

# **American National Standard for Financial Services**

**X9.42–2003**

## **Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography**

Accredited Standards Committee X9, Incorporated  
Financial Industry Standards

**Date Approved: November 19, 2003**

American National Standards Institute

This is a preview of "ANSI X9.42:2003". [Click here to purchase the full version from the ANSI store.](#)

This is a preview of "ANSI X9.42:2003". [Click here to purchase the full version from the ANSI store.](#)

**ANS X9.42–2003**

**Contents**

<b>1</b>	<b>SCOPE</b> .....	<b>1</b>
<b>2</b>	<b>NORMATIVE REFERENCES</b> .....	<b>1</b>
<b>3</b>	<b>DEFINITIONS</b> .....	<b>2</b>
<b>4</b>	<b>SYMBOLS AND ABBREVIATIONS</b> .....	<b>7</b>
4.1	SYMBOLS.....	7
4.2	ABBREVIATIONS.....	9
<b>5</b>	<b>ORGANIZATION</b> .....	<b>9</b>
<b>6</b>	<b>APPLICATION</b> .....	<b>10</b>
<b>7</b>	<b>BASIC ALGORITHMS, FUNCTIONS, AND CONVERSION RULES</b> .....	<b>11</b>
7.1	DOMAIN PARAMETER GENERATION.....	11
7.2	DOMAIN PARAMETER VALIDATION.....	12
7.3	PRIVATE/PUBLIC KEY GENERATION.....	12
7.4	PUBLIC KEY VALIDATION.....	13
7.5	CALCULATION OF SHARED SECRET ELEMENTS.....	14
7.5.1	<i>Diffie-Hellman Algorithm</i> .....	14
7.5.2	<i>MQV Algorithm</i> .....	15
7.6	DATA CONVERSION RULES.....	18
7.6.1	<i>Integer-to-Bit-String Conversion</i> .....	18
7.6.2	<i>Bit-String-to-Integer Conversion</i> .....	18
7.6.3	<i>Integer-to-Octet-String Conversion</i> .....	18
7.6.4	<i>Octet-String-to-Integer Conversion</i> .....	19
7.7	KEY DERIVATION FROM A SHARED SECRET VALUE.....	19
7.7.1	<i>Key Derivation Function Based on ASN.1</i> .....	20
7.7.2	<i>Key Derivation Function Based on Concatenation</i> .....	21
7.8	MAC COMPUTATION.....	23
7.9	ANS X9.42 IMPLEMENTATION VALIDATION.....	23
<b>8</b>	<b>KEY AGREEMENT SCHEMES</b> .....	<b>24</b>
8.1	KEY AGREEMENT USING THE DIFFIE-HELLMAN ALGORITHM.....	24
8.1.1	<i>dhStatic</i> .....	24
8.1.2	<i>dhEphem</i> .....	26
8.1.3	<i>dhOneFlow</i> .....	28
8.1.4	<i>dhHybrid1</i> .....	29
8.1.5	<i>dhHybrid2</i> .....	32
8.1.6	<i>dhHybridOneFlow</i> .....	34
8.2	KEY AGREEMENT USING THE MQV ALGORITHM.....	36
8.2.1	<i>MQV2 – Interactive Form of the MQV Algorithm</i> .....	36
8.2.2	<i>MQV1 – Store and Forward Form of the MQV Algorithm</i> .....	38

