth
Wells Fargo Bank ..... Sotos Barkas
Wells Fargo Bank ..... Tony Bautts
Wells Fargo Bank ..... David Duccini
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 ..... Mike McCormick
Wells Fargo Bank ..... David Naelon
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
Wincor Nixdorf Inc ..... Christoph Bruecher
Wincor Nixdorf Inc ..... Andrea Carozzi
Wincor Nixdorf Inc ..... Michael Nolte
Wincor Nixdorf Inc ..... Matthias Runowski

Trusted Time Stamp Management and Security for the Financial Services Industry

1 Scope

This standard specifies the minimum security requirements for the effective use of time stamps in a financial services environment. Within the scope of this Standard the following topics are addressed:

- Requirements for the secure management of the time stamp token across its life cycle, comprised of the generation, transmission and storage, validation, and renewal processes. The requirements in this Standard identify the means to securely and verifiably distribute time from a national time source down to the application level.
- Requirements for the secure management of a Time Stamp Authority (TSA)
- Requirements of a TSA to ensure that an independent third party can audit and validate the controls over the use of a time stamp process
- Techniques for the coding, encapsulation, transmission, storage, integrity and privacy protection of time stamp data
- Usage of time stamp technology

Items considered out of scope and not addressed in this Standard include the following:

- Requirements for a National Timing Authority imposed by the International Timing Authority
- Application specific requirements and limitations for employing time stamp technology
- The individual's privacy and ownership of time stamp data

Although this standard focuses on the financial services industry, it may be applied to other applications where the management and security of time stamps are necessary.

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.

ANS X9.19-1996 Financial Institution Retail Message Authentication

ANS X9.30-1997 Public Key Cryptography Using Irreversible Algorithms for the Financial Services Industry, Part 1: The Digital Signature Algorithm (DSA)

ANS X9.30-1997 Public Key Cryptography Using Irreversible Algorithms for the Financial Services Industry, Part 2: The Secure Hash Algorithm (SHA)

ANS X9.31-1998 Public Key Cryptography Using Reversible Algorithms for the Financial Services Industry: The RSA Signature Algorithm

2.1. ANS X9.62-2005 Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)