# American National Standard for Financial Services

# ANSI X9.63–2011 (R2017)

# Public Key Cryptography for the Financial Services Industry

# Key Agreement and Key Transport Using Elliptic Curve Cryptography

Developed by
Accredited Standards Committee X9, Incorporated
Financial Industry Standards

**Date Approved: December 21, 2011**

**Date Reaffirmed: February 10, 2017**

American National Standards Institute

## Foreword

Business practice has changed with the introduction of computer-based technologies. The substitution of electronic transactions for their paper-based predecessors has reduced costs and improved efficiency. Trillions of dollars in funds and securities are transferred daily by telephone, wire services, and other electronic communication mechanisms. The high value or sheer volume of such transactions within an open environment exposes the financial community and its customers to potentially severe risks from the accidental or deliberate disclosure, alteration, substitution, or destruction of data. These risks are compounded by interconnected networks, and the increased number and sophistication of malicious adversaries. Electronically communicated data may be secured through the use of symmetrically keyed encryption algorithms (e.g. FIPS, AES) in combination with public-key cryptography-based key management techniques.

This standard, X9.63-2011, *Public Key Cryptography For The Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography*, defines a suite of mechanisms designed to facilitate the secure establishment of cryptographic data for the keying of symmetrically keyed algorithms (e.g. TDEA, AES). These mechanisms are based on the elliptic curve analogue of the Diffie-Hellman key agreement mechanism. Because the mechanisms are based on the same fundamental mathematics as the Elliptic Curve Digital Signature Algorithm (ECDSA) (ANS X9.62), additional efficiencies and functionality may be obtained by combining these and other cryptographic techniques.

While the techniques specified in this standard are designed to facilitate key management applications, the standard does not guarantee that a particular implementation is secure. It is the responsibility of the financial institution 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.

The user's attention is called to the possibility that compliance with this standard may require the use of an invention covered by patent rights. By publication of this standard, no position is taken with respect to the validity of potential claims or of any patent rights in connection therewith. The patent holders have, 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 X9 Secretariat,

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 that this standard was approved, the X9 committee had the following chairs and administrators:

Roy DeCicco, Group Chair, J. P. Morgan Chase
Claudia Swendseid, Vice Chair, Federal Reserve Bank
Steve Stevens, Executive Director, Accredited Standards Committee X9, Inc.
Isabel Bailey, Administrator, Accredited Standards Committee X9, Inc.
Janet Busch, Administrator, Accredited Standards Committee X9, Inc.

The X9 committee had the following member organizations, with primary representatives:

| X9 Member Organization | Representative |
|---|---|
| ACI Worldwide | Doug Grote |
| Advance Auto Parts | Anthony Johnson |
| American Bankers Association | C. Diane Poole |
| American Express Company | Ted Peirce |
| Apriva | Len Sutton |
| BAFT/IFSA | Joseph Pawelczyk |
| Bank of America | Daniel Welch |
| Certicom Corporation | Daniel Brown |
| Citigroup, Inc. | Karla McKenna |
| CUSIP Service Bureau | James Taylor |
| Deluxe Corporation | Ralph Stolp |
| Department of the Treasury, Office of Financial Research | Michael Donnelly |
| Department of the Treasury, Office of Financial Research | Bill Nichols |
| Diebold, Inc. | Bruce Chapa |
| Discover Financial Services | Michelle Zhang |
| Federal Reserve Bank | Claudia Swendseid |
| First Data Corporation | Rick Van Luvender |
| FIS Global | Stephen Gibson-Saxty |
| Fiserv | Dan Otten |
| FIX Protocol Ltd - PTL | Jim Northey |
| Gilbraco | Bruce Welch |
| Harland Clarke | John McCleary |
| Hewlett Packard | Larry Hines |
| IBM Corporation | Todd Arnold |

