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,

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:

Organization	Representative
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

Organization Represented	Representative
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 Instittute	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

Organization	Representative
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

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 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.