<b>ANNEX A (NORMATIVE) PARAMETER SYNTAX AND ENCODING RULES .....</b>	<b>41</b>
A.1 FINITE FIELD SYNTAX.....	41
A.2 PARAMETER SYNTAX.....	42
A.2.1 Domain Parameters.....	43
A.2.2 Scheme Parameters.....	44
A.3 PUBLIC KEY SYNTAX.....	45
A.4 SCHEME SYNTAX.....	47
A.4.1 <i>dhStatic</i> .....	48
A.4.2 <i>dhEphem</i> .....	48
A.4.3 <i>dhOneFlow</i> .....	49
A.4.4 <i>dhHybrid1</i> .....	49
A.4.5 <i>dhHybrid2</i> .....	49
A.4.6 <i>dhHybridOneFlow</i> .....	49
A.4.7 <i>MQV2</i> .....	50
A.4.8 <i>MQV1</i> .....	50
A.4.9 <i>Key Agreement Object Sets</i> .....	50
A.5 KEY DERIVATION SYNTAX.....	51
A.6 MAC FOR ANS X9.42 IMPLEMENTATION VALIDATION.....	52
A.7 ASN.1 MODULE.....	52
<b>ANNEX B (NORMATIVE) DOMAIN PARAMETER GENERATION .....</b>	<b>60</b>
B.1 GENERATION OF PRIME MODULI.....	60
B.1.1 <i>Probabilistic Primality Test</i> .....	60
B.1.2 <i>Generation of Primes</i> .....	62
B.1.3 <i>Validation of Primes</i> .....	64
B.2 SELECTION OF A GENERATOR FOR Q-ORDER SUBGROUP.....	66
B.3 JACOBI SYMBOL ALGORITHM (REVISED).....	66
<b>ANNEX C (NORMATIVE) PSEUDO-RANDOM NUMBER GENERATOR.....</b>	<b>69</b>
C.1 PSEUDO-RANDOM NUMBER GENERATOR BASED ON $G(T, C)$ .....	69
C.2 PSEUDO-RANDOM NUMBER GENERATOR USING THE TDEA.....	70
<b>ANNEX D (INFORMATIVE) CALCULATION EXAMPLES.....</b>	<b>72</b>
D.1 GENERATION OF DOMAIN PARAMETERS.....	72
D.1.1 <i>Static-Key Domain Parameters (1024-bit prime)</i> .....	72
D.1.2 <i>Ephemeral-Key Domain Parameters (1024-bit prime)</i> .....	73
D.2 GENERATION OF PRIVATE/PUBLIC KEYS.....	74
D.2.1 <i>Ephemeral Private keys for U and V</i> .....	74
D.2.2 <i>Static Private and Public Keys for U and V</i> .....	74
D.3 SHARED SECRET VALUE CALCULATION – USING DIFFIE-HELLMAN ALGORITHM.....	75
D.3.1 <i>dhStatic</i> .....	75
D.3.2 <i>dhEphem</i> .....	76
D.3.3 <i>dhOneFlow</i> .....	77
D.3.4 <i>dhHybrid1</i> .....	78
D.3.5 <i>dhHybrid2</i> .....	79
D.3.6 <i>dhHybridOneFlow</i> .....	81
D.4 SHARED SECRET VALUE CALCULATIONS – USING MQV ALGORITHM.....	82
D.4.1 <i>MQV2 – Interactive Form</i> .....	82
D.4.2 <i>MQV1 – Store and Forward Form</i> .....	87
D.5 KEY DERIVATION FUNCTION.....	90
D.5.1 <i>Examples of the Key Derivation function Based on Concatenation</i> .....	90

