

American National Standard  
for Financial Services

X9.63–2001

Public Key Cryptography for the Financial Services  
Industry

Key Agreement and Key Transport Using Elliptic  
Curve Cryptography

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

Approved: November 20, 2001

**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. ANSI X9.52, Triple-DEA) in combination with public-key cryptography-based key management techniques.

This standard, X9.63-2001, *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. DEA, TDEA). These mechanisms are based on the elliptic curve analogue of the Diffie-Hellman key agreement mechanism [4]. Because the mechanisms are based on the same fundamental mathematics as the Elliptic Curve Digital Signature Algorithm (ECDSA) (see [7]), 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 2001 by Accredited Standards Committee 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. Printed in the United States of America

Suggestions for the improvement or revision of this standard are welcome. They should be sent to Accredited Standards Committee X9, Inc., P.O. Box 4035, Annapolis, Maryland, 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.

At the time that this standard was approved, the X9 Committee had the following members:

Harold G. Deal, X9 Chairman, BB&T  
Vincent DeSantis, X9 Vice Chairman, New York Clearing House  
Cynthia L. Fuller, Managing Director  
Darlene J. Schubert, Program Manager

The X9 committee had the following members:

<b>Organization</b>	<b>Representative</b>
ACI Worldwide .....	Jim Shafer
ACI Worldwide .....	Cindy Rink
American Bankers Association .....	Stephen Schutze
American Bankers Association .....	Michael Scully
American Express Company .....	Mike Jones
American Express Company .....	Dick Schreiber
American Express Company .....	Gerry Smith
American Express Company .....	Barbara Wakefield
BB&T .....	Harold Deal
Bank One Corporation.....	Jacqueline Pagan
Bank One Corporation.....	Kimberly Ray
Bank of America .....	Mack Hicks
Bank of America .....	Richard Phillips
Bank of America .....	Daniel Welch
BancTec, Inc.....	Christopher Dowdell
BancTec, Inc.....	David Hunt
Certicom Corporation.....	Daniel Brown
Certicom Corporation.....	Donald Johnson
Citigroup, Inc.....	Mark Scott
Citigroup, Inc.....	Daniel Schutzer
Citigroup, Inc.....	Skip Zehnder
Check Solutions.....	Jerry Bowman
Check Solutions.....	Donald Harman
Check Solutions.....	Ron Schultz
Compaq Computer Corp. ....	Larry Hines
Compaq Computer Corp. ....	Gary Lefkowitz
Datum .....	John Bernardi

Datum .....	Sandra Lambert
Datum .....	Jerry Willett
Diebold, Inc. ....	Bruce Chapa
Diebold, Inc. ....	Judy Edwards
Deluxe Corporation .....	Maury Jansen
Discover Financial Services .....	Pamela Ellington
Discover Financial Services .....	Masood Mirza
Discover Financial Services .....	Patsie Rinchiuso
eFunds Corporation .....	Chuck Bram
eFunds Corporation .....	Richard Fird
eFunds Corporation .....	Forrest Martin
eFunds Corporation .....	Joseph Stein
eFunds Corporation .....	Cory Surges
eFunds Corporation .....	Daniel Rick
Federal Reserve Bank.....	Dexter Holt
Federal Reserve Bank.....	Jeannine DeLano
First Data Corporation.....	Gene Kathol
Food Marketing Institute .....	Ted Mason
Food Marketing Institute .....	Stacy Fitzgerald-Redd
Griffin Consulting .....	Harriette Griffin
Griffin Consulting .....	Phillip H. Griffin
HW and W Inc.....	Martin Ferris
JP Morgan Chase and Co. ....	Robert Blair
JP Morgan Chase and Co. ....	Richard Yen
KPMG Peat Marwick LLP .....	Al Van Ranst
KPMG Peat Marwick LLP .....	Jeff Stapleton
Mag-Tek, Inc. ....	Terry Bensen
Mag-Tek, Inc. ....	Jeff Duncan
Mag-Tek, Inc. ....	Mimi Hart
Mag-Tek, Inc .....	Carlos Morales
MasterCard International.....	Ron Karlin
MasterCard International.....	Naiyre Foster
Mellon Bank, N.A. ....	Richard Adams
Mellon Bank, N.A. ....	Jennifer Smith
Mellon Bank, N.A. ....	David Taddeo
Merrill Lynch .....	John Dolan
Merrill Lynch .....	Dave Yeger
National Association of Convenience Stores .....	John Hervey
National Association of Convenience Stores .....	Teri Richman
National Association of Convenience Stores .....	Robert Swanson
National Security Agency.....	Greg Bergren
National Security Agency.....	Sheila Brand
NCR Corporation .....	David Norris
NCR Corporation .....	Steve Stevens
New York Clearing House .....	Vincent DeSantis

