



American National Standard for Financial Services

ANSI X9.98-2010 (R2017)

Lattice-Based Polynomial Public Key Establishment Algorithm for the Financial Services Industry



Accredited Standards Committee X9, Incorporated
Financial Industry Standards

Date Approved: October 15, 2010

Date Reaffirmed: February 2, 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.

This page left intentionally blank

ANSI X9.98-2010 (R2017)

Contents

Introduction.....vii

1 Scope 1

2 Conformance to this Standard 1

3 Normative References 2

4 Terms and Definitions 2

5 Symbols and Abbreviated Terms 9

6 Organization 14

6.1 Structure 14

6.2 Algorithm Specification Conventions 14

7 Security Levels 15

8 Data Types and Conversions 16

8.1 Bit Strings and Octet Strings 16

8.2 Converting Between Integers and Bit Strings (I2BSP and BS2IP) 16

8.2.1 Integer to Bit String Primitive (I2BSP) 16

8.2.2 Bit String to Integer Primitive (BS2IP) 17

8.3 Converting Between Integers and Octet Strings (I2OSP and OS2IP) 17

8.3.1 Integer to Octet String Primitive (I2OSP) 17

8.3.2 Octet String to Integer Primitive (OS2IP) 17

8.4 Converting Between Bit Strings and Right-Padded Octet Strings (BS2ROSP and ROS2BSP) ... 18

8.4.1 Bit String to Right-Padded Octet String Primitive (BS2ROSP) 18

8.4.2 Right-Padded Octet String to Bit String Primitive (ROS2BSP) 18

8.5 Converting Between Ring Elements and Octet Strings (RE2OSP and OS2REP) 19

8.5.1 Ring Element to Octet String Primitive (RE2OSP) 19

8.5.2 Octet String to Ring Element Primitive (OS2REP) 19

8.6 Converting Between Ring Elements and Bit Strings (RE2BSP and BS2REP) 20

8.6.1 Ring Element to Bit String Primitive (RE2BSP) 20

8.6.2 Bit String to Ring Element Primitive (BS2REP) 20

9 Components from other X9 sources 21

9.1 Overview 21

9.2 Random number (bit) generators 21

9.3 Hash functions 21

9.4 Message authentication codes 22

10 Polynomial representation and operations 23

10.1 Introduction 23

10.2 Polynomial representation 23

10.3 Polynomial operations 23

10.3.1 Polynomial multiplication 23

10.3.2 Reduction of a Polynomial mod q 23

10.3.3 Inversion in $(\mathbb{Z}/q\mathbb{Z})[X]/(X^N - 1)$ 23

11 Cryptographic Building Blocks 25

11.1 Introduction 25

11.2 Components 26

11.2.1 Parameters 26

11.2.2 Primitives 28

11.2.3 Encoding Methods 28

11.2.4 Supporting Algorithms 28

11.3 Primitives 29

11.3.1 Key Generation Primitives 29

ANSI X9.98-2010 (R2017)

11.3.2	Encryption Primitives	30
11.3.3	Decryption Primitives	31
11.4	Encoding Methods	31
11.4.1	Blinding Polynomial Generation Methods (BPGM)	32
11.5	Supporting Algorithms.....	32
11.5.1	Hash Functions	32
11.5.2	Mask Generation Functions.....	33
11.5.3	Index generation function	34
12	Short Vector Encryption Scheme (SVES).....	37
12.1	Encryption Scheme (SVES) Overview	37
12.2	Encryption Scheme (SVES) Operations	37
12.2.1	Key Generation.....	37
12.2.2	Encryption Operation	37
12.2.3	Decryption Operation	40
12.3	Supported Parameter Sets	43
12.3.1	Size-Optimized	43
12.3.2	Cost-Optimized	45
12.3.3	Speed-Optimized	47
13	Key management considerations for public and private keys.....	50
13.1	Overview	50
13.2	Public key distribution	50
13.3	Key usage	50
13.4	Assurances of key pair and public-key validity	51
13.4.1	Owner assurances of key pair validity	51
13.4.2	User assurances of public-key validity	52
13.4.3	Key Pair Validation Methods.....	53
13.4.4	Public-key validation	54
13.4.5	Partial public-key validation and plausibility tests.....	54
14	Key confirmation	55
14.1	Overview	55
14.2	Operation	55
14.3	MAC data	56
15	Key transport schemes	58
15.1	Overview	58
15.2	KTS1 family: Key transport based on asymmetric encryption	58
15.2.1	Overview.....	58
15.2.2	Common components.....	58
15.2.3	kts1-basic.....	59
15.2.4	kts1-receiver-confirmation	60
Annex A	(Normative) ASN.1 Syntax	62
A.1	General Types.....	62
A.1.1	General Vector Types	62
A.2	Object Identifiers	63
A.3	ASN.1 for SVES	63
A.3.1	LBP-PKE Public Keys	63
A.3.2	LBP-PKE Private Keys.....	64
A.3.3	LBP-PKE Encrypted Data	65
A.3.4	LBP-PKE Parameters	65
A.4	ASN.1 Module	66
Annex B	(normative) Random Number Generation.....	69
B.2	A DRBG Using Any Approved Hash Function	69
B.2.1	Overview	69
B.2.2	Derivation Function (<i>Hash_df</i>)	69