**ANS X9.42–2003**

D.5.2	<i>Example of the Derivation Function Based on ASN.1 - Single Invocation Where Keys are Generated for One Purpose</i> .....	95
D.6	MAC COMPUTATION.....	97
<b>ANNEX E (INFORMATIVE) SECURITY CONSIDERATIONS .....</b>		<b>100</b>
E.1	SECURITY OF THE DISCRETE LOGARITHM PROBLEM IN GF(P)* .....	100
E.1.1	<i>Discrete Logarithm Problem and Key Agreement</i> .....	100
E.1.2	<i>Complexity of the Discrete Logarithm Problem</i> .....	100
E.1.3	<i>Expense of Solving the Discrete Logarithm Problem</i> .....	101
E.1.4	<i>Relative Security Strength and Appropriate Key Lengths</i> .....	102
E.2	SECURITY OF KEY AGREEMENT SCHEMES.....	104
E.2.1	<i>Man-in-the-Middle-Attack</i> .....	104
E.2.2	<i>Small Subgroup Attacks on Invalid Public Keys</i> .....	105
E.2.3	<i>Security Attributes of the Schemes in this Standard</i> .....	105
E.3	GUIDELINES ON SELECTING AN ANS X9.42 KEY AGREEMENT SCHEME.....	108
E.4	GENERAL SECURITY CONSIDERATIONS.....	111
E.4.1	<i>Setup Negotiation</i> .....	111
E.4.2	<i>Private/Public Key Management</i> .....	111
E.4.3	<i>Parameter Management</i> .....	112
E.4.4	<i>Generation of Public and Private Keys</i> .....	112
<b>ANNEX F (INFORMATIVE) SUMMARY OF CHANGES FROM ANS X9.42–2001 .....</b>		<b>114</b>
F.1	TECHNICAL ISSUES.....	114
F.1.1	<i>Range of bases in Miller-Rabin test</i> .....	114
F.1.2	<i>Perfect squares in Lucas test</i> .....	114
F.1.3	<i>Discriminants with Jacobi symbol 0 in Lucas test</i> .....	114
F.1.4	<i>Errors in the Jacobi symbol algorithm</i> .....	114
F.2	EDITORIAL ISSUES .....	115
F.2.1	<i>Lucas-Lehmer vs. Lucas</i> .....	115
F.2.2	<i>Reference for combining Miller-Rabin and Lucas tests</i> .....	115
F.2.3	<i>Binary expansion</i> .....	115
F.2.4	<i>Inconsistent notation in the Lucas test</i> .....	115
F.2.5	<i>Modular division in Lucas test</i> .....	115
<b>ANNEX G (INFORMATIVE) REFERENCES .....</b>		<b>116</b>

## **Tables**

Table 1 – Key Agreement Scheme dhStatic .....	25
Table 2 – Key Agreement Scheme dhEphem .....	27
Table 3 – Key Agreement Scheme dhOneFlow .....	29
Table 4 – Key Agreement Scheme dhHybrid1 .....	31
Table 5 – Key Agreement Scheme dhHybrid2 .....	33
Table 6 – Key Agreement Scheme dhHybridOneFlow .....	35
Table 7 – Key Agreement Scheme MQV2 .....	38
Table 8 – Key Agreement Scheme MQV1 .....	40
Table E.1 – Complexity of Attacks on Cryptographic Algorithms .....	103
Table E.2 – Approximate Equivalence of Keys In Bits To Known Best General Attacks .....	104
Table E.3 – Attributes Provided by Key Agreement Schemes .....	107

## **ANS X9.42–2003**

### **Forward**

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**  
**P.O. Box 4035**  
**Annapolis, MD 21403 USA**  
**X9 Online <http://www.x9.org>**

Copyright © 2003 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.



## Introduction

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 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 using symmetrically-keyed encryption algorithms (e.g. ANS X9.52, Triple-DEA) in combination with public key cryptography-based key management techniques.

This standard, ANS X9.42-2003, *Public Key Cryptography For The Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography*, defines the secure establishment of cryptographic data for the keying of symmetrically-keyed algorithms (e.g. TDEA). Schemes are provided for the agreement of symmetric keys using Diffie-Hellman and MQV algorithms. The Diffie-Hellman key agreement mechanism is a well-understood and widely implemented public key technique that facilitates cost-effective cryptographic key agreement across modern distributed electronic networks such as the Internet. The MQV algorithm is a variation of the Diffie-Hellman algorithm that has more security attributes and may provide better performance over analogous Diffie-Hellman methods. Because the Diffie-Hellman and the MQV techniques are based on the same fundamental mathematics as the Digital Signature Algorithm (DSA) (see [4]), 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 (even though the techniques specified in the standard are a basis for security). 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.

This standard also does not guarantee interoperability (though, again, the techniques specified in this standard are a basis for interoperability). ANS X9.42 is not a standard for interoperability, but a set of ASC X9-approved key establishment schemes with varying attributes.

**NOTE** The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights.

By publication of this standard, no position is taken with respect to the validity of this claim or of any patent rights in connection therewith. The patent holder has, 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 standards developer.

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, P.O. Box 4035, Annapolis, MD 21403 USA.

## ANS X9.42–2003

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.

