



American National Standard for Financial Services

ANSI X9.119-2013

Retail Financial Services — Requirements for Protection of Sensitive Payment Card Data — Part 1: Using Encryption Methods



Accredited Standards Committee X9, Incorporated
Financial Industry Standards

Date Approved: 3/26/13

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 page left intentionally blank

| Contents | Page |
|---|-------------|
| Foreword | v |
| Introduction..... | vi |
| 1 Scope | 1 |
| 2 Normative references | 2 |
| 2.1 ANS INCITS 92-1981 (R2003) - Information Technology - Data Encryption Algorithm (DEA) | 2 |
| 2.2 ANS X9.24-1-2009 – Retail Financial Services Symmetric Key Management part 1: Using Symmetric Techniques | 2 |
| 2.3 ANS X9.24-2-2006 – Retail Financial Services Symmetric Key Management part 2: Using Asymmetric Techniques | 2 |
| 2.4 ANS X9.52-1998 - Triple Data Encryption Algorithm (TDEA) Modes of Operation | 2 |
| 2.5 ANS X9.65-2004 - Triple Data Encryption Algorithm (TDEA) Implementation | 2 |
| 2.6 ANS X9.82-1-2006 – Random Number Generation | 2 |
| 2.7 ANS X9.97-1-2009 - Financial Services – Secure Cryptographic Devices (Retail) – Part 1: Concepts, Requirements, and Evaluation Methods..... | 2 |
| 2.8 ANS X9.104 (all parts)-2004 –Financial Transaction Card Originated Messages | 2 |
| 2.9 ISO Technical Report 14742 Financial services — Recommendations on Cryptographic Algorithms and Their Use..... | 2 |
| 2.10 ISO/IEC 7813:2006 Information Technology – Identification cards – Financial transaction cards | 2 |
| 2.11 ISO/IEC 18033: Information Technology- Security techniques – Encryption algorithms Part 3: Block Ciphers..... | 2 |
| 3 Terms and definitions | 2 |
| 3.1 Acquirer | 2 |
| 3.2 Algorithm..... | 3 |
| 3.3 Authorization Transaction | 3 |
| 3.4 Ciphertext | 3 |
| 3.5 Cleartext | 3 |
| Data in original, unencrypted form..... | 3 |
| 3.6 Cryptographic Key A parameter that determines the operation of a cryptographic function such as: | 3 |
| 3.7 Data Encryption Algorithm (DEA) | 3 |
| 3.8 Data Encryption Standard (DES)..... | 3 |
| 3.9 Decryption | 3 |
| 3.10 Encryption | 3 |
| 3.11 Encryption Algorithm | 4 |
| 3.12 Format Preserving Encryption | 4 |
| 3.13 IC Card | 4 |
| 3.14 Infeasible A condition whereby a particular attack, although it may be technically possible, is not economically viable. E.g. the cost of the attack exceeds the economic benefit..... | 4 |
| 3.15 Institution | 4 |
| 3.16 Interchange | 4 |
| 3.17 Issuer | 4 |
| 3.18 Key | 4 |
| 3.19 Plaintext..... | 4 |
| 3.20 Point of Entry (POE) | 4 |

