



# 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

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 X9.95-2016". [Click here to purchase the full version from the ANSI store.](#)

ANS X9.95-2016

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**CAUTION NOTICE:** This American National Standard may be revised or withdrawn at any time.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

Copyright © 2016 by Accredited Standards Committee X9, Incorporated

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. Printed in the United States of America

# Contents

Page

Foreword.....	i
Introduction .....	vi
1 Scope .....	1
2 Normative References .....	1
3 Terms and Definitions .....	2
4 Symbols and Abbreviated Terms .....	5
5 Time Stamp Framework .....	6
5.1 Time Stamp Architecture.....	6
5.2 Time Stamp Applications .....	7
5.3 Non-Repudiation Considerations Relating to Time Stamp Tokens .....	10
6 Trusted Time Stamp Requirements .....	11
6.1 General Requirements.....	11
6.2 Requirements for Time Source Entity (TSE) .....	11
6.3 Requirements for TSA .....	12
6.3.1 TSA TST Requirements .....	12
6.3.2 TSA Renewal Requirements .....	13
6.4 Requirements for TST Requestor.....	14
6.4.1 Requestor TST Requirements .....	14
6.4.2 Requestor Renewal Requirements.....	14
6.5 Requirements for TST Verifier .....	14
6.5.1 Verifier TST Requirements .....	14
6.5.2 Verifier Renewal Requirements .....	15
7 Time Stamp Objects .....	15
7.1 Time Calibration Report (TCR) .....	15
7.1.1 TCR Objects.....	15
7.1.2 TCR ASN.1 .....	16
7.1.3 TCR XML .....	17
7.2 Time Stamp Request.....	18
7.2.1 Time Stamp Request Object .....	18
7.2.2 Time Stamp Request ASN.1 .....	18
7.2.3 Time Stamp Request XML .....	19
7.3 Time Stamp Response.....	20
7.3.1 Time Stamp Response Object .....	20
7.3.2 Time Stamp Response ASN.1 .....	20
7.3.3 Time Stamp Response XML.....	22
7.4 Time Stamp Token .....	22
7.5 Time Stamp Info .....	23
7.5.1 Time Stamp Info Object.....	23
7.5.2 Time Stamp Info ASN.1.....	23
7.5.3 Time Stamp Info XML.....	25
7.6 Extensions .....	26
7.6.1 Hash Extension .....	26
7.6.2 Method Extension .....	26
7.6.3 Renewal Extension .....	26
7.7 Verification Request .....	27
7.7.1 Verification Request Object .....	27

ANS X9.95-2016

7.7.2	Verification Request ASN.1 .....	27
7.7.3	Verification Request XML .....	28
7.8	Verification Response .....	28
7.8.1	Verification Response Object .....	28
7.8.2	Verification Response ASN.1 .....	28
7.8.3	Verification Response XML .....	29
7.9	Extend Request .....	29
7.9.1	Extend Request Object .....	29
7.9.2	Extend Request ASN.1 .....	29
7.9.3	Extend Request XML .....	30
7.10	Extend Response .....	30
7.10.1	Extend Response Object .....	30
7.10.2	Extend Response ASN.1 .....	31
7.10.3	Extend Response XML .....	31
7.11	Logging .....	31
8	Time Stamp Methods .....	32
8.1	Digital Signature Method .....	32
8.1.1	General .....	32
8.1.2	Time Stamp Request .....	32
8.1.3	Time Stamp Token Generation .....	33
8.1.4	Time Stamp Token Verification .....	38
8.2	MAC Method .....	39
8.2.1	General .....	39
8.2.2	Time Stamp Token Request .....	39
8.2.3	Time Stamp Token Generation .....	39
8.2.4	Time Stamp Token Verification .....	42
8.3	Linked Token Method .....	42
8.3.1	General .....	42
8.3.2	Time Stamp Token Request .....	43
8.3.3	Time Stamp Token Generation .....	43
8.3.4	Time Stamp Token Verification .....	50
8.3.5	Time Stamp Token Extend Operation .....	51
8.4	Linked and Signed Method .....	52
8.4.1	General .....	52
8.4.2	Time Stamp Token Request .....	52
8.4.3	Time Stamp Token Generation .....	52
8.4.4	Time Stamp Token Verification .....	53
8.5	Transient Key Method .....	54
8.5.1	General .....	54
8.5.2	Time Stamp Request .....	56
8.5.3	Time Stamp Token Generation .....	56
8.5.4	Time Stamp Token Verification .....	62
9	Time Stamp Message Flows .....	63
9.1	General .....	63
9.2	Time Calibration Messages .....	63
9.3	Time Stamp Acquisition Messages .....	66
9.3.1	Time Stamp Token Request .....	66
9.3.2	Time Stamp Token Response .....	68
9.4	Time Stamp Verification Messages .....	69
9.4.1	Time Stamp Token Verification .....	69
9.4.2	Time Stamp Token Verification Request .....	69
9.4.3	Time Stamp Token Verification Response .....	70
Annex A:	(Normative) ASN.1 Modules .....	A-1
A.1	TrustedTimeStamp ASN.1 Module .....	A-1
A.2	TransientKey ASN.1 Module .....	A-9
Annex B:	(Normative) TS Control Objectives .....	B-1

