American National Standard for Financial Services

X9.117–2012

Secure Remote Access Mutual Authentication

Accredited Standards Committee X9, Incorporated
Financial Industry Standards

Date Approved: December 3, 2012

American National Standards Institute

Contents

Page

Figures

Tables

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CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time.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
P.O. Box 4035
Annapolis, MD 21403 USA
X9 Online http://www.x9.org

Introduction

Institutions and intermediaries are building infrastructures to provide new electronic financial transaction capabilities to consumers. As the volume of electronic financial transactions continues to grow it is imperative that advanced security techniques (technology and business process) for identifying and authenticating counter parties and services become part of the financial transaction process. Financial transaction systems incorporating advance security technology have requirements to ensure the identity and authenticity of customers and of the underlying financial services, in support of financial transactions conducted over communications networks.

The financial services industry relies on several time-honored methods of electronically identifying, authorizing, and authenticating entities and protect financial transactions. These methods include, but are not limited to: Personal Identification Numbers (PINs) and Message Authentication Codes (MACs) for retail and wholesale financial transactions, user IDs and passwords for network and computer access, and key management for network connectivity. Over the last forty years banks, investment, and insurance companies have developed risk management processes and policies to support the use of these technologies in financial applications.

The environment in which consumers and financial institutions conduct business has changed over the last several years. The Internet has become a channel that makes it convenient to conduct business. As this environment has changed, so have the associated threats. In particular, there have been threats such as phishing, pharming, spyware and other tools that have made it easy for someone to steal identities and conduct fraudulent transactions. It is also difficult for a consumer to verify that they are conducting business with a trusted party: are they in fact on their financial institution's website? Likewise, is the financial institution able to verify the consumer? Without this verification, and the sophistication of people and groups that are determined to steal information and financial assets, it is difficult to assure a consumer that they are logged onto the correct website, and likewise difficult for the institution to validate the person logging onto their website is who they claim to be. This changing environment has become a driver to adopt stronger methods of authentication.

The purpose of this standard is to create an authentication framework that can be adopted by both financial institutions and their customers that allows them to achieve a higher level of confidence they are communicating and transacting with the appropriate party. The overall intent of this standard and the framework is to enable a reduction of risk and exposure of both the financial institutions and their customers.

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, P.O. Box 4035, Annapolis, MD 21403 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.

The X9 committee had the following members:

Roy DeCicco, X9 Chairman
Claudia Swendseid, X9 Vice-Chairman
Cynthia Fuller, Executive Director
Janet Busch, Program Manager

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.	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
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

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

Ed Scheidt, 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
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 ..... Daniel Brown
Certicom ..... John O. Goyo
Certicom ..... Sandra Lambert
Certicom ..... Scott Vanstone
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
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
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
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
Mike Rudolph, Jeff Stapleton, Mick Talley, X9.117 Editors

Organization Represented — *Representative*

Bank of America ..... Andi Coleman
Certicom ..... Sandra Lambert
Certicom ..... Scott Vanstone
Comet Capital ..... Lawrence Levine
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 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
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 standard supersedes the previous ANS X9.49-1998 Secure Remote Access to Financial Services. Changes in this standard include the following:

X9.117–2012 Secure Remote Access – Mutual Authentication

1 Scope

This standard defines a taxonomy, requirements, operating principles, controls objectives, techniques, and technical approaches to enable financial institutions (FI) to support secure remote access.

Topics considered within the scope of this standard include the following:

- Risk management
- Mutual authentication between two entities, i.e., an end user and a financial services application, performing a financial transaction

- End user multi-factor and multi-channel authentication
- End user interface devices, e.g., browser and other computer applications, cell phones, USB fobs, and RFID
- Financial services applications, e.g., Internet / home banking, loan applications, insurance, bill presentment, and bill payment, account to account funds transfer, brokerage
- Financial services applications operated by any financial institution, agent, affiliate and service providers
- Authentication assurance value for various authentication mechanisms
- Layered security approach – Security approach that requires a criminal to penetrate or overcome a series of security layers before reaching a target, where a layer can refer to different techniques, different points in the technology stack, or at different steps in the business process.

Topics considered out of scope of this standard include the following:

- Identity provisioning and management.
- Federation and user system provisioning.
- Physical security.
- ATM, POS, kiosks, and Bluetooth enabled devices
- Risk assessment methods
- Transactions mediated by a human, such as a customer service agent

Assumptions applicable to this standard include the following:

- Financial institutions are capable of performing a risk assessment and can select a solution based on the associated risk.
- Mutual authentication will be used to support financial transactions.
- Multi-factor authentication will be used to support financial transactions based on risk.
- Remote access may occur from any endpoint such as home PCs, laptops and cell phones. These endpoints may be trusted or not (i.e., untrusted).
- There is a relationship with the financial institution and their customers such that all provisioning of identifiers and authenticators will be managed according to each institution's security policies.
- The appropriate security controls for mutual authentication, integrity, confidentiality and privacy for an application service will be determined by the FI, or by the application service provider, and approved by the financial institution's appropriate management authority, for outsourced applications.
- The FI utilizes back-end controls in addition to authentication, to prevent fraud and safeguard customer information.

Organizations considering remote access to financial services should perform a business risk assessment and evaluate their needs against the authentication framework provided in this standard to determine their requirements. Organizations implementing remote access methods should evaluate solutions against the requirements provided in this standard to measure compliance. Organizations validating compliance should use the control objectives provided in this standard. Manufacturers or implementers of remote access solutions should provide or enable sufficient functionality to achieve compliance with this standard.