

American National Standard  
for Financial Services

X9.63–2011

Public Key Cryptography for the Financial Services  
Industry

Key Agreement and Key Transport Using Elliptic  
Curve Cryptography

Secretariat:  
**Accredited Standards Committee X9, Inc.**

Approved: 2011 December 21

**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 draft 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,

Copyright 2011 by ASC X9

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

Suggestions for the improvement or revision of this standard are welcome. They should be sent to the X9 Secretariat, American Bankers Association, 1120 Connecticut Avenue, N.W., Washington D.C. 20036.

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  
Cynthia Fuller, Administrator, Accredited Standards Committee X9, Inc.  
Isabel Bailey, Administrator, Accredited Standards Committee X9, Inc.  
Janet Busch, Administrator, Accredited Standards Committee X9, Inc.  
Ed Stana, Administrator, Accredited Standards Committee X9, Inc.

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

<b>X9 Member Organization</b>	<b>Representative</b>
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
- Cynthia Fuller, Administrator, 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:

<b>X9F Member Organization</b>	<b>Representative</b>
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 Technologies.....	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:

<b>X9F1 Member Organization</b>	<b>Representative</b>
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

X9 MEMBER ORGANIZATION REPRESENTATIVE .....	II
X9F MEMBER ORGANIZATION REPRESENTATIVE .....	III
X9F1 MEMBER ORGANIZATION REPRESENTATIVE .....	VI
<b>1 SCOPE .....</b>	<b>1</b>
<b>2 DEFINITIONS, ABBREVIATIONS AND REFERENCES.....</b>	<b>1</b>
2.1 DEFINITIONS AND ABBREVIATIONS .....	1
2.2 SYMBOLS AND NOTATION .....	10
2.3 NORMATIVE REFERENCES .....	13
<b>3 APPLICATION.....</b>	<b>15</b>
3.1 GENERAL .....	15
3.2 THE SCHEMES IN THIS STANDARD.....	15
3.3 IMPLEMENTING THE SCHEMES SECURELY .....	16
3.4 ANNEXES .....	17
4 MATHEMATICAL CONVENTIONS .....	18
4.1 FINITE FIELD ARITHMETIC .....	18
4.1.1 <i>The Finite Field <math>F_p</math></i> .....	18
4.1.2 <i>The Finite Field <math>F_{2^m}</math></i> .....	18
4.2 ELLIPTIC CURVES AND POINTS.....	18
4.2.1 <i>Point Compression Technique for Elliptic Curves over <math>F_p</math> (Optional)</i> .....	18
4.2.2 <i>Point Compression Technique for Elliptic Curves over <math>F_{2^m}</math> (Optional)</i> .....	19
4.3 DATA CONVERSIONS.....	19
4.3.1 <i>Integer-to-Octet-String Conversion</i> .....	19
4.3.2 <i>Octet-String-to-Integer Conversion</i> .....	19
4.3.3 <i>Field-Element-to-Octet-String Conversion</i> .....	19
4.3.4 <i>Octet-String-to-Field-Element Conversion</i> .....	19
4.3.5 <i>Field-Element-to-Integer Conversion</i> .....	19
4.3.6 <i>Point-to-Octet-String Conversion</i> .....	19
4.3.7 <i>Octet-String-to-Point Conversion</i> .....	19
<b>5 CRYPTOGRAPHIC INGREDIENTS .....</b>	<b>19</b>
5.1 ELLIPTIC CURVE DOMAIN PARAMETER GENERATION AND VALIDATION.....	19
5.1.1 <i>Primitives for Elliptic Curve Domain Parameter Generation and Validation over <math>F_p</math></i> .....	19
5.1.2 <i>Primitives for Elliptic Curve Domain Parameter Generation and Validation over <math>F_{2^m}</math></i> .....	20
5.2 KEY PAIR GENERATION AND PUBLIC KEY VALIDATION .....	20
5.2.1 <i>Key Pair Generation Primitive</i> .....	20
5.2.2 <i>Public Key Validation</i> .....	20
5.3 CHALLENGE GENERATION PRIMITIVE .....	20
5.4 DIFFIE-HELLMAN PRIMITIVES.....	21
5.4.1 <i>Standard Diffie-Hellman Primitive</i> .....	21
5.4.2 <i>Modified Diffie-Hellman Primitive</i> .....	22
5.5 MQV PRIMITIVE .....	22
5.6 AUXILIARY FUNCTIONS .....	23
5.6.1 <i>Associate Value Function (avf)</i> .....	24
5.6.2 <i>Cryptographic Hash Functions</i> .....	24
5.6.3 <i>Key Derivation Function (kdf)</i> .....	25
5.7 MAC SCHEMES .....	26



