



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

Foreword.....	vii
Introduction	viii
1 Scope	1
2 Normative references	2
3 Terms and definitions.....	2
4 Symbols and abbreviated terms	7
5 Overview and organization	14
5.1 General.....	14
5.2 Compatibility modes.....	15
5.3 Organization	15
6 Security levels.....	16
7 Data conversion primitives.....	17
7.1 Overview	17
7.2 Integer to Octet String Primitive (I2OSP).....	17
7.3 Octet String to Integer Primitive (OS2IP)	18
8 Components from other X9 sources.....	19
8.1 Overview	19
8.2 Random number (bit) generators (RNGs)	19
8.3 Prime number generators	19
8.4 Primality testing methods.....	19
8.5 Hash functions	20
8.6 Message authentication codes.....	20
8.7 Symmetric key-wrapping schemes.....	22
8.8 Signature schemes with appendix.....	22
9 Additional components	23
9.1 Overview	23
9.2 Mask generation functions	23
9.2.1 Overview	23
9.2.2 MGF1	23
9.3 Key derivation functions.....	24
9.3.1 Overview	24
9.3.2 KDF2/KDF3	25
10 Public-key components	27
10.1 Overview	27
10.2 RSA key pairs.....	27
10.3 RSA key pair generators	28
10.3.1 RSAKPG1 family: RSA key pair generation with a fixed public exponent.....	29
10.3.2 RSAKPG2: RSA key pair generation with a random public exponent	32
10.4 RSA key pair validation.....	35
10.4.1 Overview	35
10.4.2 RSAKPV1: RSA Key Pair Validation with a Fixed Exponent	36
10.4.3 RSAKPV2: RSA Key Pair Validation with a Random Exponent	39
10.5 Partial public-key validation and plausibility tests	43
10.5.1 Overview	43

ANSI X9.44–2007

10.5.2	Plausible Size Tests	44
10.5.3	Plausible size and value tests	44
10.6	Encryption and decryption primitives	46
10.6.1	Overview	46
10.6.2	RSAEP	46
10.6.3	RSADP	47
10.7	Asymmetric encryption schemes	49
10.7.1	Overview	49
10.7.2	RSAES-OAEP	49
10.7.3	RSAES-KEM-KWS	56
10.8	Secret-value encapsulation scheme	60
10.8.1	Overview	60
10.8.2	RSASVES1.....	61
11	Key management considerations for public and private keys	63
11.1	Overview	63
11.2	Public-key distribution.....	63
11.3	Assurance of possession of the private key associated with the public key	63
11.4	Key usage.....	63
11.5	Assurances of key pair and public-key validity	64
11.5.1	Owner assurances of key pair validity	64
11.5.2	User assurances of public-key validity	66
12	Key confirmation	67
12.1	Overview	67
12.2	Operation.....	68
12.3	MAC data	68
13	Key agreement schemes	69
13.1	Overview	69
13.2	KAS1 family: Key agreement based on secret-value encapsulation	70
13.2.1	Overview	70
13.2.2	Common components.....	70
13.2.3	kas1-basic	72
13.2.4	kas1-responder-confirmation.....	74
13.2.5	kas1-bilateral-confirmation.....	76
13.2.6	kas1-bilateral-confirmation-initiator-authentication	79
14	Key transport schemes	82
14.1	Overview	82
14.2	KTS1 family: Key transport based on asymmetric encryption.....	82
14.2.1	Overview	82
14.2.2	Common components.....	82
14.2.3	kts1-basic	84
14.2.4	kts1-receiver-confirmation	86
Annex A (normative)	Compatibility Components	89
A.1	Overview	89
A.2	US-ASCII to Octet String Primitive (ASC2OSP).....	89
A.3	PRF-TLS.....	89
A.4	RSA Signature Primitive (RSASP)	91
A.5	RSA Verification Primitive (RSVP)	91
A.6	RSAES-PKCS1-v1_5.....	92
A.6.1	Overview	92
A.6.2	Encryption operation	92
A.6.3	Decryption operation	93
A.7	RSASVES-TLS.....	95

