American National Standard for Financial Services

ANSI X9.122-2020
Secure Customer Authentication for Internet Payments

Accredited Standards Committee X9, Incorporated

Financial Industry Standards

Date Approved: January 24, 2020

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 USA, X9 Online http://www.x9.org.
Contents

1 SCOPE .......................................................................................................................... 1
2 NORMATIVE REFERENCES .......................................................................................... 2
3 TERMS AND DEFINITIONS ......................................................................................... 3
4 SYMBOLS AND ABBREVIATED TERMS ................................................................. 7
5 GENERAL REQUIREMENTS ......................................................................................... 8
  5.1 LOGICAL REQUIREMENTS ..................................................................................... 8
  5.2 PHYSICAL REQUIREMENTS .................................................................................. 10
6 PIN ................................................................................................................................. 11
7 PASSCODE .................................................................................................................... 11
  7.1 GRAPHICAL PASSCODE ENTRY METHOD .......................................................... 12
  7.2 IVR PASSCODE ENTRY ........................................................................................ 13
8 STATIC PASSWORD ....................................................................................................... 13
  8.1 INTRODUCTION ..................................................................................................... 13
  8.2 STRONG PASSWORDS ............................................................................................ 13
  8.3 MINIMUM PASSWORD POLICIES ......................................................................... 13
9 DYNAMIC PASSWORD ................................................................................................. 15
  9.1 INTRODUCTION ..................................................................................................... 15
  9.2 ONE-TIME PASSWORD .......................................................................................... 15
    9.2.1 OTP Lifecycle Operations ............................................................................... 15
    9.2.2 Client-side requirements: .............................................................................. 15
    9.2.3 Server-side requirements: ............................................................................. 16
10 BIOMETRICS ............................................................................................................... 16
11 PHYSICALLY UNCLONABLE FUNCTION (PUF) ....................................................... 17
  11.1 INTRODUCTION .................................................................................................... 17
  11.2 DYNAMIC AUTHENTICATION VALUE ............................................................. 17
  11.3 AUTHENTICATION METHOD .............................................................................. 17
  11.4 READER ................................................................................................................ 17
  11.5 ENCRYPTION ........................................................................................................ 18
  11.6 CHALLENGE/RESPONSE ..................................................................................... 18
  11.7 CLIENT-SIDE REQUIREMENTS .......................................................................... 18
  11.8 SERVER-SIDE REQUIREMENTS .......................................................................... 18
12 AUTHENTICATION TECHNIQUES USING CRYPTOGRAPHY .................................... 18
  12.1 INTRODUCTION .................................................................................................... 18
  12.2 MECHANISMS USING SYMMETRIC ENCRYPTION ALGORITHMS ..................... 19
  12.3 MECHANISMS USING DIGITAL SIGNATURE TECHNIQUES ............................... 19
  12.4 MECHANISMS USING A CRYPTOGRAPHIC CHECK FUNCTION ....................... 20
  12.5 IDENTITY BASED ENCRYPTION ......................................................................... 20

BIBLIOGRAPHY .............................................................................................................. 21
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 © 2020 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.
Introduction

Customer demand and industry trends are moving towards transactions on the Internet. In order to keep up with the demand and trend, financial institutions must take advantage of this opportunity to strategically advance products and services so that “alternative” methods of payment are working in their favor.

Financial institutions must offer dynamic payment solutions that make use of existing infrastructure to service customer needs in a manner that is compatible with other constituents in the ecosystem such as merchants, mobile carriers, and payment networks.

Methods of payment that customers deem to be unfamiliar and unsecure are likely to yield low transaction volume and negatively impact customer confidence in the integrity of the financial institution. These methods will add no value for the financial institution. Conversely, by providing secure Internet payment options with which customers are comfortable and confident, the payment stakeholders will strengthen their relationships with their customers.

Though industry trends have indicated a significant movement of customers from using credit cards to debit cards for payments in the physical point-of-sale (POS) environment, the same trend has not been fully realized for internet transactions due to customer concerns regarding security and the sharing of confidential card/account information.