5.7.1	<i>Tagging Transformation</i> .....	27
5.7.2	<i>Tag Checking Transformation</i> .....	27
5.8	ASYMMETRIC ENCRYPTION SCHEME.....	28
5.8.1	<i>Encryption Transformation</i> .....	29
5.8.2	<i>Decryption Transformation</i> .....	30
5.9	SIGNATURE SCHEME.....	31
5.9.1	<i>Signing Transformation</i> .....	32
5.9.2	<i>Verifying Transformation</i> .....	32
5.10	KEY CONFIRMATION SCHEMES.....	32
<b>6</b>	<b>KEY AGREEMENT SCHEMES</b> .....	<b>33</b>
6.1	EPHEMERAL UNIFIED MODEL SCHEME.....	35
6.2	1-PASS DIFFIE-HELLMAN SCHEME.....	37
6.2.1	<i>Initiator Transformation</i> .....	38
6.2.2	<i>Responder Transformation</i> .....	39
6.3	STATIC UNIFIED MODEL SCHEME.....	40
6.4	COMBINED UNIFIED MODEL WITH KEY CONFIRMATION SCHEME.....	41
6.5	1-PASS UNIFIED MODEL SCHEME.....	42
6.5.1	<i>Initiator Transformation</i> .....	43
6.5.2	<i>Responder Transformation</i> .....	44
6.6	FULL UNIFIED MODEL SCHEME.....	45
6.7	FULL UNIFIED MODEL WITH KEY CONFIRMATION SCHEME.....	47
6.8	STATION-TO-STATION SCHEME.....	48
6.8.1	<i>Initiator Transformation</i> .....	49
6.8.2	<i>Responder Transformation</i> .....	51
6.9	1-PASS MQV SCHEME.....	54
6.9.1	<i>Initiator Transformation</i> .....	55
6.9.2	<i>Responder Transformation</i> .....	55
6.10	FULL MQV SCHEME.....	56
6.11	FULL MQV WITH KEY CONFIRMATION SCHEME.....	58
<b>7</b>	<b>KEY TRANSPORT SCHEMES</b> .....	<b>59</b>
7.1	1-PASS TRANSPORT SCHEME.....	59
7.2	3-PASS TRANSPORT SCHEME.....	59
	<b>ANNEX A (NORMATIVE) NORMATIVE NUMBER-THEORETIC ALGORITHMS</b> .....	<b>60</b>
	<b>ANNEX B (INFORMATIVE) MATHEMATICAL BACKGROUND</b> .....	<b>61</b>
	<b>ANNEX C (INFORMATIVE) TABLES OF TRINOMIALS, PENTANOMIALS, AND GAUSSIAN NORMAL BASES</b> .....	<b>62</b>
	<b>ANNEX D (INFORMATIVE) INFORMATIVE NUMBER-THEORETIC ALGORITHMS</b> .....	<b>63</b>
	<b>ANNEX E (INFORMATIVE) COMPLEX MULTIPLICATION (CM) ELLIPTIC CURVE GENERATION METHOD</b> .....	<b>64</b>
	<b>ANNEX F (INFORMATIVE) SECURITY CONSIDERATIONS</b> .....	<b>65</b>
F.1	THE ELLIPTIC CURVE DISCRETE LOGARITHM PROBLEM.....	65
F.2	ELLIPTIC CURVE DOMAIN PARAMETERS.....	65
F.3	KEY PAIRS.....	65
F.4	KEY ESTABLISHMENT SCHEMES.....	65
F.4.1	<i>The ECDLP and Key Establishment Schemes</i> .....	65
F.4.2	<i>Security Attributes and Key Establishment Schemes</i> .....	66
F.4.3	<i>Security Attributes of the Schemes in this Standard</i> .....	67
F.4.4	<i>Appropriate Key Lengths</i> .....	69