A.7.1	Overview	95
A.7.2	Generation operation.....	95
A.7.3	Recovery operation	96
A.8	RSASSA-TLS	98
A.8.1	Overview	98
A.8.2	Signature operation	98
A.8.3	Verification operation	99
Annex B (normative)	ASN.1 Syntax	101
B.1	Overview	101
B.2	Useful types and definitions.....	101
B.3	Components from other X9 sources.....	102
B.3.1	Overview	102
B.3.2	Hash functions	102
B.3.3	Message authentication codes.....	104
B.3.4	Symmetric key-wrapping schemes.....	105
B.3.5	Signature schemes with appendix.....	106
B.4	Additional components	106
B.4.1	Overview	106
B.4.2	MGF1	106
B.4.3	KDF2.....	107
B.4.4	KDF3.....	107
B.5	Public-key components	107
B.5.1	Overview	107
B.5.2	Public and private keys	107
B.5.3	RSAES-OAEP	109
B.5.4	RSAES-KEM-KWS.....	110
B.5.5	RSASVES1.....	111
B.6	Key establishment schemes.....	111
B.6.1	Overview	111
B.6.2	KAS1 family	112
B.6.3	KTS1 family	116
B.7	Compatibility components.....	118
B.7.1	Overview	118
B.7.2	PRF-TLS	118
B.7.3	RSAES-PKCS1-v1_5	118
B.7.4	RSASVES-TLS.....	119
B.7.5	RSASSA-TLS.....	119
B.8	ASN.1 module.....	119
Annex C (informative)	Security Considerations	132
C.1	Overview	132
C.2	RSA Problem	132
C.3	Integer factoring.....	134
C.4	RSA key pairs.....	135
C.4.1	Overview	135
C.4.2	Key size.....	135
C.4.3	Prime factors	135
C.4.4	Public exponent	136
C.4.5	Private exponent.....	137
C.4.6	Private-key representation.....	137
C.5	Public-key techniques	137
C.5.1	Encryption and decryption primitives	137
C.5.2	Asymmetric encryption schemes	137
C.5.3	Secret-value encapsulation schemes.....	138
C.5.4	Signature schemes with appendix.....	139
C.6	Key establishment schemes.....	139
C.6.1	KAS1 family	141

ANSI X9.44–2007

C.6.2	KTS1 family	142
C.7	Side-channel attacks	142
C.8	Hash Functions	143
Annex D (informative)	Assurance of Validity for RSA Public Keys	144
D.1	Introduction	144
D.2	Assurance through validation	144
D.3	Motivations for checking public keys	145
D.4	Relying on other parties	146
D.5	Full public-key validation	147
Annex E (informative)	TLS Profile of KAS1 Family	149
E.1	Overview	149
E.2	TLS handshake with server authentication	149
E.3	TLS handshake with mutual authentication	152
E.4	Summary of TLS messages	153
E.5	Recommended enhancements	154
E.6	Assurance of public-key validity in TLS	155
Annex F (informative)	ANS X9.73 and S/MIME CMS Profile of KTS1 Family	156
F.1	Overview	156
F.2	kts1-basic parameters	156
F.3	Summary of protocol fields	156
F.4	Recommended enhancements	157
Annex G (informative)	Supporting Algorithms	159
G.1	Greatest common divisor	159
G.2	Least common multiple	160
G.3	Modular inverse	160
G.4	Prime factor recovery	162
G.5	Enhanced Miller-Rabin Provable Compositeness / Probabilistic Primality Test	163
Annex H (informative)	Examples	165
H.1	Example values for rsakpg1-basic	165
H.2	Example values for rsakpg1-prime-factor	167
H.3	Example Values for RSAkpg1-crt	169
H.4	Example values for RSAEP	172
H.5	Example values for RSADP	174
H.6	Example values for RSAES-OAEP.Encrypt	176
	Inputs: 176	
	Outputs	177
	Support Values	178
H.7	Example values for RSAES-KEM-KWS.Encrypt	179
	Inputs: 179	
	Outputs:	180
H.8	Example values for KAS1-basic	181
	Step 1 - Initiator	181
	Step 2 - Responder	184
	Step 3 - Initiator	186
	Support Values	186
H.9	Example values for KTS1-basic	186
	Step 1 - Sender	186
	Step 2 - Responder	188
	Support Values	189
	Bibliography	191

Figures

Figure 1: RSAES-OAEP encryption operation..... 53

Figure 2: RSAES-OAEP decryption operation..... 56

Figure 3: RSAES-KEM-KWS encryption operation 58

Figure 4: RSAES-KEM-KWS decryption operation 60

Figure 5: kas1-basic scheme 74

Figure 6: kas1-responder-confirmation scheme 76

Figure 7: kas1-bilateral-confirmation scheme..... 78

Figure 8: kas1-bilateral-confirmation-initiator-authentication scheme 81

Figure 9: kts1-basic scheme 85

Figure 10: kts1-receiver-confirmation scheme..... 88

Figure E.1: TLS handshake with server authentication, as a profile of kas1-bilateral-confirmation..... 152