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
Corby Dear, X9 Vice-Chairman
Steve Stevens, Executive Director
Janet Busch, Program Manager
Ambria Frazier, Program Manager

Organization Represented	Representative
ACI Worldwide .................................................................Doug Grote
Amazon...........................................................................Igor Kleyman
American Bankers Association.........................................Diane Poole
Bank of America ..............................................................Daniel Welch
BDO ................................................................................Tim Crawford
Bloomberg LP .....................................................................Corby Dear
Communications Security Establishment ...........................David Smith
Conexxus, Inc. .................................................................Gray Taylor
CUSIP Global Services .....................................................Gerard Faulkner
Delap LLP .........................................................................Andrea Beatty
Deluxe Corporation ..........................................................Andy Vo
Diebold Nixdorf ..................................................................Bruce Chapa
Digicert ............................................................................Dean Coclin
Dover Fueling Solutions ....................................................Henry Fieglein
At the time this standard was approved, the X9F subcommittee on Data and Information Security had the following members:

Dave Faoro, X9F Chair
Steve Bowles, X9F Vice Chair
Ed Scheidt, X9F Vice Chair

Organization Represented  Representative
ACI Worldwide .......................................................... Doug Grote
ACI Worldwide .......................................................... Dan Kinney
ACI Worldwide .......................................................... Julie Samson
American Bankers Association ...................................... Tom Judd
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
### ISO 8583-1:2020