| | |
|---|---|
| Independent Bankers of America | Viveca Ware |
| Ingenico | John Spence |
| J. P. Morgan Chase | Roy DeCicco |
| Key Innovations | Scott Spiker |
| KPMG LLP | Mark Lundin |
| MagTek, Inc. | Terry Benson |
| MasterCard International | Mark Kamers |
| NACHA The Electronic Payments Association | Robert Unger |
| National Association of Convenience Stores | Michael Davis |
| National Security Agency | Paul Timmel |
| NCR Corporation | Steve Stevens |
| RMG-ISITC | Genevy Dimitrion |
| RouteOne | Travis Bully |
| SWIFT/Pan Americas | Juliette Kennel |
| Symcor, Inc. | Brian Salway |
| TECSEC Incorporated | Ed Scheidt |
| The Bank of New York Mellon | David Goldberg |
| The Clearing House | Sharon Jablon |
| U. S. Bank | Brian Fickling |
| U. S. Securities and Exchange Commission | Matthew Reed |
| USDA Food and Nutrition Service | Kathy Ottobre |
| VeriFone, Inc. | Brad McGuinness |
| VISA | Kim Wagner |
| Wells Fargo Bank | Mark Tiggas |
| Wincor Nixdorf Inc | Ramesh Arunashalam |
| XAC Automation Corporation | Chuck Chagas |
| XBRL US, Inc. | Campbell Pryde |

At the time that this standard was approved, the X9F subcommittee on Data and Information Security had the following chairs and administrators:

Richard J. Sweeney, Former Chair, Proofspace
Sandra Lambert, Vice Chair, Certicom Corporation
Steve Stevens, Executive Director, Accredited Standards Committee X9, Inc.
Isabel Bailey, Administrator, Accredited Standards Committee X9, Inc.
Janet Busch, Administrator, Accredited Standards Committee X9, Inc.

The X9F subcommittee had the following member organizations, with representatives:

| **X9F Member Organization** | **Representative** |
|---|---|
| Acculynk | John Herr |
| ACI Worldwide | Doug Grote |
| Advance Auto Parts | Anthony Johnson |
| American Bankers Association | Tom Judd |
| American Express Company | Vicky Sammons |

| | |
|---|---|
| Apriva | Paul Coppinger |
| BAFT/IFSA | Joseph Pawelczyk |
| Bank of America | Andi Coleman |
| Burroughs Payments Systems, Inc. | David J. Concannon |
| Certicom Corporation | Daniel Brown |
| Citigroup, Inc. | Chii-Ren Tsai |
| Communications Security Establishment | Jonathan Hammel |
| CUSIP Service Bureau | Scott Preiss |
| DeLap LLP | Darlene Kargel |
| Deluxe Corporation | Andy Vo |
| Depository Trust and Clearing Corporation | Robert Palatnick |
| Diebold, Inc. | Bruce Chapa |
| Discover Financial Services | Jordan Schaefer |
| Equinox Payments | Gary Zempich |
| Federal Reserve Bank | Deb Hjortland |
| Ferris and Associates, Inc. | J. Martin Ferris |
| First Data Corporation | Lisa Curry |
| First National Bank of Omaha | Kristi White |
| Fiserv | Bud Beattie |
| GEOBRIDGE Corporation | Jason Way |
| Gilbraco | Bruce Welch |
| Harland Clarke | John Petrie |
| Hewlett Packard | Larry Hines |
| IBM Corporation | Todd Arnold |
| Independent Community Bankers of America | Cary Whaley |
| Ingenico | John Spence |
| ITS, Inc. (SHAZAM Networks) | Manish Nathwani |
| J. P. Morgan Chase | Edward Koslow |
| K3DES LLC | Azie Amini |
| Key Innovations | Scott Spiker |
| KPMG LLP | Mark Lundin |
| MagTek, Inc. | Terry Benson |
| Marriott International | Jude Sylvestre |
| MasterCard International | Michael Ward |
| Mustang Microsystems, Inc. | Tami Harris |
| National Association of Convenience Stores | Alan Thiemann |
| National Institute of Standards and Technology | Elaine Barker |
| National Security Agency | Paul Timmel |
| NCR Corporation | David Norris |
| PCI Security Standards Council | Troy Leach |
| Pitney Bowes, Inc. | Rick Ryan |
| Proofspace | Paul Doyle |
| Rosetta Techologies | Jim Maher |
| RSA, The Security Division of EMC | Steve Schmalz |
| Security Innovation | William Whyte |