New York Clearing House .....	John Dunn
PricewaterhouseCoopers .....	Jeff Zimmerman
Silas Technologies.....	Andrew Garner
Silas Technologies.....	Ray Gatland
SPYRUS.....	Karen Randall
SPYRUS.....	James Randall
Star Systems, Inc. ....	Elizabeth Lynn
Star Systems, Inc. ....	Michael Wade
Sun Microsystems .....	Yvonne Humphery
Sun Microsystems .....	Joel Weise
Unisys Corporation .....	Thomas Hayosh
Unisys Corporation .....	Navnit Shah
VeriFone, Inc.....	Brad McGuinness
VeriFone, Inc.....	John Sheets
VeriFone, Inc.....	Brenda Watlington
Visa International .....	Patricia Greenhalgh
Wells Fargo Bank.....	Terry Leahy
Wells Fargo Bank.....	Ruven Schwartz

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

Mr. Richard J. Sweeney, Chairman, Inovant

<b>Organization Represented</b>	<b>Representative</b>
ACI Worldwide .....	Cindy Rink
ACI Worldwide .....	Jim Shaffer
American Bankers Association .....	Stephen Schutze
American Bankers Association .....	Donald Rhodes
American Express Company .....	Mike Jones
American Express Company .....	Mark Merkow
American Express Company .....	Gerry Smith
American Express Company .....	Dick Schreiber
BancTec, Inc.....	Christopher Dowdell
Bank of America .....	Mack Hick
Bank of America .....	Richard Phillips
Bank of America .....	Craig Worstell
Bank One Corporation.....	Mark Ryding
BB&T .....	Harold Deal
Caradas .....	John Gould
Caradas .....	Tom Johnston
Caradas .....	Richard Kastner
Certicom Corporation.....	Daniel Brown
Certicom Corporation.....	Donald Johnson
Certicom Corporation.....	Brenda Klein
Certicom Corporation.....	Sherry Vanstone

Check Solutions.....	Harry Hankla
Check Solutions.....	Ron Schultz
Check Solutions.....	Jerry Bowman
Chrysalis-ITS.....	Terry Fletcher
Communications Security Establishment.....	Alan Poplove
Communications Security Establishment.....	Mike Chawrun
Compaq Computer Corporation .....	Larry Hines
Compaq Computer Corporation .....	Gary Lefkowitz
Datum, Inc. ....	Sandra Lambert
Deluxe Corporation .....	Maury Jansen
Diebold, Inc. ....	Bruce Chapa
Diebold, Inc. ....	Judy Edwards
Digital Signature Trust .....	Brandon Brown
Digital Signature Trust .....	Trent Henry
Discover Financial Services .....	Pamela Ellington
Discover Financial Services .....	Masood Mirza
Diversinet Corporation .....	Michael Crerar
eFunds Corporation .....	Chuck Bram
eFunds Corporation .....	Forrest Martin
Entrust Technologies .....	Santosh Chokhani
Entrust Technologies .....	Miles Smid
Entrust Technologies .....	Mike Just
Federal Reserve Bank.....	Dexter Holt
First Data Corporation.....	Gene Kathol
Food Marketing Institute .....	Ted Mason
Food Marketing Institute.....	Stacy Fitzgerald-Redd
Griffin Consulting .....	Phillip H. Griffin
Griffin Consulting .....	Harriette Griffin
H W and W, Inc.....	Martin Ferris
IBM Corporation .....	Michael Kelly
IBM Corporation .....	Stephen Mike Matyas
Ingenico Canada, Ltd. ....	John Spence
Inovant.....	Richard Sweeney
Jones Futurex, Inc.....	Ray Bryan
Jones Futurex, Inc.....	Steve Junod
JP Morgan Chase & Co .....	Robert Blair
JP Morgan Chase & Co .....	Richard Yen
KPMG Peat Marwick LLP .....	Jeff Stapleton
KPMG Peat Marwick LLP .....	Al Van Ranst, Jr.
KPMG Peat Marwick LLP .....	Azita Amini
Mag-Tek, Inc. ....	Mimi Hart
Mag-Tek, Inc. ....	Terry Benson
MasterCard International.....	Ron Karlin
MasterCard International.....	William Poletti
Mellon Bank, N.A. ....	David Taddeo