ANSI X9.98-2010 (R2017)

B.2.3	Instantiation of the <i>Hash_DRBG</i>	69
B.2.4	Reseeding a <i>Hash_DRBG</i> Instantiation.....	71
B.2.5	Pseudorandom Bit Generation Using the <i>Hash_DRBG</i>	72
Annex C	(Informative) Security Considerations	75
C.1	Lattice Security: Background	75
C.1.1	Lattice Definitions.....	75
C.1.2	Hard Lattice Problems.....	75
C.1.3	Theoretical Complexity of Hard Lattice Problems.....	76
C.1.4	Lattice Reduction Algorithms	76
C.1.5	The Gaussian Heuristic and the Closest Vector Problem.....	77
C.1.6	Modular Lattices: Definition.....	77
C.1.7	Modular Lattices and Quotient Polynomial Rings	77
C.1.8	Balancing CVP in Modular Lattices.....	78
C.1.9	Fundamental CVP Ratios in Modular Lattices	78
C.1.10	Creating a Balanced CVP for Modular Lattices Containing a Short Vector	79
C.1.11	Modular Lattices Containing (Short) Binary Vectors	79
C.1.12	Convolution Modular Lattices	80
C.1.13	Heuristic Solution Time for CVP in Modular Lattices.....	80
C.1.14	Zero-forcing.....	81
C.2	Experimental Solution Times for NTRU lattices – full key recovery	81
C.2.1	Experimental Solution Times for NTRU lattices using BKZ reduction	81
C.2.2	Alternative Target Vectors.....	83
C.3	Combined Lattice and Combinatorial Attacks on LBP-PKE Keys and Messages.....	83
C.3.1	Overview	83
C.3.2	Lattice Strength	83
C.3.3	Reduced lattices and the “cliff”	84
C.3.4	Combinatorial Strength	87
C.3.5	Summary.....	89
C.4	Other Security Considerations for LBP-PKE Encryption	89
C.4.1	Entropy Requirements for Key and Salt Generation.....	89
C.4.2	Reduction mod q	89
C.4.3	Selection of N	89
C.4.4	Relationship between q and N	89
C.4.5	Form of q	89
C.4.6	Leakage of $m'(1)$	90
C.4.7	Relationship between p , q and N	90
C.4.8	Adaptive Chosen Ciphertext Attacks	90
C.4.9	Invertibility of g in R_q	91
C.4.10	Decryption Failures.....	91
C.4.11	OID.....	91
C.4.12	Use of Hash Functions by Supporting Functions	92
C.4.13	Generating Random Numbers in $[0, N-1]$	92
C.4.14	Attacks based on variation in decryption times	92
C.4.15	Choosing to attack r or m	93
C.4.16	Quantum Computers	93
C.4.17	Other Considerations.....	93
C.5	Security levels of Parameter Sets in this Standard.....	93
C.5.1	Assumed security levels versus current knowledge	93
C.5.2	Potential research	94
Annex D	(normative) A Parameter Set Generation Algorithm	94
Annex E	(Informative) Security attributes of the schemes in this standard	95
Annex F	(Informative) Comparison of key sizes	96
Annex G	(Informative) Test Vectors	97