The X9 committee had the following members:

Harold Deal, X9 Chairman  
Vincent DeSantis, X9 Vice-Chairman  
Cynthia Fuller, Executive Director  
Isabel Bailey, Managing Director

### Organization Represented

ACI Worldwide  
ACI Worldwide  
American Express Company  
American Express Company  
American Financial Services Association  
American Financial Services Association  
Bank of America  
Bank of America  
Bank of America  
Bank One Corporation  
BB and T  
BB and T  
Cable & Wireless America  
Cable & Wireless America  
Cable & Wireless America  
Cable & Wireless America  
Citigroup, Inc.  
Citigroup, Inc.  
Citigroup, Inc.  
Deluxe Corporation  
Deluxe Corporation  
Deluxe Corporation  
Deluxe Corporation  
Deluxe Corporation  
Diebold, Inc.  
Diebold, Inc.  
Diebold, Inc.  
Discover Financial Services  
Discover Financial Services  
Discover Financial Services  
Discover Financial Services  
Discover Financial Services  
eFunds Corporation  
eFunds Corporation  
eFunds Corporation

### Representative

Cindy Rink  
Jim Shaffer  
Mike Jones  
Barbara Wakefield  
John Freeman  
Mark Zalewski  
Mack Hicks  
Richard Phillips  
Daniel Welch  
Jacqueline Pagan  
Michael Saviak  
Woody Tyner  
Dr. William Hancock CISSP CISM  
Shannon Myers  
Kevin M. Nixon CISSP CISM  
Jonathan Siegel  
Paul Gubiotti  
Daniel Schutzer  
Mark Scott  
Bill Ferguson  
John Fitzpatrick  
Alain Rault  
John Toedter  
Mike Valiquet  
Bruce Chapa  
Anne Doland  
Judy Edwards  
Todd Douthat  
Pamela Ellington  
Matt Johanson  
Dan Kniola  
Jon Mills  
Chuck Bram  
Richard Fird  
Daniel Rick

eFunds Corporation	Joseph Stein
eFunds Corporation	Cory Surges
Federal Reserve Bank	Jeannine M. DeLano
Federal Reserve Bank	Dexter Holt
Federal Reserve Bank	Lori Hood
First Data Corporation	Gene Kathol
First Data Corporation	Todd Nuzum
Fiserv	Bud Beattie
Fiserv	Kevin Finn
Fiserv	Dan Otten
Fiserv	William Saffici
Fiserv	Linda Weber
Hewlett Packard	Larry Hines
Hewlett Packard	Gary Lefkowitz
Hypercom	Scott Spiker
Hypercom	Dennis Sullivan
Hypercom	Gary Zempich
IBM Corporation	Todd Arnold
Ingenico	John Sheets
Ingenico	John Spence
Inovant	Richard Sweeney
KPMG LLP	Tim Gartin
KPMG LLP	Mark Lundin
KPMG LLP	Jeff Stapleton
KPMG LLP	Alfred F. Van Ranst Jr.
MagTek, Inc.	Terry Benson
MagTek, Inc.	Jeff Duncan
MagTek, Inc.	Mimi Hart
MagTek, Inc.	Carlos Morales
MasterCard International	Caroline Dionisio
MasterCard International	Naiyre Foster
MasterCard International	Ron Karlin
MasterCard International	William Poletti
Mellon Bank, N.A.	Richard H. Adams
Mellon Bank, N.A.	David Taddeo
National Association of Convenience Stores	John Hervey
National Association of Convenience Stores	Teri Richman
National Association of Convenience Stores	Robert Swanson
National Security Agency	Sheila Brand
NCR Corporation	David Norris
NCR Corporation	Steve Stevens
Niteo Partners	Charles Friedman
Niteo Partners	Michael Versace
Star Systems, Inc.	Elizabeth Lynn
Star Systems, Inc.	Michael Wade
Symmetricom	Sandra Lambert

**ANS X9.42–2003**

The Clearing House  
The Clearing House  
Unisys Corporation  
Unisys Corporation  
VeriFone, Inc.  
VeriFone, Inc.  
VeriFone, Inc.  
VeriFone, Inc.  
VeriFone, Inc.  
VeriFone, Inc.  
VISA  
VISA International  
Wachovia Bank  
Wachovia Bank  
Wells Fargo Bank