Merrill Lynch .....	Lawrence LaBella
Merril Lynch.....	Jennifer Smith
National Association of Convenience Stores .....	John Hervey
National Association of Convenience Stores .....	Robert Swanson
National Security Agency.....	Gregory Bergren
National Security Agency.....	Sheila Brand
National Security Agency.....	John Stevens
nCipher .....	William Franklin
NCR Corporation .....	David Norris
NCR Corporation .....	Adrian Shields
NCR Corporation .....	Steve Stevens
NIST .....	Elaine Barker
NIST .....	Lawrence Bassham III
NIST .....	Morris Dworkin
NIST .....	Annabelle Lee
Pitney Bowes, Inc.....	Andrei Obrea
Pitney Bowes, Inc.....	Leon Pintsov
Pitney Bowes, Inc.....	Matthew Campagna
PricewaterhouseCoopers .....	Jeff Zimmerman
Rainbow Technologies .....	Georgina Schroder
Rainbow Technologies .....	Vic Sundararajan
RSA Securities .....	Russ Housley
RSA Securities .....	Robert Silverman
SPYRUS.....	Karen Randall
SPYRUS.....	James Randall
Star Systems, Inc. ....	Elizabeth Lynn
Star Systems, Inc. ....	Michael Wade
Star Systems, Inc. ....	Carol Fazzone
Sun Microsystems PS .....	Yvonne Humphery
Sun Microsystems PS .....	Joel Weise
TECSEC Incorporated.....	Ed Scheidt
TECSEC Incorporation .....	Pud Reaver
TECSEC Incorporated.....	Jay Wack
VeriFone.....	John Sheets
Verisign, Inc. ....	Warwick Ford
VISA International .....	Richard Hite
Wells Fargo Bank.....	Terry Leahy
Wells Fargo Bank.....	Gordon Martin
Wells Fargo Bank.....	Ruven Schwartz
Zaxus, Inc. ....	Samuel Epstein
Zefer Boston.....	Michael Versace

The X9F1 Cryptographic Tool Standards and Guidelines group that developed this standard had the following members:

Miles Smid, Chairman, Entrust Technologies  
 Phillip H. Griffin, Vice Chair, Griffin Consulting  
 Daniel Brown, Project Editor, Certicom Corporation

<b>Organization</b>	<b>Representative</b>
Certicom Corporation.....	Daniel Brown
Certicom Corporation.....	Don Johnson
Certicom Corporation.....	Alfred Menezes
Certicom Corporation.....	Scott Vanstone
Certicom Corporation.....	Simon Blake-Wilson
Chrysalis-ITS.....	Francois Rousseau
Chrysalis-ITS.....	Terry Fletcher
Communications Security Establishment of Canada .....	Mike Chawrun
Communications Security Establishment of Canada .....	Alan Poplove
Diversinet .....	Michael Crerar
Entrust .....	Miles Smid
Entrust .....	Robert Zuccherato
Federal Reserve Bank of Atlanta.....	John Hannan
Federal Reserve Bank of Atlanta.....	Jeff Harris
Griffin Consulting .....	Phillip H. Griffin
IBM Corporation .....	Todd Arnold
IBM Corporation .....	Allen Roginsky
IBM Corporation .....	Steven Matyas
JP Morgan Chase & Co. ....	Gene Rao
JP Morgan Chase & Co. ....	Richard Yen
M. Blake Greenlee Associates, Ltd. ....	M. Blake Greenlee
Merrill Lynch .....	Larry LaBella
National Institute of Standards and Technology .....	Morris Dworkin
National Institute of Standards and Technology .....	Elaine Barker
National Institute of Standards and Technology .....	Sharon Keller
National Security Agency.....	Paul Timmel
National Security Agency.....	Bob Reiter
Pitney Bowes, Inc.....	Leon Pintsov
RSA Security.....	Russ Housley
RSA Security.....	Burt Kaliski
RSA Security.....	Robert Silverman
SPYRUS.....	Karen Randall
SPYRUS.....	James Randall
SPYRUS.....	Peter Yee
TecSec .....	Ersin Domangue