<b>ANNEX G (INFORMATIVE) EXAMPLES.....</b>	<b>72</b>
G.1	EXAMPLES OF DATA CONVERSION METHODS ..... 72
G.2	EXAMPLES OF SCHEMES OVER THE FIELD $F_{2^m}$ ..... 75
G.3	EXAMPLES OF SCHEMES OVER THE FIELD $F_p$ ..... 75
G.4	SAMPLE ELLIPTIC CURVES OVER THE FIELD $F_{2^m}$ ..... 75
G.4.1	2 Examples with $m = 193$ ..... 75
G.4.2	2 Examples with $m = 233$ ..... 77
G.4.3	Example with $m = 239$ ..... 78
G.4.4	2 Examples with $m = 283$ ..... 79
G.4.5	2 Examples with $m = 409$ ..... 81
G.4.6	2 Examples with $m = 571$ ..... 82
G.5	SAMPLE ELLIPTIC CURVES OVER THE FIELD $F_p$ ..... 84
G.5.1	2 Examples with a 192-bit Prime ..... 84
G.5.2	2 Examples with a 224-bit Prime ..... 86
G.5.3	2 Examples with a 256-bit Prime ..... 88
G.5.4	An Example with a 384-bit Prime ..... 90
G.5.5	An Example with a 521-bit Prime ..... 91
<b>ANNEX H (INFORMATIVE) ASN.1.....</b>	<b>93</b>
H.1	SYNTAX FOR FINITE FIELD IDENTIFICATION..... 93
H.2	SYNTAX FOR FINITE FIELD ELEMENTS AND ELLIPTIC CURVE POINTS ..... 96
H.3	SYNTAX FOR ELLIPTIC CURVE DOMAIN PARAMETERS..... 96
H.4	SYNTAX FOR PUBLIC KEYS ..... 97
H.5	SCHEME SYNTAX ..... 101
H.5.1	Ephemeral Unified Model Scheme..... 102
H.5.2	1-Pass Diffie-Hellman Scheme ..... 103
H.5.3	Static Unified Model Scheme..... 103
H.5.4	Combined Unified Model with Key Confirmation Scheme ..... 103
H.5.5	1-Pass Unified Model Scheme ..... 104
H.5.6	Full Unified Model Scheme ..... 104
H.5.7	Full Unified Model with Key Confirmation Scheme ..... 105
H.5.8	Station-to-Station Scheme..... 105
H.5.9	1-Pass MQV Scheme..... 106
H.5.10	Full MQV Scheme ..... 106
H.5.11	Full MQV with Key Confirmation Scheme..... 106
H.5.12	1-Pass Key Transport Scheme ..... 106
H.5.13	3-Pass Key Transport Scheme ..... 107
H.6	KEY DERIVATION SYNTAX..... 107
H.7	ASN.1 MODULE..... 109
<b>ANNEX I (NORMATIVE) LEGACY SCHEMES.....</b>	<b>116</b>
I.1	OVERVIEW ..... 116
I.2	LEGACY KEY AGREEMENT SCHEMES..... 116
I.2.1	Combined Unified Model with Key Confirmation ..... 116
I.2.2	Full Unified Model with Key Confirmation Scheme ..... 122
I.2.3	Full MQV with Key Confirmation Scheme ..... 127
I.3	LEGACY KEY TRANSPORT SCHEMES..... 132
I.3.1	1-Pass Transport Scheme ..... 133
I.3.2	3-Pass Transport Scheme ..... 136
<b>ANNEX J (INFORMATIVE) BIBLIOGRAPHY.....</b>	<b>142</b>

## Figures

Figure 1 – Ephemeral Unified Model Scheme .....	35
Figure 2 – 1-Pass Diffie-Hellman Scheme .....	37
Figure 3 – Static Unified Model Scheme.....	40
Figure 4 – 1-Pass Unified Model Scheme .....	42
Figure 5 – Full Unified Model Scheme .....	45
Figure 6 – Station-to-Station Scheme.....	48
Figure 7 – 1-Pass MQV Scheme.....	54
Figure 8 – Full MQV Scheme.....	57
Figure I-1 – Combined Unified Model with Key Confirmation Scheme .....	117
Figure I-2 – Full Unified Model with Key Confirmation Scheme .....	122
Figure I-3 – Full MQV with Key Confirmation Scheme.....	128
Figure I-4 – 1-Pass Key Transport Scheme .....	134
Figure I-5 – 3-Pass Key Transport Scheme .....	137

## Tables

Table F-1 – Attributes Provided by Key Establishment Schemes .....	68
Table F-2 – Guidelines on Aligning Parameter Sizes and Symmetric Key Size .....	71

# 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 “Information 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.