Vincent DeSantis  
John Dunn  
David J. Concannon  
Navnit Shah  
David Ezell  
Dave Faoro  
Allison Holland  
Brad McGuinness  
Brenda Watlington  
Brian Hamilton  
Patricia Greenhalgh  
Andrew Garner  
Ray Gatland  
Terry Leahy

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

Richard Sweeney, Chairman

Organization Represented

3PEA Technologies, Inc.  
3PEA Technologies, Inc.  
ACI Worldwide  
ACI Worldwide  
American Express Company  
American Express Company  
American Express Company  
American Financial Services Association  
American Financial Services Association  
Bank of America  
Bank of America  
Bank of America  
Bank of America  
Bank of America  
Bank of America  
Bank of America  
Bank One Corporation  
BB and T  
BB and T  
Cable & Wireless America  
Cable & Wireless America  
Cable & Wireless America  
Cable & Wireless America  
Certicom Corporation  
Citigroup, Inc.  
Communications Security Establishment  
Communications Security Establishment  
Deluxe Corporation  
Deluxe Corporation  
Deluxe Corporation  
Deluxe Corporation  
Deluxe Corporation  
Diebold, Inc.  
Diebold, Inc.  
Diebold, Inc.  
Discover Financial Services  
Discover Financial Services  
Discover Financial Services  
Discover Financial Services  
Discover Financial Services  
Diversinet Corporation  
Diversinet Corporation

Representative

Mark Newcomer  
Daniel Spence  
Cindy Rink  
Jim Shaffer  
William J. Gray  
Mike Jones  
Mark Merkow  
John Freeman  
Mark Zalewski  
Andi Coleman  
Mack Hicks  
Todd Inskeep  
Richard Phillips  
Daniel Welch  
Craig Worstell  
Jacqueline Pagan  
Michael Saviak  
Woody Tyner  
Dr. William Hancock CISSP CISM  
Shannon Myers  
Kevin M. Nixon CISSP CISM  
Jonathan Siegel  
Daniel Brown  
Paul Gubiotti  
Mike Chawrun  
Alan Poplove  
Bill Ferguson  
John Fitzpatrick  
Alain Rault  
John Toedter  
Mike Valiquet  
Bruce Chapa  
Anne Doland  
Judy Edwards  
Todd Douthat  
Pamela Ellington  
Matt Johanson  
Dan Kniola  
Jon Mills  
Rick (Richard P.) Kastner  
David Simonetti

**ANS X9.42–2003**

eFunds Corporation	Chuck Bram
Federal Reserve Bank	Neil Hersch
Ferris and Associates, Inc.	J. Martin Ferris
First Data Corporation	Gene Kathol
First Data Corporation	Todd Nuzum
Fiserv	Bud Beattie
Fiserv	Dan Otten
Hewlett Packard	Larry Hines
Hewlett Packard	Gary Lefkowitz
Hypercom	Scott Spiker
Hypercom	Dennis Sullivan
Hypercom	Gary Zempich
IBM Corporation	Todd Arnold
IBM Corporation	Michael Kelly
IBM Corporation	Allen Roginsky
Identrus	Brandon Brown
InfoGard Laboratories	Tom Caddy
InfoGard Laboratories	Ken Kolstad
Ingenico	John Sheets
Ingenico	John Spence
Inovant	Richard Sweeney
International Biometric Group	Mcken Mak CISSP
International Biometric Group	Mike Thieme
Jones Futurex, Inc.	Ray Bryan
Jones Futurex, Inc.	Scott Davis
Jones Futurex, Inc.	Barry Golden
Jones Futurex, Inc.	Steve Junod
KPMG LLP	Azita Amini
KPMG LLP	Tim Gartin
KPMG LLP	Mark Lundin
KPMG LLP	Jeff Stapleton
KPMG LLP	Alfred F. Van Ranst Jr.
MagTek, Inc.	Terry Benson
MagTek, Inc.	Mimi Hart
MasterCard International	Ron Karlin
MasterCard International	William Poletti
Mellon Bank, N.A.	David Taddeo
National Association of Convenience Stores	John Hervey
National Association of Convenience Stores	Robert Swanson
National Security Agency	Sheila Brand
NCR Corporation	Wayne Doran
NCR Corporation	Charlie Harrow
NCR Corporation	David Norris
NCR Corporation	Steve Stevens
Niteo Partners	Charles Friedman