G.1	ees401ep1	97
G.2	ees449ep1	105
G.3	ees677ep1	114
G.4	ees1087ep2	127
G.5	ees541ep1	147
G.6	ees613ep1	157
G.7	ees887ep1	168
G.8	ees1171ep1	184
G.9	ees659ep1	206
G.10	ees761ep1	218
G.11	ees1087ep1	232
G.12	ees1499ep1	251
Annex H	(Informative) Bibliography	278

Flows

Figure 1: Encryption Operation	39
Figure 2: kts1-basic scheme	59
Figure 3: kts1-receiver-confirmation scheme.....	61
Figure 4: Lattice Breaking Times and Linear Extrapolations	82
Figure 5: Time to remove x q vectors by different lattice reduction techniques, experimentally determined.	84
Figure 6 Lattice Profiles	85
Figure 7 The attacker's view of the lattice following reduction	86
Figure 8: A case where Babai reduction will not be successful	86

Tables

Table 1 – Recommended algorithms and parameter sets	15
Table 2: X9-approved hash functions (as of publication of this Standard)	22
Table 3: X9-approved message authentication codes (as of publication of this Standard).....	22
Table 4 – ees401ep1	43
Table 5 – ees449ep1	43
Table 6 – ees677ep1	44
Table 7 – ees1087ep2	45
Table 8 – ees541ep1	45
Table 9 – ees613ep1	46
Table 10 – ees887ep1	46
Table 11 – ees1171ep1	47
Table 12 – ees659ep1	48
Table 13 – ees761ep1	48
Table 14 – ees1087ep1	49
Table 15 – ees1499ep1	49
Table 16 – Approved additional components for key confirmation in the KTS1 family.....	60
Table A.1 — Security Level that that may be provided by each hash function	69
Table 2 – Lattice Security.....	82
Table 3 Assumptions used to generate parameters in this standard vs current best known attacks.....	94
Table 4 Strengths of recommended parameter sets in this standard vs best current attacks.....	94

Algorithms

Algorithm 1 – I2BSP.....	16
Algorithm 2 – BS2IP.....	17
Algorithm 3 – I2OSP	17
Algorithm 4 – OS2IP	18
Algorithm 5 – BS2ROSP	18

ANSI X9.98-2010 (R2017)

Algorithm 6 – ROS2BSP	18
Algorithm 7 – RE2OSP	19
Algorithm 8 – OS2REP	19
Algorithm 9 – RE2BSP	20
Algorithm 10 – BS2REP	20
Algorithm 11 – Polynomial Division Algorithm in $Z_p[X]$	23
Algorithm 12 – Extended Euclidean Algorithm in $Z_p[X]$	24
Algorithm 13 – Inverses in $Z_p[X]/(XN - 1)$	25
Algorithm 14 – Inverses in $Z_p[X]/(XN - 1)$	25
Algorithm 15 – Random Key Generation Primitive kgp-3	30
Algorithm 16 – Encryption Primitive	31
Algorithm 17 – Decryption Primitive	31
Algorithm 18 – Blinding Polynomial Generation From dr	32
Algorithm 19 – Mask Generation Function for Trinary Polynomials (MGF-TP-1).....	33
Algorithm 20 – Index generation function (IGF-2).....	34
Algorithm 21 – Index generation function (IGF-RBG).....	36
Algorithm 22 – Key Generation	37
Algorithm 23 – Encryption Operation	37
Algorithm 24 – Decryption Operation	40
Algorithm 25 – kpv3, Key Pair Validation for Trinary Keys	53

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 <http://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.

ANSI X9.98-2010 (R2017)

Introduction

This Standard specifies key establishment techniques using public-key cryptography based on the problems of finding short vectors or close vectors in a lattice. The keying material established may be used to obtain one or more individual keys used to provide other cryptographic services outside the scope of this Standard, e.g. data confidentiality, data integrity, or symmetric-key-based key establishment

There are two primary reasons to consider the use of the techniques in this Standard:

1. The techniques are based on a different hard problem than other X9 approved public key algorithms. If the integer factorization problem, the finite field discrete logarithm problem and the elliptic curve discrete logarithm problem were all to be broken (for example, by the realization of a quantum computer of sufficient size), this method might remain unbroken.
2. The techniques may have performance advantages in some environments, provided that the stated security levels for domain parameters and key sizes specified herein are accurate.

