American National Standard for Financial Services

ANSI X9.44–2007 (R2017)

Public-Key Cryptography for the Financial Services Industry

Key Establishment Using Integer Factorization Cryptography

Developed By
Accredited Standards Committee X9, Incorporated
Financial Industry Standards

Date Approved: August 24, 2007
Date Reaffirmed: February 10, 2017

American National Standards Institute

American National Standards, Technical Reports and Guides developed through the Accredited Standards Committee X9, Inc., are copyrighted. Copying these documents for personal or commercial use outside X9 membership agreements is prohibited without express written permission of the Accredited Standards Committee X9, Inc. For additional information please contact ASC X9, Inc., 275 West Street, Suite 107, Annapolis, MD 21401.
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Foreword</td>
<td>vii</td>
</tr>
<tr>
<td>Introduction</td>
<td>viii</td>
</tr>
<tr>
<td>1 Scope</td>
<td>1</td>
</tr>
<tr>
<td>2 Normative references</td>
<td>2</td>
</tr>
<tr>
<td>3 Terms and definitions</td>
<td>2</td>
</tr>
<tr>
<td>4 Symbols and abbreviated terms</td>
<td>7</td>
</tr>
<tr>
<td>5 Overview and organization</td>
<td>14</td>
</tr>
<tr>
<td>5.1 General</td>
<td>14</td>
</tr>
<tr>
<td>5.2 Compatibility modes</td>
<td>15</td>
</tr>
<tr>
<td>5.3 Organization</td>
<td>15</td>
</tr>
<tr>
<td>6 Security levels</td>
<td>16</td>
</tr>
<tr>
<td>7 Data conversion primitives</td>
<td>17</td>
</tr>
<tr>
<td>7.1 Overview</td>
<td>17</td>
</tr>
<tr>
<td>7.2 Integer to Octet String Primitive (I2OSP)</td>
<td>17</td>
</tr>
<tr>
<td>7.3 Octet String to Integer Primitive (OS2IP)</td>
<td>18</td>
</tr>
<tr>
<td>8 Components from other X9 sources</td>
<td>19</td>
</tr>
<tr>
<td>8.1 Overview</td>
<td>19</td>
</tr>
<tr>
<td>8.2 Random number (bit) generators (RNGs)</td>
<td>19</td>
</tr>
<tr>
<td>8.3 Prime number generators</td>
<td>19</td>
</tr>
<tr>
<td>8.4 Primality testing methods</td>
<td>19</td>
</tr>
<tr>
<td>8.5 Hash functions</td>
<td>20</td>
</tr>
<tr>
<td>8.6 Message authentication codes</td>
<td>20</td>
</tr>
<tr>
<td>8.7 Symmetric key-wrapping schemes</td>
<td>22</td>
</tr>
<tr>
<td>8.8 Signature schemes with appendix</td>
<td>22</td>
</tr>
<tr>
<td>9 Additional components</td>
<td>23</td>
</tr>
<tr>
<td>9.1 Overview</td>
<td>23</td>
</tr>
<tr>
<td>9.2 Mask generation functions</td>
<td>23</td>
</tr>
<tr>
<td>9.2.1 Overview</td>
<td>23</td>
</tr>
<tr>
<td>9.2.2 MGF1</td>
<td>23</td>
</tr>
<tr>
<td>9.3 Key derivation functions</td>
<td>24</td>
</tr>
<tr>
<td>9.3.1 Overview</td>
<td>24</td>
</tr>
<tr>
<td>9.3.2 KDF2/KDF3</td>
<td>25</td>
</tr>
<tr>
<td>10 Public-key components</td>
<td>27</td>
</tr>
<tr>
<td>10.1 Overview</td>
<td>27</td>
</tr>
<tr>
<td>10.2 RSA key pairs</td>
<td>27</td>
</tr>
<tr>
<td>10.3 RSA key pair generators</td>
<td>28</td>
</tr>
<tr>
<td>10.3.1 RSKPG1 family: RSA key pair generation with a fixed public exponent</td>
<td>29</td>
</tr>
<tr>
<td>10.3.2 RSKPG2: RSA key pair generation with a random public exponent</td>
<td>32</td>
</tr>
<tr>
<td>10.4 RSA key pair validation</td>
<td>35</td>
</tr>
<tr>
<td>10.4.1 Overview</td>
<td>35</td>
</tr>
<tr>
<td>10.4.2 RSKPV1: RSA Key Pair Validation with a Fixed Exponent</td>
<td>36</td>
</tr>
<tr>
<td>10.4.3 RSKPV2: RSA Key Pair Validation with a Random Exponent</td>
<td>39</td>
</tr>
<tr>
<td>10.5 Partial public-key validation and plausibility tests</td>
<td>43</td>
</tr>
<tr>
<td>10.5.1 Overview</td>
<td>43</td>
</tr>
</tbody>
</table>
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 (RSAVP) ....................................... 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
B.5.2 Public-key components ................................................................................................................... 107
B.4.4 KDF3................................................................................................................................................... 107
B.4.3 KDF2................................................................................................................................................... 107
C.6.1 KAS1 family ....................................................................................................................................... 141
C.6 Key establishment schemes ............................................................................................................ 139
C.1 Over view ............................................................................................................................................ 132
C.4 RSA key pairs .................................................................................................................................... 135
C.3 Integer factoring................................................................................................................................ 134
C.2 RSA Problem ................................................................................................................................. 132
C.4.6 Private exponent ........................................................................................................................... 137
C.4.5 Private exponent ........................................................................................................................... 137
C.4.4 Public exponent ........................................................................................................................... 136
C.4.3 Prime factors .............................................................................................................................. 135
C.4.1 Overview ........................................................................................................................................ 135
C.4.2 Key size ........................................................................................................................................ 135
C.4 RSA key pairs .................................................................................................................................... 135
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
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
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
275 West Street Suite 107
Annapolis, MD 21401 USA
X9 Online www.x9.org

Copyright © 2017 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
Steve Stevens, 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 Howsor
Dexter Holt
Elizabeth Lynn
Skip Smith
Daniel Schutzer
Larry Hines
Scott Spiker
The X9F subcommittee on Data and Information Security had the following members:

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

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

© 2017 ASC X9 Inc. - All rights reserved
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

<table>
<thead>
<tr>
<th>Organization</th>
<th>Representative</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certicom Corporation</td>
<td>Dan Brown</td>
</tr>
<tr>
<td>Certicom Corporation</td>
<td>Scott Vanstone</td>
</tr>
<tr>
<td>Communications Security Establishment of Canada</td>
<td>Bridget Walshe</td>
</tr>
<tr>
<td>Entrust</td>
<td>Don Johnson</td>
</tr>
<tr>
<td>Entrust</td>
<td>Miles Smid</td>
</tr>
<tr>
<td>HP</td>
<td>Susan Langford</td>
</tr>
<tr>
<td>MasterCard</td>
<td>Mike Ward</td>
</tr>
<tr>
<td>National Institute of Standards and Technology</td>
<td>Morris Dworkin</td>
</tr>
<tr>
<td>National Institute of Standards and Technology</td>
<td>Elaine Barker</td>
</tr>
<tr>
<td>National Institute of Standards and Technology</td>
<td>John Kelsey</td>
</tr>
<tr>
<td>National Institute of Standards and Technology</td>
<td>Lily Chen</td>
</tr>
</tbody>
</table>
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 ANSI 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.

© 2017ASC X9 Inc. - All rights reserved