ANSI X9.119-2013

| | | |
|---------------------|--|----|
| 3.21 | Privacy | 4 |
| 3.22 | Protection | 5 |
| 3.23 | Secure Cryptographic Device (SCD) | 5 |
| 3.24 | Sensitive payment card data | 5 |
| 3.25 | Triple Data Encryption Algorithm (TDEA) | 5 |
| 3.26 | Transaction..... | 5 |
| 3.27 | Verification | 5 |
| 4 | Symbols and abbreviated terms | 5 |
| 5 | Sensitive Payment Card Data Elements | 6 |
| 6 | Sensitive Payment Card Data Protection Requirements | 6 |
| 6.1 | General..... | 6 |
| 6.2 | Data Element Specific Requirements | 7 |
| 6.2.1 | Cardholder Name | 7 |
| 6.2.2 | Primary Account Number (PAN) | 7 |
| 6.2.3 | Expiration Date..... | 8 |
| 6.2.4 | Service Code | 8 |
| 6.2.5 | Discretionary Data | 8 |
| 6.2.6 | Track Data..... | 9 |
| 6.2.7 | Manually Entered Security Validation Code | 9 |
| 6.2.8 | Matrix of Security Requirements and Recommendations for Protection of Sensitive Payment Card Data outside of an SCD and prior to the point of decryption | 10 |
| 6.3 | Requirements When Employing Encryption Methods to Protect Sensitive Payment Card Data | 11 |
| 6.3.1 | Data Encryption Algorithm and Key Strength Requirements | 11 |
| 6.3.2 | Data Encryption Key Management Security Requirements | 11 |
| 6.3.3 | Prevention of Dictionary Attacks | 11 |
| 6.3.4 | Distinguishing Protected Data from Cleartext Data When Employing Format Preserving Methods | 12 |
| Annex A (normative) | Acceptable Data Encryption Algorithms | 13 |
| A.1 | General..... | 13 |
| A.2 | Approved Algorithms | 13 |
| A.2.1 | TDEA | 13 |
| A.2.2 | AES..... | 13 |
| A.2.3 | RSAES using OAEP (Optimal Asymmetric Encryption Padding)..... | 13 |
| A.3 | Minimum Security Level..... | 13 |

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 © 2013 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.

ANSI X9.119-2013

Introduction

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:

X9 Chairman – Roy DeCicco
X9 Vice-Chairman – Claudia Swendseid
Executive Director- Cynthia Fuller

Organization Represented

ACI Worldwide
American Bankers Association
Bank of America
Bank of New York Mellon
BP Products North America
Certicom Corporation
Citigroup, Inc.
CLS Bank
CUSIP Service Bureau
Deluxe Corporation
Diebold, Inc.
Discover Financial Services
Federal Reserve Bank
First Data Corporation
FIS Global
Fiserv
FIX Protocol Ltd - FPL
Gilbarco
Harland Clarke
Hewlett Packard
IBM Corporation
Independent Community Bankers of America
Infinium Capital Management
Ingenico
ISITC
J.P. Morgan Chase
Key Innovations
KPMG LLP
MagTek, Inc.
MasterCard Europe Sprl
NACHA The Electronic Payments Association
National Security Agency
NCR Corporation

Representative

| | |
|----------|--------------|
| Doug | Grote |
| C. Diane | Poole |
| Daniel | Welch |
| David | Goldberg |
| Robert | Slimmer |
| Daniel | Brown |
| Karla | McKenna |
| Ram | Komaraju |
| James | Taylor |
| Angela | Hendershott |
| Bruce | Chapa |
| Michelle | Zhang |
| Claudia | Swendseid |
| Rick | Van Luvender |
| Stephen | Gibson-Saxty |
| Bud | Beattie |
| Jim | Northey |
| Bruce | Welch |
| John | McCleary |
| Larry | Hines |
| Todd | Arnold |
| Viveca | Ware |
| Gregory | Eickbush |
| John | Spence |
| Genevy | Dimitrion |
| Roy | DeCicco |
| Scott | Spiker |
| Mark | Lundin |
| Mimi | Hart |
| Mark | Kamers |
| Robert | Unger |
| Paul | Timmel |
| Steve | Stevens |

| | | |
|---|--------|--------------|
| Office of Financial Research, U.S. Treasury Department | Con | Crowley |
| Petroleum Convenience Alliance for Technology Standards (PCATS) | Gray | Taylor |
| RouteOne | Chris | Irving |
| SWIFT/Pan Americas | Frank | Vandriessche |
| Symcor Inc. | Brian | Salway |
| TECSEC Incorporated | Ed | Scheidt |
| The Clearing House | Sharon | Jablon |
| Unissant | Mark | Bolgiano |
| USDA Food and Nutrition Service | Kathy | Ottobre |
| Vantiv LLC | Patty | Walters |
| VeriFone, Inc. | Dave | Faoro |
| VerifyValid | Paul | Doyle |
| VISA | Kim | Wagner |
| Wells Fargo Bank | Mark | Tiggas |
| WEX | Russ | Lamer |