## Contents

<b>1</b>	<b>SCOPE .....</b>	<b>1</b>
<b>2</b>	<b>DEFINITIONS, ABBREVIATIONS AND REFERENCES .....</b>	<b>1</b>
2.1	DEFINITIONS AND ABBREVIATIONS .....	1
2.2	SYMBOLS AND NOTATION .....	9
2.3	NORMATIVE REFERENCES .....	12
<b>3</b>	<b>APPLICATION .....</b>	<b>13</b>
3.1	GENERAL.....	13
3.2	THE SCHEMES IN THIS STANDARD.....	13
3.3	IMPLEMENTING THE SCHEMES SECURELY .....	14
3.4	ANNEXES.....	15
<b>4</b>	<b>MATHEMATICAL CONVENTIONS .....</b>	<b>16</b>
4.1	FINITE FIELD ARITHMETIC .....	16
4.1.1	<i>The Finite Field <math>F_p</math></i> .....	17
4.1.2	<i>The Finite Field <math>F_{2^m}</math></i> .....	17
4.2	ELLIPTIC CURVES AND POINTS.....	21
4.2.1	<i>Point Compression Technique for Elliptic Curves over <math>F_p</math> (Optional)</i> .....	22
4.2.2	<i>Point Compression Technique for Elliptic Curves over <math>F_{2^m}</math> (Optional)</i> .....	22
4.3	DATA CONVERSIONS .....	23
4.3.1	<i>Integer-to-Octet-String Conversion</i> .....	23
4.3.2	<i>Octet-String-to-Integer Conversion</i> .....	23
4.3.3	<i>Field-Element-to-Octet-String Conversion</i> .....	24
4.3.4	<i>Octet-String-to-Field-Element Conversion</i> .....	25
4.3.5	<i>Field-Element-to-Integer Conversion</i> .....	25
4.3.6	<i>Point-to-Octet-String Conversion</i> .....	25
4.3.7	<i>Octet-String-to-Point Conversion</i> .....	26
<b>5</b>	<b>CRYPTOGRAPHIC INGREDIENTS .....</b>	<b>27</b>
5.1	ELLIPTIC CURVE DOMAIN PARAMETER GENERATION AND VALIDATION .....	28
5.1.1	<i>Primitives for Elliptic Curve Domain Parameter Generation and Validation over <math>F_p</math></i> .....	29
5.1.2	<i>Primitives for Elliptic Curve Domain Parameter Generation and Validation over <math>F_{2^m}</math></i> .....	30
5.2	KEY PAIR GENERATION AND PUBLIC KEY VALIDATION .....	32
5.2.1	<i>Key Pair Generation Primitive</i> .....	32
5.2.2	<i>Public Key Validation</i> .....	33
5.3	CHALLENGE GENERATION PRIMITIVE .....	35
5.4	DIFFIE-HELLMAN PRIMITIVES .....	36
5.4.1	<i>Standard Diffie-Hellman Primitive</i> .....	36
5.4.2	<i>Modified Diffie-Hellman Primitive</i> .....	37
5.5	MQV PRIMITIVE .....	37
5.6	AUXILIARY FUNCTIONS.....	38
5.6.1	<i>Associate Value Function (avf)</i> .....	38
5.6.2	<i>Cryptographic Hash Functions</i> .....	39
5.6.3	<i>Key Derivation Function (kdf)</i> .....	40

