American National Standard
for Financial Services

ANSI X9.44–2007

Public-Key Cryptography for the Financial Services Industry

Key Establishment Using Integer Factorization Cryptography

Accredited Standards Committee X9, Incorporated
Financial Industry Standards

Date Approved: August 24, 2007

American National Standards Institute

Contents

Page

Figures

Tables

Foreword

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CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time.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

Introduction

This Standard specifies key establishment schemes using public-key cryptography based on the integer factorization problem.

Two types of key establishment schemes are specified. In the first type, *key transport*, one party selects keying material and conveys it to the other party with cryptographic protection. In the second, *key agreement*, both parties actively share in the establishment of the keying material. The keying material may consist of one or more individual keys used to provide other cryptographic services that are outside the scope of this Standard, e.g. data confidentiality, data integrity, or symmetric-key-based key establishment.

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.

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:
James Shaffer, X9 Chairman
Vincent DeSantis, X9 Vice-Chairman
Cynthia Fuller, Executive Director
Susan Yashinskie, Managing Director

Organization Represented	Representative
ACI Worldwide	James Shaffer
American Bamkers Association	C. Diane Poole
American Financial Services Association	Mark Zalewski
American Express Company	John Allen
Bank of America	Daniel Welch
Certicom Corporation	Daniel Brown
Citigroup, Inc.	Mike Halpern
Clarke American Checks Inc.	John W. McCleary
CUSIP Service Bureau	James Taylor
Deluxe Corporation	John FitzPatrick
Diebold, Inc.	Bruce Chapa
Discover Financial Services	Katie Howser
Federal Reserve Bank	Dexter Holt
First Data Corporation	Elizabeth Lynn
Fiserv	Skip Smith
FSTC, Financial Services Consortium	Daniel Schutzer
Hewlett Packard	Larry Hines
Hypercom	Scott Spiker

IBM Corporation	Todd Arnold
Ingenico	John Spence
Intuit, Inc.	Jana Hocker
iStream Imaging Bank of Kenney	Ken Biel
JP Morgan Chase & Co	Jacqueline Pagan
KPMG LLP	Mark Lundin
Mag-Tek, Inc.	Carlos Morales
MasterCard International	William Poletti
National Association of Convenience Stores	Michael Davis
National Security Agency	Sheila Brand
NCR Corporation	Steve Stevens
RMG SWIFT	Jean-Marie Eloy
SWIFT/Pan Americas	Malene McMahon
The Clearing House	Vincent DeSantis
U. S. Bank	Marc Morrison
University Bank	Stephen Ranzini
VECTORsgi	Ron Schultz
VeriFone	Brad McGuinnes
VISA	Richard Sweeney
Wachovia Bank	Ray Gatland
Wells Fargo Bank	Ruven Schwartz

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

Richard J. Sweeney, X9F Chairman
Sandra Lambert, X9F Vice Chairman

Organization	**Representative**
3PEA Technologies, Inc.	Mark Newcomer
ACI Worldwide	Jim Shaffer
American Financial Services Association	Mark Zalewski
Bank of America	Daniel Welch
Certicom Corporation	Daniel Brown
Citigroup, Inc.	Gary Word
ClearWave Electronics	Mark Ross
CUSIP Servis Bureau	Scott Preiss
DeLap, White, Caldwell and Croy, LLP	Darlene Kargel
Deluxe Corporation	John Fitzpatrick
Depository Trust and Clearing Corporation	Robert Palatnick
Diebold, Inc.	Bruce Chapa
Discover Financial Services	Julie Shaw
Entrust, Inc.	Miles Smid
Federal Reserve Bank	Jeannine M. DeLano
Federal Reserve Bank	Dexter Holt
Ferris and Associates, Inc.	J. Martin Ferris
First Data Corporation	Rick Van Luvender
Fiserv	Bud Beattie
FSTC, Financial Services Technical Consortium	Daniel Schutzer
Futurex	Jason Anderson
Harland Clarke	John McCleary
Hewlett Packard	Larry Hines
Hypercom	Scott Spiker
IBM Corporation	Todd Arnold
InfoGuard Laboratories	Tom Caddy