ANSI X9.119-2013

At the time this standard was approved, the X9F6 subcommittee on Cardholder Authentication and ICC's had the following members:

Scott Spiker, Chairman

Organization Represented

Acculynk
Acculynk
ACI Worldwide
ACI Worldwide
ACI Worldwide
ACI Worldwide
ACI Worldwide
American Bankers Association
Apriva
Bank of America
Bank of America
Bank of America
Bank of America
Bank of America
Bank of America
Bank of America
BP Products North America
Certicom Corporation
Certicom Corporation
Certicom Corporation
Certicom Corporation
Cirque Inc.
Citigroup, Inc.
Clearkey, Inc.
comForte 21 GmbH
comForte 21 GmbH
comForte 21 GmbH
CUSIP Service Bureau
CUSIP Service Bureau
DeLap LLP
DeLap LLP
DeLap LLP
Depository Trust and Clearing Corporation
Diebold, Inc.
Diebold, Inc.
Diebold, Inc.
Diebold, Inc.
Diebold, Inc.
Diebold, Inc.
Discover Financial Services
Discover Financial Services
Discover Financial Services
Discover Financial Services
Discover Financial Services
Dresser Wayne
Dresser Wayne
Dresser Wayne
Equinox Payments

Representative

John Herr
Philip Patrick
Charles Collins
Richard DuVall
Doug Grote
Dan Kinney
Julie Samson
Tom Judd
Len Sutton
Dion Bellamy
Peter Capraro
Terrelle Carswell
Andi Coleman
Chris Schrick
Jeff Stapleton
Daniel Welch
Robert Slimmer
Daniel Brown
Matt Campagna
John O. Goyo
Sandra Lambert
Keith Paulsen
Chii-Ren Tsai
Paul Reimer
Thomas Burg
Thomas Gloerfeld
Michael Horst
Scott Preiss
James Taylor
David Buchanan
Stephen Case
Darlene Kargel
Robert Palatnick
Rick Brunt
Bruce Chapa
Amanda Cummins
Scott Harroff
Anne Konecny
Michael Ott
David Kloser
Diana Pauliks
Julie Quandt
Jordan Schaefer
Michelle Zhang
Steven Bowles
Tom Chittenden
Tim Weston
Mohammad Arif