<table>
<thead>
<tr>
<th>Organization Represented</th>
<th>Representative</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon</td>
<td>Igor Kleyman</td>
</tr>
<tr>
<td>Amazon</td>
<td>Rahul Prabhakar</td>
</tr>
<tr>
<td>American Express Company</td>
<td>Gail Chapman</td>
</tr>
<tr>
<td>Bank of America</td>
<td>Amanda Adams</td>
</tr>
<tr>
<td>Bank of America</td>
<td>Peter Capraro</td>
</tr>
<tr>
<td>Bank of America</td>
<td>Andi Coleman</td>
</tr>
<tr>
<td>Bank of America</td>
<td>Joel Kazin</td>
</tr>
<tr>
<td>Bank of America</td>
<td>Terry McKinney</td>
</tr>
<tr>
<td>Bank of America</td>
<td>David Mortman</td>
</tr>
<tr>
<td>Bank of America</td>
<td>Matt Sharp</td>
</tr>
<tr>
<td>Bank of America</td>
<td>Daniel Welch</td>
</tr>
<tr>
<td>BBVA Compass</td>
<td>Omar Jarrar</td>
</tr>
<tr>
<td>BDO</td>
<td>Tim Crawford</td>
</tr>
<tr>
<td>BlackBerry Limited</td>
<td>Daniel Brown</td>
</tr>
<tr>
<td>Bloomberg LP</td>
<td>Erik Anderson</td>
</tr>
<tr>
<td>Capital One</td>
<td>Johnny Lee</td>
</tr>
<tr>
<td>conforto AG</td>
<td>Henning Horst</td>
</tr>
<tr>
<td>Conexxus, Inc.</td>
<td>David Ezell</td>
</tr>
<tr>
<td>Conexxus, Inc.</td>
<td>Alan Thiemann</td>
</tr>
<tr>
<td>Conexxus, Inc.</td>
<td>Linda Toth</td>
</tr>
<tr>
<td>Delap LLP</td>
<td>Andrea Beatty</td>
</tr>
<tr>
<td>Delap LLP</td>
<td>Spencer Giles</td>
</tr>
<tr>
<td>Diebold Nixdorf</td>
<td>Christoph Bruecher</td>
</tr>
<tr>
<td>Diebold Nixdorf</td>
<td>Rick Brunt</td>
</tr>
<tr>
<td>Diebold Nixdorf</td>
<td>Andrea Carozzi</td>
</tr>
<tr>
<td>Diebold Nixdorf</td>
<td>Bruce Chapa</td>
</tr>
<tr>
<td>Diebold Nixdorf</td>
<td>Scott Harroff</td>
</tr>
<tr>
<td>Diebold Nixdorf</td>
<td>Anne Konecny</td>
</tr>
<tr>
<td>Diebold Nixdorf</td>
<td>Michael Nolte</td>
</tr>
<tr>
<td>Diebold Nixdorf</td>
<td>Michael Ott</td>
</tr>
<tr>
<td>Diebold Nixdorf</td>
<td>David Phister</td>
</tr>
<tr>
<td>Diebold Nixdorf</td>
<td>Matthias Runowski</td>
</tr>
<tr>
<td>Digicert</td>
<td>Tim Hollebeek</td>
</tr>
<tr>
<td>Digicert</td>
<td>Steve Medin</td>
</tr>
<tr>
<td>Discover Financial Services</td>
<td>Cheryl Mish</td>
</tr>
<tr>
<td>Discover Financial Services</td>
<td>Diana Pauliks</td>
</tr>
<tr>
<td>Discover Financial Services</td>
<td>Lakshmi Ramanathan</td>
</tr>
<tr>
<td>Discover Financial Services</td>
<td>Jordan Schaefer</td>
</tr>
<tr>
<td>Discover Financial Services</td>
<td>Jorge Vargas</td>
</tr>
<tr>
<td>Dover Fueling Solutions</td>
<td>Henry Fieglein</td>
</tr>
<tr>
<td>Federal Reserve Bank</td>
<td>Patrick Adler</td>
</tr>
<tr>
<td>Federal Reserve Bank</td>
<td>Guy Berg</td>
</tr>
<tr>
<td>Federal Reserve Bank</td>
<td>Marianne Crowe</td>
</tr>
<tr>
<td>Federal Reserve Bank</td>
<td>Pieralberto Deganello</td>
</tr>
<tr>
<td>Federal Reserve Bank</td>
<td>Amanda Dorphy</td>
</tr>
<tr>
<td>Federal Reserve Bank</td>
<td>Ken Han</td>
</tr>
<tr>
<td>Federal Reserve Bank</td>
<td>Ainsley Hargest</td>
</tr>
<tr>
<td>Federal Reserve Bank</td>
<td>Daniel Littman</td>
</tr>
<tr>
<td>Federal Reserve Bank</td>
<td>Daniel Maynard</td>
</tr>
<tr>
<td>Federal Reserve Bank</td>
<td>Paul Nunnally</td>
</tr>
</tbody>
</table>
Federal Reserve Bank
First Data Corporation
First Data Corporation
First Data Corporation
First Data Corporation
FIS
FIS
FIS
Fiserv
FIX Protocol Ltd - FPL
GEOBRIDGE Corporation
GEOBRIDGE Corporation
GEOBRIDGE Corporation
Gilbarco
IBM Corporation
IBM Corporation
Inmar
ISARA Corporation
ISARA Corporation
ITS, Inc. (SHAZAM Networks)
ITS, Inc. (SHAZAM Networks)
J.P. Morgan Chase
J.P. Morgan Chase
J.P. Morgan Chase
J.P. Morgan Chase
K3DES LLC
Level 10
MagTek, Inc.
MasterCard Europe Sprl
MasterCard Europe Sprl
MasterCard Europe Sprl
Member Emeritus
Member Emeritus
Member Emeritus
Member Emeritus
Member Emeritus
Member Emeritus
Member Emeritus
Member Emeritus
Member Emeritus
Member Emeritus
National Institute of Standards and Technology (NIST)
National Institute of Standards and Technology (NIST)
National Security Agency
National Security Agency
National Security Agency
NCR Corporation
NCR Corporation
NCR Corporation
PCI Security Standards Council
PCI Security Standards Council
Paul Timmel
Tim Havighurst
Vinayak Kagalkar
Brian Kean
Brian Murray
Allisa Walker
Saman Amighi
Ian Lumsden
Sunny Wear
Dan Otten
James Northey
Donna Gem
Dean Macinski
Jason Way
Bruce Welch
Todd Arnold
Richard Kisley
Steven Bowles
Poovannan Rathinam
Mike Brown
Philip Lafrance
Alexander Truskovsky
Janet LaFrence
Manish Nathwani
Roger Cowie
Robin Doyle
Clinton Jones
Jackie Pagán
Darryl Scott
Davi Ottenheimer
Allan Elder
Mimi Hart
Simon Dix
Leland Englebardt
Mark Kamers
Darlene Kargel
Gene Kathol
Lawrence LaBella
John McCleary
Mike McCormick
Bill Poletti
Richard Sweeney
Mark Tiggas
Elaine Barker
Lily Chen
Greg Gilbert
Tim Havighurst
Paul Timmel
Charlie Harrow
Bradford Loewy
Brian Wotherspoon
Leon Fell
Troy Leach
ANSI X9.122-2020