Niteo Partners	Michael Versace
NIST	Elaine Barker
NIST	Lawrence Bassham III
NIST	Morris Dworkin
NIST	Annabelle Lee
NTRU Cryptosystems, Inc.	Ari Singer
NTRU Cryptosystems, Inc.	William Whyte
Orion Security Solutions	Santosh Chokhani
Orion Security Solutions	Miles Smid
Pitney Bowes, Inc.	Matthew Campagna
Pitney Bowes, Inc.	Andrei Obrea
Pitney Bowes, Inc.	Leon Pintsov
R Squared Academy Ltd.	Richard E. Overfield Jr.
R Squared Academy Ltd.	Ralph Spencer Poore
RSA Security	Burt Kaliski
Star Systems, Inc.	Elizabeth Lynn
Star Systems, Inc.	Michael Wade
Surety, Inc.	Dimitrios Andivahis
Symmetricon	Sandra Lambert
TECSEC Incorporated	Pud Reaver
TECSEC Incorporated	Ed Scheidt
TECSEC Incorporated	Dr. Wai Tsang
TECSEC Incorporated	Jay Wack
Thales e-Security, Inc.	Paul Meadowcroft
Thales e-Security, Inc.	Brian Sullivan
Thales e-Security, Inc.	James Torjussen
VeriFone, Inc.	Dave Faoro
VeriFone, Inc.	Brad McGuinness
VISA International	Patricia Greenhalgh
VISA International	Richard Hite
Wachovia Bank	Andrew Garner
Wachovia Bank	Ray Gatland
Wells Fargo Bank	Terry Leahy
Wells Fargo Bank	Gordon Martin
Wells Fargo Bank	Ruven Schwartz

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 publication, the X9 Secretariat received an original signed release permitting such company names to appear in print.)

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

**ANS X9.42–2003**

Miles Smid, Chairman and Elaine Barker, Project Editor

Organization Represented

ACI Worldwide  
American Express Company  
BB and T  
Cable & Wireless America  
Cable & Wireless America  
Cable & Wireless America  
Cable & Wireless America  
Certicom Corporation  
Certicom Corporation  
Communications Security Establishment  
Communications Security Establishment  
DeLap, White, Caldwell and Croy, LLP  
Diebold, Inc.  
Diebold, Inc.  
Diebold, Inc.  
Discover Financial Services  
Discover Financial Services  
Diversinet Corporation  
Diversinet Corporation  
eFunds Corporation  
Entrust, Inc.  
Entrust, Inc.  
Federal Reserve Bank  
First Data Corporation  
First Data Corporation  
First Data Corporation  
First Data Corporation  
Fiserv  
Fiserv  
Hewlett Packard  
Hypercom  
Hypercom  
Hypercom  
IBM Corporation  
IBM Corporation  
IBM Corporation  
Identrus  
InfoGard Laboratories  
InfoGard Laboratories  
Ingenico  
Ingenico  
Inovant

Representative

Jim Shaffer  
Mike Jones  
Michael Saviak  
Dr. William Hancock CISSP CISM  
Shannon Myers  
Kevin M. Nixon CISSP CISM  
Jonathan Siegel  
Daniel Brown  
Scott Vanstone  
Mike Chawrun  
Alan Poplove  
Darlene Kargel  
Bruce Chapa  
Anne Doland  
Judy Edwards  
Todd Douthat  
Jon Mills  
Rick (Richard P.) Kastner  
David Simonetti  
Chuck Bram  
Don Johnson  
Robert Zuccherato  
Neil Hersch  
Lisa Curry  
Michael Hodges  
Todd Nuzum  
Lynn Wheeler  
Bud Beattie  
Dan Otten  
Larry Hines  
Scott Spiker  
Dennis Sullivan  
Gary Zempich  
Todd Arnold  
Michael Kelly  
Allen Roginsky  
Brandon Brown  
Tom Caddy  
Ken Kolstad  
John Sheets  
John Spence  
Richard Sweeney