5.7	MAC SCHEMES .....	41
5.7.1	Tagging Transformation .....	42
5.7.2	Tag Checking Transformation .....	42
5.8	ASYMMETRIC ENCRYPTION SCHEME.....	43
5.8.1	Encryption Transformation.....	43
5.8.2	Decryption Transformation.....	44
5.9	SIGNATURE SCHEME .....	46
5.9.1	Signing Transformation .....	46
5.9.2	Verifying Transformation.....	46
<b>6</b>	<b>KEY AGREEMENT SCHEMES.....</b>	<b>47</b>
6.1	EPHEMERAL UNIFIED MODEL SCHEME .....	49
6.2	1-PASS DIFFIE-HELLMAN SCHEME.....	50
6.2.1	Initiator Transformation .....	52
6.2.2	Responder Transformation .....	52
6.3	STATIC UNIFIED MODEL SCHEME .....	53
6.4	COMBINED UNIFIED MODEL WITH KEY CONFIRMATION SCHEME.....	55
6.4.1	Initiator Transformation .....	57
6.4.2	Responder Transformation .....	59
6.5	1-PASS UNIFIED MODEL SCHEME.....	61
6.5.1	Initiator Transformation .....	62
6.5.2	Responder Transformation .....	63
6.6	FULL UNIFIED MODEL SCHEME.....	64
6.7	FULL UNIFIED MODEL WITH KEY CONFIRMATION SCHEME.....	66
6.7.1	Initiator Transformation .....	68
6.7.2	Responder Transformation .....	70
6.8	STATION-TO-STATION SCHEME.....	72
6.8.1	Initiator Transformation .....	73
6.8.2	Responder Transformation .....	75
6.9	1-PASS MQV SCHEME .....	77
6.9.1	Initiator Transformation .....	78
6.9.2	Responder Transformation .....	79
6.10	FULL MQV SCHEME .....	80
6.11	FULL MQV WITH KEY CONFIRMATION SCHEME.....	82
6.11.1	Initiator Transformation .....	83
6.11.2	Responder Transformation .....	85
<b>7</b>	<b>KEY TRANSPORT SCHEMES .....</b>	<b>86</b>
7.1	1-PASS TRANSPORT SCHEME.....	87
7.1.1	Initiator Transformation .....	89
7.1.2	Responder Transformation .....	90
7.2	3-PASS TRANSPORT SCHEME.....	90
7.2.1	Initiator Transformation .....	92
7.2.2	Responder Transformation .....	94
<b>8</b>	<b>ASN.1 SYNTAX .....</b>	<b>95</b>
8.1	SYNTAX FOR FINITE FIELD IDENTIFICATION.....	96
8.2	SYNTAX FOR FINITE FIELD ELEMENTS AND ELLIPTIC CURVE POINTS .....	98
8.3	SYNTAX FOR ELLIPTIC CURVE DOMAIN PARAMETERS .....	99
8.4	SYNTAX FOR PUBLIC KEYS .....	100
8.5	SCHEME SYNTAX.....	103
8.5.1	Ephemeral Unified Model Scheme.....	104
8.5.2	1-Pass Diffie-Hellman Scheme .....	105
8.5.3	Static Unified Model Scheme .....	105