STAR .....Lilik Kazaryan
Surety, Inc. .....Dimitrios Andivahis
Symcor, Inc. .....Brian Salway
TECSEC Incorporated .....Ed Scheidt
Thales e-Security, Inc. .....James Torjussen
The Clearing House .....Henry Farrar
Trustwave.....John Amaral
U. S. Bank .....Peter Skirvin
University Bank .....Stephen Ranzini
VeriFone, Inc. .....Dave Faoro
VISA .....John Sheets
Voltage Security, Inc. .....Martin Luther
Wells Fargo Bank .....Mark Tiggas
Wincor Nixdorf Inc.....Michael Nolte
XAC Automation Corporation .....Chuck Chagas

At the time that this standard was approved, the X9F1 Cryptographic Tool Standards and Guidelines working group that developed this standard had the following chair:

Terence Spies, Chair, Voltage Security, Inc.

Previously but for a significant portion of the time during which the current edition of this standard was developed, the X9F1 working group chair was:

Miles Smid, Orion Security Solutions, Inc.

The main editor of the current of the current edition of this standard was:

Daniel Brown, Certicom Corporation (a wholly owned subsidiary of Research in Motion, Inc.)

Others who provided comments contributing significantly to this edition of this standard were:

Elaine Barker, National Institute of Standards and Technology
Paul Timmel, National Security Agency
Rich Davis, National Security Agency
Nick Gajcowski, National Security Agency

The X9F1 working group member (and former member) organization, and including representatives, that participated actively in the development of this standard during working group discussions were:

| X9F1 Member Organization | Representative |
|---|---|
| Bank of America | Jeff Stapleton |
| Bank of America | Lawrence LaBella |
| Certicom Corporation | Daniel Brown |
| Certicom Corporation | Matthew Campagna |
| Certicom Corporation | Greg Zaverucha |
| Communications Security Establishment of Canada | Jonathan Hammell |
| LE Technology Co., Ltd. | John Lewis |
| MasterCard International | Michael Ward |
| National Institute of Standards and Technology | Elaine Barker |
| National Institute of Standards and Technology | John Kelsey |
| National Security Agency | Mary Baish |
| National Security Agency | Mike Boyle |
| National Security Agency | Paul Timmel |
| PCI Security Standards Council | Ralph Poore |
| RSA, The Security Division of EMC | Steve Schmalz |
| Security Innovation | William Whyte |
| TecSec | Ed Scheidt |
| TecSec | Wai Tsang |
| University Bank | Mick Talley |
| Verifone | Joachim Vance |
| VISA | Kim Wagner |
| Voltage Security Inc. | Terence Spies |

## Contents

## Figures

## Tables

# Public Key Cryptography for the Financial Service Industry Key Agreement and Key Transport Using Elliptic Curve Cryptography

## 1 Scope

This Standard specializes ISO/IEC 11740-3 "Informational Technology - Security Techniques - Key Management - Part 3: Mechanisms using asymmetric techniques" for use by the financial services industry.

This Standard defines key establishment schemes that employ asymmetric cryptographic techniques. The arithmetic operations involved in the operation of the schemes take place in the algebraic structure of an elliptic curve over a finite field.

Both key agreement and key transport schemes are specified.

The schemes may be used by two parties to compute shared keying data that may then be used by symmetric schemes to provide cryptographic services, e.g., data confidentiality and data integrity.

Supporting mathematical definitions and examples are also provided.

## 2 Definitions, Abbreviations and References

### 2.1 Definitions and Abbreviations

**2.1.1**
**addition rule**
An addition rule describes the addition of two elliptic curve points $P_1$ and $P_2$ to produce a third elliptic curve point $P_3$.

**2.1.2**
**approved**
An cryptographic technique, such as a hash function, key derivation function or digital signature scheme, is Approved if it is approved by the X9 Registry. SD-34, or if it is explicitly identified as Approved in this Standard.

**2.1.3**
**associate value**
Given an elliptic curve point and corresponding elliptic curve parameters, the associate value is an integer associated with the point.