KPMG LLP	Tim Gartin
KPMG LLP	Mark Lundin
KPMG LLP	Jeff Stapleton
Landgrave Smith, Jr.	Landgrave Smith
MasterCard International	William Poletti
National Security Agency	Mike Boyle
National Security Agency	Sheila Brand
National Security Agency	Paul Timmel
NCR Corporation	Charlie Harrow
NCR Corporation	Ali Lowden
NCR Corporation	Ally Whytock
Niteo Partners	Charles Friedman
Niteo Partners	Michael Versace
NIST	Elaine Barker
NIST	Lawrence Bassham III
NIST	William Burr
NIST	Morris Dworkin
NIST	Randall Easter
NIST	Sharon Keller
NIST	John Kelsey
NTRU Cryptosystems, Inc.	Nick Howgrave-Graham
NTRU Cryptosystems, Inc.	Ari Singer
NTRU Cryptosystems, Inc.	William Whyte
Orion Security Solutions	Santosh Chokhani
Orion Security Solutions	Miles Smid
Pitney Bowes, Inc.	Matthew Campagna
Pitney Bowes, Inc.	Leon Pintsov
R Squared Academy Ltd.	Richard E. Overfield Jr.
R Squared Academy Ltd.	Ralph Spencer Poore
Relyco Sales Inc	Christopher Dowdell
RSA Security	Burt Kaliski
RSA Security	Mark McCutcheon
Symmetricom	Sandra Lambert
TECSEC Incorporated	Pud Reaver
TECSEC Incorporated	Ed Scheidt
TECSEC Incorporated	Dr. Wai Tsang
Thales e-Security, Inc.	Tim Fox
Thales e-Security, Inc.	Doug Grote
Thales e-Security, Inc.	Brian Sullivan
Thales e-Security, Inc.	James Torjussen
Unisys Corporation	David J. Concannon
VeriFone, Inc.	Dave Faoro
VISA International	Richard Hite
Wells Fargo Bank	Gordon Martin

**ANS X9.42–2003**

This document cancels and replaces ANS X9.42—2001, the previous edition of this Standard. The technical changes to the 2001 edition are described in Annex F.

# ANS X9.42 – 2003, Public Key Cryptography for The Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography

## 1 Scope

This standard, partially adapted from ISO 11770-3 (see [13]), specifies schemes for the agreement of symmetric keys using Diffie-Hellman and MQV algorithms. It covers methods of domain parameter generation, domain parameter validation, key pair generation, public key validation, shared secret value calculation, key derivation, and test message authentication code computation for discrete logarithm problem based key agreement schemes. These methods may be used by different parties to establish a piece of common shared secret information such as cryptographic keys. The shared secret information may be used with symmetrically-keyed algorithms to provide confidentiality, authentication, and data integrity services for financial information, or used as a key-encrypting key with other ASC X9 key management protocols.

The key agreement schemes given herein do not provide certain desired assurances of security, such as key confirmation and entity authentication. However, these schemes may be used in conjunction with key confirmation and entity authentication mechanisms in key establishment protocols that are specified in other ASC X9 standards. These key agreement schemes may be used as subroutines to build key establishment protocols (see [8]). The key establishment methods specified in ANS X9.63 provide examples of mechanisms for obtaining these additional security properties. Further references for key agreement can be found in [33].

## 2 Normative References

ANS X3.92 –1981 (Revised 1998): *American National Standard - Data Encryption Algorithm.*

ANS X9.30 - Part 1 (Revised) - 1997: *Public Key Cryptography For the Financial Services Industry: The Digital Signature Algorithm (DSA).*

ANS X9.30 - Part 2 (Revised) - 1997: *Public Key Cryptography For the Financial Services Industry: Secure Hash Algorithm (SHA-1).*

ANS X9.52-1998: *Triple Data Encryption Algorithm Modes of Operation.*

ANS X9.57-1997: *Public Key Cryptography For the Financial Services Industry: Certificate Management.*

IEEE P1363-2000, *Standard Specifications for Public Key Cryptography.*