| | | |
|--|-------------|-------------|
| Equinox Payments | Alan | Fong |
| Federal Reserve Bank | Jeremy | Brotherton |
| Federal Reserve Bank | Julia | Cheney |
| Federal Reserve Bank | Pieralberto | Deganello |
| Federal Reserve Bank | Amanda | Dorphy |
| Federal Reserve Bank | Deb | Hjortland |
| Federal Reserve Bank | Mary | Hughes |
| Federal Reserve Bank | Bob | Hunt |
| Federal Reserve Bank | Kathleen | Jacob |
| Federal Reserve Bank | Joonho | Lee |
| Federal Reserve Bank | Dave | McDermitt |
| Federal Reserve Bank | Jim | O'Connell |
| Federal Reserve Bank | Mike | Ram |
| Federal Reserve Bank | John | Rhodes |
| Ferris and Associates, Inc. | J. Martin | Ferris |
| Ferris and Associates, Inc. | Lynda R. | Strickland |
| First Data Corporation | Andrea | Beatty |
| First Data Corporation | Lisa | Curry |
| First Data Corporation | Lilik | Kazaryan |
| First Data Corporation | Brian | Kean |
| First National Bank of Omaha | Kristi | White |
| FIS Global | Tami | Harris |
| Fiserv | Bud | Beattie |
| Fiserv | Mary | Bland |
| Fiserv | Dan | Otten |
| Futurex | Chris | Hamlett |
| Futurex | Jim | Lambert |
| Futurex | Ryan | Smith |
| GEOBRIDGE Corporation | Dean | Macinkas |
| GEOBRIDGE Corporation | Jason | Way |
| Gilbarco | Bruce | Welch |
| Harland Clarke | John | McCleary |
| Harland Clarke | John | Petrie |
| Heartland Payment Systems | Kevin | Halliburton |
| Heartland Payment Systems | Patricia | Hoskinson |
| Heartland Payment Systems | Scott | Meeker |
| Heartland Payment Systems | Robin | Trickel |
| Hewlett Packard | Larry | Hines |
| Hewlett Packard | Susan | Langford |
| IBM Corporation | Todd | Arnold |
| IBM Corporation | Michael | Kelly |
| Independent Community Bankers of America | Cary | Whaley |
| Ingenico | Steve | McKibben |
| Ingenico | John | Spence |
| ITS, Inc. (SHAZAM Networks) | Manish | Nathwani |
| J.P. Morgan Chase | Bruce | Geller |
| J.P. Morgan Chase | Edward | Koslow |
| J.P. Morgan Chase | Kathleen | Krupa |
| J.P. Morgan Chase | Donna | Meagher Gem |
| J.P. Morgan Chase | Jackie | Pagan |
| J.P. Morgan Chase | Thomas | Pageler |
| K3DES LLC | Azie | Amini |
| K3DES LLC | James | Richardson |
| Key Innovations | Scott | Spiker |
| KPMG LLP | Mark | Lundin |

ANSI X9.119-2013

| | | |
|---|-----------|-------------|
| MagTek, Inc. | Jeff | Duncan |
| MagTek, Inc. | Mimi | Hart |
| MagTek, Inc. | Larry | Meyers |
| Marriott International | Jude | Sylvestre |
| MasterCard Europe Sprl | Jeanne | Moore |
| MasterCard Europe Sprl | Susie | Thompson |
| MasterCard Europe Sprl | Michael | Ward |
| Mustang Microsystems, Inc. | Tami | Harris |
| 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 | Annabelle | Lee |
| National Institute of Standards and Technology | Fernando | Podio |
| National Security Agency | Paul | Timmel |
| NCR Corporation | Charlie | Harrow |
| NCR Corporation | Ali | Lowden |
| NCR Corporation | David | Norris |
| NCR Corporation | Ron | Rogers |
| NCR Corporation | Steve | Stevens |
| NCR Corporation | Ally | Whytock |
| PCI Security Standards Council | Leon | Fell |
| PCI Security Standards Council | Troy | Leach |
| PCI Security Standards Council | Ralph | Poore |
| Petroleum Convenience Alliance for Technology Standards (PCATS) | Ann | Seki |
| Petroleum Convenience Alliance for Technology Standards (PCATS) | Alan | Thiemann |
| Petroleum Convenience Alliance for Technology Standards (PCATS) | Linda | Toth |
| Rosetta Technologies | Jim | Maher |
| RSA, The Security Division of EMC | Steve | Schmalz |
| SafeNet, Inc. | Chris | Dunn |
| SafeNet, Inc. | Terry | Fletcher |
| SafeNet, Inc. | Skip | Norton |
| SafeNet, Inc. | Kuldeep | Saini |
| SafeNet, Inc. | Brett | Thompson |
| STAR | Lisa | Besack |
| STAR | Scott | Quinn |
| STAR | Robert | Ribble |
| Surety, Inc. | Dimitrios | Andivahis |
| Symcor Inc. | Brian | Salway |
| TECSEC Incorporated | Ed | Scheidt |
| TECSEC Incorporated | Dr. Wai | Tsang |
| TECSEC Incorporated | Jay | Wack |
| Thales e-Security, Inc. | Jose | Diaz |
| Thales e-Security, Inc. | Tim | Fox |
| Thales e-Security, Inc. | James | Torjussen |
| The Clearing House | Henry | Farrar |
| The Clearing House | Susan | Long |
| Trustwave | John | Amaral |
| Trustwave | Tim | Hollebeek |
| Trustwave | Patrick | McGregor |
| Trustwave | Alexander | Volyntkin |