Ingenico	John Spence
Innove	Steven Teppler
Intel Massachusetts, Inc.	Paul Posco
JP Morgan Chase & Co	Edward Koslow
KPMG LLP	Mark Lundin
Mag-Tek, Inc.	Carlos Morales
MasterCard International	Michael Ward
National Institute of Standards and Technology	Elaine Barker
National Security Agency	Sheila Brand
NCR Corporation	David Norris
NTRU Cryptosystems	William Whyte
Pitney Bowes Inc.	Leon Pintsov
Proofspace	Paul F. Doyle
Rosetta Technologies	Jim Maher
Rosetta Technologies	Paul Malinowski
RSA, The Security Division of EMC	James Randall
Surety, Inc.	Dimitrios Andivahis
TECSEC Incorporated	Ed Scheidt
Thales e-Security, Inc.	James Torjussen
The Clearing House	Vincent DeSantis
Triton Systems of Delaware	Daryll Cordeiro
U.S. Bank	Marc Morrison
Unisys Corporation	David J. Concannon
University Bank	Stephen Ranzini
VECTORsgi	Ron Schultz
VeriFone	Dave Faoro
VISA	John Sheets
Voltage Security Inc.	Luther Martin
Wachovia Bank	Ray Gatland
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 that developed this standard had the following members:

Miles Smid, Chairman and James Randall, Project Editor

Organization	**Representative**
Certicom Corporation	Dan Brown
Certicom Corporation	Scott Vanstone
Communications Security Establishment of Canada	Bridget Walshe
Entrust	Don Johnson
Entrust	Miles Smid
HP	Susan Langford
MasterCard	Mike Ward
National Institute of Standards and Technology	Morris Dworkin
National Institute of Standards and Technology	Elaine Barker
National Institute of Standards and Technology	John Kelsey
National Institute of Standards and Technology	Lily Chen

National Security Agency	Paul Timmel
National Security Agency	Michael Boyle
NTRU	William Whyte
Pitney Bowes, Inc	Matt Compagna
Pitney Bowes, Inc	Rick Ryan
RSA, The Security Division of EMC	James Randall
RSA, The Security Division of EMC	Steve Schmalz
RSA, The Security Division of EMC	Burt Kaliski

Public-Key Cryptography for the Financial Services Industry Key Establishment Using Integer Factorization Cryptography

1 Scope

This Standard specifies key establishment schemes using public-key cryptography based on the integer factorization problem. Both key agreement and key transport schemes are specified. The schemes may be used by two parties to transport or agree on shared keying material (see Note 1). The keying material may be used to provide other cryptographic services that are outside the scope of this Standard, e.g. data confidentiality, data integrity, and symmetric-key-based key establishment. The key pair generators may be used in other Standards based on the integer factorization problem.

The Standard also specifies key pair generators and corresponding key pair validation methods supporting the key establishment schemes. (See Note 2) The key pair generators may also be used to produce key pairs for other schemes (e.g., digital signature schemes) based on the integer factorization problem, and the key pair validation methods may likewise be used to validate such key pairs.

This version of the Standard is limited to key establishment schemes and key pair generators and validation methods based on the RSA public-key cryptosystem [88], and are intended to reflect and guide current industry practice. Future versions may include schemes based on other types of integer factorization cryptography (see Note 3) and/or additional schemes with different attributes (see Note 4).

NOTES

1. The keying material established by these schemes is assumed to be secret. Key establishment schemes may also be defined for establishing non-secret values securely (e.g., for distributing a public key with integrity protection, as in a certificate). Such schemes are not considered in this Standard.

2. A key pair validation method determines whether a candidate public-key/private-key pair meets the constraints for key pairs produced by a particular key pair generation method. A *public-key validation method* determines whether a candidate public key meets those constraints, without knowledge of the private key. Public-key validation methods are not specified in this version of the Standard, but are expected to be developed in future X9 work. For general discussion, please see Annex D.

3. Forms of integer factorization cryptography that are supported in other standards documents include the Rabin-Williams cryptosystem [85][104], ESIGN [79][80], and the Okamoto-Uchiyama cryptosystem [81]. Rabin-Williams is supported in ANS X9.31 and IEEE Std 1363-2000 [49], and the others are in IEEE Std 1363a-2004 [50].

4. The schemes in this Standard were selected with two primary purposes: to allow compatibility with current industry practice, where appropriate, and to offer enhancements to current industry practice that provide greater security assurance. The set of attributes offered by the schemes is thus limited when compared to the full portfolio of schemes in integer factorization cryptography, as well as what is available in ASC X9 standards for other families of public-key cryptography.

5. The key establishment schemes specified in this Standard involve general constructions with underlying components specific to integer factorization cryptography. For other purposes, underlying components from finite field DLC (discrete logarithm cryptography) or elliptic curve DLC could also be employed in the constructions, though such use is outside the scope of this Standard.