PCI Security Standards Council ........................................... John Markh
PCI Security Standards Council ........................................... Ralph Poore
PCI Security Standards Council ........................................... Randall Rieth
PCI Security Standards Council ........................................... Joel Weisz
PricewaterhouseCoopers LLP .............................................. Madison Horn
PricewaterhouseCoopers LLP .............................................. Michael Versace
PriVerify Corp ................................................................. Adam Glynn
SafeNet Infotech Pvt. Ltd ................................................... Amit Sinha
Silicon Valley Law Group .................................................. Stephen Wu
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
The Clearing House .......................................................... Miguel Sanchez
The Phoenix Group .......................................................... Candice Hoft
TokenEx ................................................................. Ulf Mattsson
U.S. Bank ............................................................................ Stephen Case
U.S. Bank ............................................................................ Steven Fenter
U.S. Bank ............................................................................ David Lord
U.S. Bank ............................................................................ Darin Pettis
University Bank ................................................................. Stephen Ranzini
University Bank ................................................................. Michael Talley
Utimaco Inc ................................................................. Susan Langford
Utimaco Inc ................................................................. Manish Upasani
VeriFone, Inc ................................................................. Dave Faoro
VeriFone, Inc ................................................................. LeAnn Hostetler
VeriFone, Inc ................................................................. Doug Manchester
VeriFone, Inc ................................................................. Saxon Noh
VeriFone, Inc ................................................................. Joachim Vance
VISA ................................................................................. Kristina Breen
VISA ................................................................................. Ben Choong
VISA ................................................................................. Adam Clark
VISA ................................................................................. Naga Vinod Duggirala
VISA ................................................................................... June Qiu
VISA ................................................................................. Marcelo Silva
VISA ................................................................................. Hans Van Tilburg
VISA ................................................................................... Kim Wagner
Wells Fargo Bank ............................................................. Rao Abhijit
Wells Fargo Bank ............................................................. Sotos Barkas
Wells Fargo Bank ............................................................. William Felts, IV
Wells Fargo Bank ............................................................. Matthew Greenwell
Wells Fargo Bank .............................................................. Sam Groisy
Wells Fargo Bank .............................................................. Jeff Jacoby
Wells Fargo Bank .............................................................. Amanda Judge
Wells Fargo Bank .............................................................. Joseph Kaluzny
Wells Fargo Bank .............................................................. Arun Kamath
Wells Fargo Bank .............................................................. Brian Keitner
Wells Fargo Bank .............................................................. Rameshchandra
Ketharaju
Wells Fargo Bank ............................................................ Jan Kohl
Wells Fargo Bank ............................................................. Eric Lengvenis

© ASC X9, Inc. 2020 –All rights reserved
Secure Customer Authentication for Internet Payments

1 Scope

The scope of this standard defines the requirements for secure customer authentication in order to support electronic payment transactions over multiple channels initiated through the interchange system (debit/credit network).

Electronic transactions for purposes of this document are confined to payment transactions only via Internet, mobile or voice channels.

There are two different types of authentication credential entry devices, “private” and “public”. A “private” access device is one that is under the direct control of the user, plus perhaps a small number of people known to and trusted by the user. An example of a “private” access device is a home personal computer. A “public” access device is one over which the user does not have such control, for example a personal computer in a public library. This standard specifies the minimum security requirements and means for managing the customer authentication credentials for electronic payment (e.g., debit card and credit card) transactions.

The Internet represents a ubiquitous but insecure channel for exchanging information with a high risk of intrusion, such as screen scraping, malware or spyware that can lead to fraud. Transactions requiring a certain level of security should maintain consistency across different originating points. Because of these risks it is highly recommended that two or more authentication factors be used in combination to provide sufficiently strong customer authentication for card payment transactions on the Internet.

Assumptions applicable to this standard include, but are not limited to, the following:

1. Financial institutions are capable of performing a risk assessment and can select a solution based on the associated risk;
2. Remote access may occur from any endpoint such as kiosks or home machines. These endpoints may be trusted or untrusted.
3. There is a relationship with the financial institution and their customers and all provisioning of identifiers and authenticators will be managed according to each institutions security policies.
4. Since absolute security is not practically achievable, it is not realistic to describe an authentication method as being an absolute “secure method”. With enough cost, effort, and skill, any security scheme can be compromised.
5. Furthermore, as technology continues to evolve, new techniques may be developed to attack a security scheme that was previously believed to be immune to feasible attack.

Topics considered out of scope of this document include, but are not limited to, the following:

- The techniques for performing a risk assessment
- Mutual authentication and multifactor authentication – refer to ANSI X9.117 [2.3]
- Personal Identification Number (PIN) used in financial services as one method of cardholder verification - refer to X9.8 [2.4].