B.1	Overview .....	B-1
B.2	Environmental Controls .....	B-2
B.2.1	Security Policy .....	B-2
B.2.2	Security Organization .....	B-4
B.2.3	Asset Classification and Management .....	B-5
B.2.4	Personnel Security.....	B-5
B.2.5	Physical and Environmental Security.....	B-6
B.2.6	Operations Management .....	B-8
B.2.7	System Access Management.....	B-10
B.2.8	Systems Development and Maintenance .....	B-12
B.2.9	Business Continuity Management .....	B-14
B.2.10	Monitoring and Compliance .....	B-15
B.2.11	Event Journaling.....	B-16
B.3	Key Management Controls.....	B-19
B.3.1	Key Generation.....	B-19
B.3.2	Key Storage, Backup and Recovery .....	B-20
B.3.3	Key Distribution .....	B-21
B.3.4	Key Usage.....	B-21
B.3.5	Key Destruction and Archival.....	B-22
B.3.6	Cryptographic Device Controls .....	B-23
B.4	Time Management Controls .....	B-25
B.4.1	Time Calibration .....	B-26
B.4.2	Time Stamp Token Request.....	B-26
B.4.3	Time Stamp Token Response .....	B-27
B.4.4	Time Stamp Token Handling.....	B-28
B.4.5	Time Stamp Token Verification .....	B-28
B.4.6	Time Stamp Token Extend Operation .....	B-29
Annex C:	(Informative) TS Policy and TS Practice Statement .....	C-1
C.1	Overview .....	C-1
C.2	Time Stamp Policy (TSP).....	C-1
C.2.1	Environmental Policies.....	C-1
C.2.2	Key Management Policies .....	C-3
C.2.3	Time Management Policies .....	C-4
C.3	Time Stamp Practice Statement (TSPS) .....	C-5
C.3.1	Environmental Practice Statements.....	C-5
C.3.2	Key Management Practice Statements .....	C-8
C.3.3	Time Management Practice Statements .....	C-11
Annex D:	(Informative) OASIS DSS TC Time Stamp Protocols .....	D-1
D.1	OASIS DSS TC Time Stamp Protocols.....	D-1
D.2	Time Stamp Request.....	D-1
D.3	Time Stamp Verify Protocol .....	D-2
D.4	OASIS DSS TC Time Stamp Token.....	D-2
D.4.1	XML <dss:TSTInfo> Structure .....	D-2
D.5	References .....	D-3
Annex E:	(Informative) Algorithms .....	E-1
E.1	Linear Chain Linking.....	E-1
E.2	Merkle Tree Aggregation .....	E-2
E.3	Publishing Algorithms.....	E-5
Bibliography	.....	1

## Figures

Figure 1 - Time Stamp Entities .....	7
Figure 2 - TST Request on Digital Data .....	8
Figure 3 - TST Response on Digital Data .....	8
Figure 4 - TST Request on Digital Signature .....	9
Figure 5 - TST Response on Digital Signature .....	9
Figure 6 - TST Request on Signed Digital Data .....	10
Figure 7 - TST Response on Signed Digital Data .....	10
Figure 8 - NIST Traceable Calibration .....	64
Figure 9 - Example of Linear Chain Linking .....	E-1
Figure 10 - Example of Merkle Tree Aggregation .....	E-3

## Tables

Table 1 - TSA Actions .....	67
Table 2 - Requestor Actions .....	68
Table 3 - Verification Service Provider Actions .....	70

## Flows

Flow 1 - Time Calibration Review .....	64
Flow 2 - Time Calibration Report .....	65
Flow 3 - Time Stamp Token Request .....	66
Flow 4 - Time Stamp Token Information Generation .....	67
Flow 5 - Time Stamp Token Response .....	68
Flow 6 - Time Stamp Token Verification Request .....	69
Flow 7 - Verify Request Validation .....	70
Flow 8 - Time Stamp Token Verification Response .....	71

## Introduction

As financial institutions increasingly conduct more business electronically, it is correspondingly becoming more important to ensure that there is a secure, standardized 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.



ANS X9.95-2016

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

<i>Organization Represented</i>	<i>Representative</i>
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 Komaraju
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

<i>Organization Represented</i>	<i>Representative</i>
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
Conexus, Inc. ....	Alan Thiemann
CUSIP Service Bureau.....	Scott Preiss
Delap LLP.....	David Buchanan
Delap LLP.....	Darlene Kargel
Deluxe Corporation.....	Angela Hendershott

ANS X9.95-2016

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

ANS X9.95-2016

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

<i>Organization Represented</i>	<i>Representative</i>
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
Conexus, Inc. ....	Alan Thiemann
Conexus, 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 Pandey
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

ANS X9.95-2016

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

This is a preview of "ANSI X9.95-2016". [Click here to purchase the full version from the ANSI store.](#)



# 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)