8.5.4	<i>Combined Unified Model with Key Confirmation Scheme</i> .....	105
8.5.5	<i>1-Pass Unified Model Scheme</i> .....	106
8.5.6	<i>Full Unified Model Scheme</i> .....	106
8.5.7	<i>Full Unified Model with Key Confirmation Scheme</i> .....	107
8.5.8	<i>Station-to-Station Scheme</i> .....	107
8.5.9	<i>1-Pass MQV Scheme</i> .....	108
8.5.10	<i>Full MQV Scheme</i> .....	108
8.5.11	<i>Full MQV with Key Confirmation Scheme</i> .....	108
8.5.12	<i>1-Pass Key Transport Scheme</i> .....	108
8.5.13	<i>3-Pass Key Transport Scheme</i> .....	109
8.6	KEY DERIVATION SYNTAX.....	109
8.7	ASN.1 MODULE.....	111
<b>ANNEX A (NORMATIVE) NORMATIVE NUMBER-THEORETIC ALGORITHMS.....</b>		<b>118</b>
A.1	AVOIDING CRYPTOGRAPHICALLY WEAK CURVES .....	118
A.1.1	<i>The MOV Condition</i> .....	118
A.1.2	<i>The Anomalous Condition</i> .....	119
A.2	PRIMALITY .....	119
A.2.1	<i>A Probabilistic Primality Test</i> .....	119
A.2.2	<i>Checking for Near Primality</i> .....	120
A.3	ELLIPTIC CURVE ALGORITHMS .....	121
A.3.1	<i>Finding a Point of Large Prime Order</i> .....	121
A.3.2	<i>Selecting an Appropriate Curve and Point</i> .....	121
A.3.3	<i>Selecting an Elliptic Curve Verifiably at Random</i> .....	123
A.3.4	<i>Verifying that an Elliptic Curve was Generated at Random</i> .....	124
A.4	PSEUDORANDOM NUMBER GENERATION .....	126
A.4.1	<i>Algorithm Derived from FIPS 186</i> .....	126
<b>ANNEX B (INFORMATIVE) MATHEMATICAL BACKGROUND .....</b>		<b>128</b>
B.1	THE FINITE FIELD $F_p$ .....	128
B.2	THE FINITE FIELD $F_{2^m}$ .....	129
B.2.1	<i>Polynomial Bases</i> .....	129
B.2.2	<i>Trinomial and Pentanomial Bases</i> .....	132
B.2.3	<i>Normal Bases</i> .....	132
B.2.4	<i>Gaussian Normal Bases</i> .....	133
B.3	ELLIPTIC CURVES OVER $F_p$ .....	134
B.4	ELLIPTIC CURVES OVER $F_{2^m}$ .....	136
<b>ANNEX C (INFORMATIVE) TABLES OF TRINOMIALS, PENTANOMIALS, AND GAUSSIAN NORMAL BASES.....</b>		<b>140</b>
C.1	TABLE OF GNB FOR $F_{2^m}$ .....	140
C.2	IRREDUCIBLE TRINOMIALS OVER $F_2$ .....	142
C.3	IRREDUCIBLE PENTANOMIALS OVER $F_2$ .....	143
C.4	TABLE OF FIELDS $F_{2^m}$ WHICH HAVE BOTH AN ONB AND A TPB OVER $F_2$ .....	144
<b>ANNEX D (INFORMATIVE) INFORMATIVE NUMBER-THEORETIC ALGORITHMS .....</b>		<b>145</b>
D.1	FINITE FIELDS AND MODULAR ARITHMETIC .....	145
D.1.1	<i>Exponentiation in a Finite Field</i> .....	145
D.1.2	<i>Inversion in a Finite Field</i> .....	145
D.1.3	<i>Generating Lucas Sequences</i> .....	146
D.1.4	<i>Finding Square Roots Modulo a Prime</i> .....	146
D.1.5	<i>Trace and Half-Trace Functions</i> .....	148
D.1.6	<i>Solving Quadratic Equations over <math>F_{2^m}</math></i> .....	148