Figure E.2: TLS handshake with mutual authentication, as a profile of kas1-bilateral-confirmation-initiator-authentication 153

Tables

Table 1: Recommended algorithms and minimum key sizes. 17

Table C.1: Corresponding RSA and symmetric key sizes based on GNFS running time 134

Table C.2: Security assurances provided by the key establishment schemes..... 140

Table E.1: TLS with server authentication as a profile of KAS1 150

Table E.2: Additional elements in TLS with mutual authentication, as a profile of KAS1 152

Table E.3: Proposed enhancements to TLS profile 155

Table F.1: ANS X9.73 and S/MIME CMS KeyTransRecipientInfo as a profile of kts1-basic 157

ANSI X9.44–2007

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>

Copyright © 2007 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

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

ACI Worldwide
American Bankers Association
American Financial Services Association
American Express Company
Bank of America
Certicom Corporation
Citigroup, Inc.
Clarke American Checks Inc.
CUSIP Service Bureau
Deluxe Corporation
Diebold, Inc.
Discover Financial Services
Federal Reserve Bank
First Data Corporation
Fiserv
FSTC, Financial Services Consortium
Hewlett Packard
Hypercom

Representative

James Shaffer
C. Diane Poole
Mark Zalewski
John Allen
Daniel Welch
Daniel Brown
Mike Halpern
John W. McCleary
James Taylor
John FitzPatrick
Bruce Chapa
Katie Howser
Dexter Holt
Elizabeth Lynn
Skip Smith
Daniel Schutzer
Larry Hines
Scott Spiker

ANSI X9.44-2007

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 McMahan
The Clearing House	Vincent DeSantis
U. S. Bank	Marc Morrison
University Bank	Stephen Ranzini
VECTORsgj	Ron Schultz
VeriFone	Brad McGuinness
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

3PEA Technologies, Inc.
ACI Worldwide
American Financial Services Association
Bank of America
Certicom Corporation
Citigroup, Inc.
ClearWave Electronics
CUSIP Servis Bureau
DeLap, White, Caldwell and Croy, LLP
Deluxe Corporation
Depository Trust and Clearing Corporation
Diebold, Inc.
Discover Financial Services
Entrust, Inc.
Federal Reserve Bank
Federal Reserve Bank
Ferris and Associates, Inc.
First Data Corporation
Fiserv
FSTC, Financial Services Technical Consortium
Futurex
Harland Clarke
Hewlett Packard
Hypercom
IBM Corporation
InfoGuard Laboratories

Representative

Mark Newcomer
Jim Shaffer
Mark Zalewski
Daniel Welch
Daniel Brown
Gary Word
Mark Ross
Scott Preiss
Darlene Kargel
John Fitzpatrick
Robert Palatnick
Bruce Chapa
Julie Shaw
Miles Smid
Jeannine M. DeLano
Dexter Holt
J. Martin Ferris
Rick Van Luvender
Bud Beattie
Daniel Schutzer
Jason Anderson
John McCleary
Larry Hines
Scott Spiker
Todd Arnold
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

Certicom Corporation
Certicom Corporation
Communications Security Establishment of Canada
Entrust
Entrust
HP
MasterCard
National Institute of Standards and Technology
National Institute of Standards and Technology
National Institute of Standards and Technology
National Institute of Standards and Technology

Representative

Dan Brown
Scott Vanstone
Bridget Walshe
Don Johnson
Miles Smid
Susan Langford
Mike Ward
Morris Dworkin
Elaine Barker
John Kelsey
Lily Chen

ANSI X9.44–2007

National Security Agency
National Security Agency
NTRU
Pitney Bowes, Inc
Pitney Bowes, Inc
RSA, The Security Division of EMC
RSA, The Security Division of EMC
RSA, The Security Division of EMC

Paul Timmel
Michael Boyle
William Whyte
Matt Compagna
Rick Ryan
James Randall
Steve Schmalz
Burt Kaliski

This is a preview of "ANSI X9.44-2007". [Click here to purchase the full version from the ANSI store.](#)

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.