The techniques described in this Standard were developed more recently than the techniques described in other X9 standards that use public key cryptography. As such, although this standard reflects the state of the art in knowledge about the security of these techniques, they may be considered to face a greater risk than other public key techniques that improved attacks will be discovered. Implementers who are considering implementing this system should determine for themselves how to balance this potentially greater risk with the benefits described above.

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, 275 West Street, Suite 107, Annapolis, MD 21401 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 this standard was approved, the X9 committee had the following members:

Roy CeCicco, X9 Chairman
 Vincent DeSantis, X9 Vice-Chairman
 Steve Stevens, Executive Director
 Janet Busch, Program Manager

Organization Represented	Representative
ACI Worldwide	Doug Grote
ACI Worldwide	Cindy Rink
American Bankers Association	Tom Judd
American Bankers Association	C. Diane Poole
American Express Company.....	Ted Peirce
Apriva	Len Sutton
BAFT/IFSA	Dexter Holt
BAFT/IFSA	Joseph Pawelczyk
BAFT/IFSA	Dan Taylor

ANSI X9.98-2010 (R2017)

Bank of America	Andi Coleman
Bank of America	Jeff Stapleton
Bank of America	Daniel Welch
Certicom Corporation	Daniel Brown
Citigroup, Inc.	Michael Knorr
Citigroup, Inc.	Karla McKenna
Citigroup, Inc.	Chii-Ren Tsai
CUSIP Service Bureau.....	Gerard Faulkner
CUSIP Service Bureau.....	James Taylor
Deluxe Corporation	John FitzPatrick
Deluxe Corporation	Deb Lynch
Deluxe Corporation	Ralph Stolp
Diebold, Inc.	Bruce Chapa
Diebold, Inc.	Anne Konecny
Federal Reserve Bank	Deb Hjortland
Federal Reserve Bank	Claudia Swendseid
First Data Corporation.....	Todd Nuzum
First Data Corporation.....	Rick Van Luvender
Fiserv.....	Bud Beattie
Fiserv.....	Kevin Finn
Fiserv.....	Lori Hood
Fiserv.....	Dan Otten
Fiserv.....	Skip Smith
FIX Protocol Ltd	Jim Northey
Harland Clarke	John McCleary
Hewlett Packard	Larry Hines
Hewlett Packard	Gary Lefkowitz
IBM Corporation	Todd Arnold
Independent Community Bankers of America	Viveca Ware
Independent Community Bankers of America	Cary Whaley
Ingenico.....	Steve McKibben
Ingenico.....	John Spence
ISITC	Tara Gonzales
J.P. Morgan Chase & Co	Robert Blair
J.P. Morgan Chase & Co	Roy DeCicco
J.P. Morgan Chase & Co	Edward Koslow
J.P. Morgan Chase & Co	Kathleen Krupa
J.P. Morgan Chase & Co	Jackie Pagan
J.P. Morgan Chase & Co	Charita Wamack
Key Innovations.....	Scott Spiker
Key Innovations.....	Paul Walters
KPMG LLP	Mark Lundin
MagTek, Inc.	Terry Benson
MagTek, Inc.	Jeff Duncan
MagTek, Inc.	Mimi Hart
MasterCard International.....	Mark Kamers
Merchant Advisory Group	Dodd Roberts
Metavante Image Solutions.....	Stephen Gibson-Saxty
National Association of Convenience Stores	Michael Davis
National Association of Convenience Stores	Alan Thiemann
National Security Agency	Paul Timmel
NCR Corporation.....	David Norris
NCR Corporation.....	Steve Stevens
RMG-SWIFT.....	Jamie Shay
RouteOne	Mark Leonard
SWIFT/Pan Americas.....	Jean-Marie Eloy

ANSI X9.98-2010 (R2017)