D.1.7	Checking the Order of an Integer Modulo a Prime .....	149
D.1.8	Computing the Order of a Given Integer Modulo a Prime .....	150
D.1.9	Constructing an Integer of a Given Order Modulo a Prime .....	150
D.2	POLYNOMIALS OVER A FINITE FIELD.....	151
D.2.1	GCD's over a Finite Field.....	151
D.2.2	Finding a Root in $F_{2^m}$ of an Irreducible Binary Polynomial.....	151
D.2.3	Change of Basis .....	152
D.2.4	Checking Binary Polynomials for Irreducibility.....	155
D.3	ELLIPTIC CURVE ALGORITHMS .....	155
D.3.1	Finding a Point on an Elliptic Curve.....	156
D.3.2	Scalar Multiplication (Computing a Multiple of an Elliptic Curve Point).....	157
<b>ANNEX E (INFORMATIVE) COMPLEX MULTIPLICATION (CM) ELLIPTIC CURVE GENERATION METHOD .....</b>		<b>158</b>
E.1	MISCELLANEOUS NUMBER-THEORETIC ALGORITHMS .....	158
E.1.1	Evaluating Jacobi Symbols .....	158
E.1.2	Finding Square Roots Modulo a Power of 2.....	160
E.1.3	Exponentiation Modulo a Polynomial .....	160
E.1.4	Factoring Polynomials over $F_p$ (Special Case).....	161
E.1.5	Factoring Polynomials over $F_2$ (Special Case).....	162
E.2	CLASS GROUP CALCULATIONS.....	162
E.2.1	Overview .....	162
E.2.2	Class Group and Class Number.....	163
E.2.3	Reduced Class Polynomials.....	164
E.3	COMPLEX MULTIPLICATION.....	167
E.3.1	Overview .....	167
E.3.2	Finding a Nearly Prime Order over $F_p$ .....	168
E.3.3	Finding a Nearly Prime Order over $F_{2^m}$ .....	172
E.3.4	Constructing a Curve and Point (Prime Case).....	174
E.3.5	Constructing a Curve and Point (Binary Case).....	177
<b>ANNEX F (INFORMATIVE) AN OVERVIEW OF ELLIPTIC CURVE SYSTEMS .....</b>		<b>180</b>
<b>ANNEX G (INFORMATIVE) COMPARISON OF ELLIPTIC CURVES AND FINITE FIELD GROUPS..</b>		<b>181</b>
<b>ANNEX H (INFORMATIVE) SECURITY CONSIDERATIONS .....</b>		<b>184</b>
H.1	THE ELLIPTIC CURVE DISCRETE LOGARITHM PROBLEM .....	184
H.1.1	Software Attacks.....	186
H.1.2	Hardware Attacks .....	186
H.1.3	Key Length Considerations.....	187
H.2	ELLIPTIC CURVE DOMAIN PARAMETERS .....	188
H.3	KEY PAIRS.....	190
H.4	KEY ESTABLISHMENT SCHEMES.....	191
H.4.1	The ECDLP and Key Establishment Schemes.....	191
H.4.2	Security Attributes and Key Establishment Schemes .....	192
H.4.3	Security Attributes of the Schemes in this Standard.....	193
H.4.4	Appropriate Key Lengths .....	195
H.4.5	Choosing a Key Establishment Scheme .....	197
H.5	VALIDATION ISSUES.....	200
<b>ANNEX I (INFORMATIVE) ALIGNMENT WITH OTHER STANDARDS .....</b>		<b>204</b>
<b>ANNEX J (INFORMATIVE) EXAMPLES .....</b>		<b>205</b>
J.1	EXAMPLES OF DATA CONVERSION METHODS .....	205

J.2	EXAMPLES OF SCHEMES OVER THE FIELD $F_{2^m}$ .....	208
J.2.1	<i>Ephemeral Unified Model Scheme</i> .....	208
J.2.2	<i>1-Pass Diffie-Hellman Scheme</i> .....	215
J.2.3	<i>Static Unified Model Scheme</i> .....	221
J.2.4	<i>Combined Unified Model with Key Confirmation Scheme</i> .....	226
J.2.5.	<i>1-Pass Unified Model Scheme</i> .....	238
J.2.6	<i>Full Unified Model Scheme</i> .....	246
J.2.7	<i>Full Unified Model with Key Confirmation Scheme</i> .....	255
J.2.8	<i>Station to Station Scheme</i> .....	268
J.2.9.	<i>1-Pass MQV Scheme</i> .....	280
J.2.10	<i>Full MQV Scheme</i> .....	283
J.2.11	<i>Full MQV with Key Confirmation Scheme</i> .....	287
J.2.12	<i>1-Pass Key Transport Scheme</i> .....	293
J.2.13	<i>3-Pass Key Transport Scheme</i> .....	302
J.3	EXAMPLES OF SCHEMES OVER THE FIELD $F_p$ .....	314
J.3.1	<i>Ephemeral Unified Model Scheme</i> .....	314
J.3.2	<i>1-Pass Diffie-Hellman Scheme</i> .....	317
J.3.3	<i>Static Unified Model Scheme</i> .....	320
J.3.4	<i>Combined Unified Model with Key Confirmation Scheme</i> .....	323
J.3.5.	<i>1-Pass Unified Model Scheme</i> .....	329
J.3.6	<i>Full Unified Model Scheme</i> .....	333
J.3.7	<i>Full Unified Model with Key Confirmation Scheme</i> .....	337
J.3.8	<i>Station-to-Station Scheme</i> .....	343
J.3.9.	<i>1-Pass MQV Scheme</i> .....	349
J.3.10	<i>Full MQV Scheme</i> .....	352
J.3.11	<i>Full MQV with Key Confirmation Scheme</i> .....	356
J.3.12	<i>1-pass key transport Scheme</i> .....	362
J.3.13	<i>3-Pass Key Transport Scheme</i> .....	366
J.4	SAMPLE ELLIPTIC CURVES OVER THE FIELD $F_{2^m}$ .....	372
J.4.1	<i>3 Examples with <math>m = 163</math></i> .....	372
J.4.2	<i>2 Examples with <math>m = 193</math></i> .....	374
J.4.3	<i>2 Examples with <math>m = 233</math></i> .....	376
J.4.4	<i>Example with <math>m = 239</math></i> .....	377
J.4.5	<i>2 Examples with <math>m = 283</math></i> .....	378
J.4.6	<i>2 Examples with <math>m = 409</math></i> .....	380
J.4.7	<i>2 Examples with <math>m = 571</math></i> .....	381
J.5	SAMPLE ELLIPTIC CURVES OVER THE FIELD $F_p$ .....	383
J.5.1	<i>3 Examples with a 160-bit Prime</i> .....	383
J.5.2	<i>2 Examples with a 192-bit Prime</i> .....	386
J.5.3	<i>2 Examples with a 224-bit Prime</i> .....	388
J.5.4	<i>2 Examples with a 256-bit Prime</i> .....	389
J.5.5	<i>An Example with a 384-bit Prime</i> .....	391
J.5.6	<i>An Example with a 521-bit Prime</i> .....	392
<b>ANNEX K (INFORMATIVE) BIBLIOGRAPHY</b> .....		<b>395</b>