| | | |
|---------------------------------|----------------|-------------|
| USDA Food and Nutrition Service | Kathy | Ottobre |
| Vantiv LLC | Dick | Bloss |
| Vantiv LLC | Tom | Humphrey |
| Vantiv LLC | Scott | Mackelprang |
| Vantiv LLC | Patty | Walters |
| Vantiv LLC | Bill | Weingart |
| Vantiv LLC | James | Zerfas |
| VeriFone, Inc. | John | Barrowman |
| VeriFone, Inc. | LeAnn | Brown |
| VeriFone, Inc. | David | Ezell |
| VeriFone, Inc. | Dave | Faoro |
| VeriFone, Inc. | Chris | Madden |
| VeriFone, Inc. | Doug | Manchester |
| VeriFone, Inc. | Brad | McGuinness |
| VeriFone, Inc. | Joachim | Vance |
| VeriFone, Inc. | Gary | Zempich |
| VerifyValid | Richard | Sweeney |
| VISA | Adam | Clark |
| VISA | Hap | Huynh |
| VISA | Chackan | Lai |
| VISA | Stoddard | Lambertson |
| VISA | John | Sheets |
| VISA | Michael | Stefanich |
| VISA | Johan ("Hans") | Van Tilburg |
| VISA | Kim | Wagner |
| Voltage Security, Inc. | Luther | Martin |
| Voltage Security, Inc. | Terence | Spies |
| Voltage Security, Inc. | Richard | Sweeney |
| Wells Fargo Bank | William | Felts, IV |
| Wells Fargo Bank | Andrew | Garner |
| Wells Fargo Bank | Jeff | Jacoby |
| Wells Fargo Bank | Brian | Keltner |
| Wells Fargo Bank | Eric | Lengvenis |
| Wells Fargo Bank | David | Naelon |
| Wells Fargo Bank | Brian | Parks |
| Wells Fargo Bank | Doug | Pelton |
| Wells Fargo Bank | Chuck | Perry |
| Wells Fargo Bank | Marv | Peterson |
| Wells Fargo Bank | Keith | Ross |
| Wells Fargo Bank | Mike | Rudolph |
| Wells Fargo Bank | Tony | Stieber |
| Wells Fargo Bank | Mark | Tiggas |
| Wincor Nixdorf Inc | Christoph | Bruecher |
| Wincor Nixdorf Inc | Andrea | Carozzi |
| Wincor Nixdorf Inc | Michael | Nolte |
| Wincor Nixdorf Inc | Matthias | Runowski |

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

ANSI X9.119-2013

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 X9F6-1 X9.119 Protection of Sensitive Payment Card Data working group which developed this standard had the following active members:

Scott Spiker, Chairman and Sarah McCrary, Project Editor

Organization Represented

Representative

Retail Financial Services — Requirements for Protection of Sensitive Payment Card Data — Part 1: Using Encryption Methods

1 Scope

This part of X9.119 defines minimum security requirements when employing encryption methods to protect sensitive payment card data. For the purpose of this standard “protection” refers to maintaining the secrecy of the data from unauthorized disclosure. It applies to protection of the data from the point of encryption to the point of decryption, wherever those points may be in a given system.

Additional parts may be created to address alternative methods for protecting sensitive payment card data.

The following are outside the scope of the standard:

- Methods of cardholder authentication, such as Personal Identification Number (PIN)
- Physical or logical security requirements for protecting the sensitive payment card data at the point of entry prior to entering a Secure Cryptographic Device (SCD).