## Figures

Figure 1 – Data Types and Conversion Conventions.....	24
Figure 2 - Ephemeral Unified Model Scheme.....	48
Figure 3 - 1-Pass Diffie-Hellman Scheme.....	50
Figure 4 - Static Unified Model Scheme.....	53
Figure 5 - Combined Unified Model with Key Confirmation Scheme.....	55
Figure 6 - 1-Pass Unified Model Scheme.....	60
Figure 7 - Full Unified Model Scheme.....	63
Figure 8 - Full Unified Model with Key Confirmation Scheme.....	66
Figure 9 - Station-to-Station Scheme.....	71
Figure 10 - 1-Pass MQV Scheme.....	76
Figure 11 - Full MQV Scheme.....	79
Figure 12 - Full MQV with Key Confirmation Scheme.....	82
Figure 13 - 1-Pass Key Transport Scheme.....	88
Figure 14 - 3-Pass Key Transport Scheme.....	91

## Tables

Table C-1 – The type of GNB that shall be used for $F_{2^m}$ .....	140
Table C-2 – Irreducible trinomials $x^m + x^k + 1$ over $F_2$ .....	142
Table C-3 – Irreducible pentanomials $x^m + x^{k3} + x^{k2} + x^{k1} + 1$ over $F_2$ . ....	143
Table C-4 – Values of $m$ for which the field $F_{2^m}$ has both an ONB and a TPB over $F_2$ .....	144
Table G-1 – $F_p^*$ and $E(F_q)$ Group Information.....	181
Table G-2 – Comparison of Notation in ANSI X9.42 and ANSI X9.63 .....	181
Table G-3 – ANSI X9.42 and ANSI X9.63 Setup .....	182
Table G-4 – ANSI X9.42 and ANSI X9.63 Key Generation .....	183
Table G-5 – Comparison of the Full Unified Model Scheme .....	183
Table H-1 - Computing power required to compute logarithms with the Pollard-p method.....	186
Table H-2 – Attributes Provided by Key Establishment Schemes.....	194
Table H-3 – Guidelines on Aligning Elliptic Curve Size and Symmetric Key Size.....	197
Table H-4 - Validation Methods and the Risks they Mitigate .....	203

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

## 1 Scope

This Standard specializes ISO/IEC 15946-3 “Cryptographic Techniques Based on Elliptic Curves – Part 3: Key Establishment” [42] 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

#### **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  $P_3$ . (See Annexes B.3 and B.4.)

#### **associate value**

Given an elliptic curve point and corresponding elliptic curve parameters, the associate value is an integer associated with the point. (See Section 5.6.1.)

#### **asymmetric cryptographic algorithm**

A cryptographic algorithm that uses two related keys, a public key and a private key; the two keys have the property that, given the public key, it is computationally infeasible to derive the private key.