SWIFT/Pan Americas.....	James Wills
Symantec Corporation	Alex Deacon
Symcor Inc.	Brian Salway
TECSEC Incorporated	Ed Scheidt
The Clearing House	Vincent DeSantis
The Clearing House	Sharon Jablon
U.S. Bank	Brian Fickling
U.S. Bank	Gregg Walker
University Bank	Stephen Ranzini
University Bank	Michael Talley
USDA Food and Nutrition Service	Kathy Ottobre
VeriFone, Inc.....	David Ezell
VeriFone, Inc.....	Dave Faoro
VeriFone, Inc.....	Allison Holland
VeriFone, Inc.....	Doug Manchester
VeriFone, Inc.....	Brad McGuinness
VeriFone, Inc.....	Brenda Watlington
VISA	Brian Hamilton
VISA	John Sheets
VISA	Kim Wagner
Wells Fargo Bank.....	Andrew Garner
Wells Fargo Bank.....	Mike McCormick
Wells Fargo Bank.....	Mike Rudolph
Wells Fargo Bank.....	Mark Tiggas
Wincor Nixdorf Inc.....	Ramesh Arunashalam
XBRL US, Inc.	Mark Bolgiano

The X9F Subcommittee on Information Security had the following members:

Organization Represented	Representative
American Bankers Association	Tom Judd
Bank of America.....	Andi Coleman
Certicom Corporation	Daniel Brown
Citigroup, Inc.	Dr. Chii-Ren Tsai
Communications Security Establishment.....	Alan Poplove
Cryptographic Assurance Services	Ralph Poore
CUSIP Service Bureau.....	Scott Preiss
DeLap LLP	Darlene Kargel
Deluxe Corporation	John Fitzpatrick
Depository Trust and Clearing Corporation	Robert Palatnick
Diebold, Inc.	Bruce Chapa
Discover Financial Services	Jordan Schaefer
Entrust, Inc.	Miles Smid
Federal Reserve Bank	Deb Hjortland
Ferris and Associates, Inc.	Martin J. Ferris
First Data Corporation.....	Lisa Curry
Fiserv.....	Bud Beattie
GEOBRIDGE Corporation.....	Jason Way
Harland Clarke	John Petrie
Heartland Payment Systems.....	Glenda Preen
Hewlett Packard	Larry Hines
Hypercom	Gary Zempich
IBM Corporation	Todd Arnold
InfoGard Laboratories	Doug Biggs

ANSI X9.98-2010 (R2017)

Ingenico.....	John Spence
ITS, Inc. (SHAZAM Networks)	Manish Nathwani
J.P. Morgan Chase & Co	Edward Koslow
Key Innovations.....	Scott Spiker
KPMG LLP	Mark Lundin
MasterCard International.....	Michael Ward
Merchant Advisory Group	Dodd Roberts
Merchant Link.....	Scott Franklin
National Institute of Standards and Technology	Elaine Barker
National Security Agency	Paul Timmel
NCR Corporation.....	David Norris
Pitney Bowes, Inc.....	Rick Ryan
RBS Group.....	Dan Collins
Rosetta Technologies	Jim Maher
Rosetta Technologies	Paul Malinowski
Security Innovation.....	William Whyte
STAR.....	Lilik Kazaryan
Surety, Inc.	Dimitrios Andivahis
Symcor Inc.	Brian Salway
TECSEC Incorporated	Ed Scheidt
Thales e-Security, Inc.	James Torjussen
The Clearing House	Vincent DeSantis
Trustwave.....	John Amaral
Unisys Corporation.....	David J. Concannon
University Bank	Stephen Ranzini
VeriFone, Inc.....	Dave Faoro
Voltage Security, Inc.	Luther Martin
Wells Fargo Bank.....	Mark Tiggas
Wincor Nixdorf Inc.....	Michael Nolte

The X9F1 Working Group on Applications Security had the following members:

Terence Spies, Voltage Security, Inc., Chairman

Organization Represented	Representative
American Bankers Association	Tom Judd
Bank of America.....	Andi Coleman
Certicom Corporation.....	Daniel Brown
Communications Security Establishment.....	Bridget Walshe
Cryptographic Assurance Services.....	Ralph Poore
Entrust, Inc.	Miles Smid
Hewlett Packard	Susan Langford
Hypercom.....	Mohammad Arif
IBM Corporation	Todd Arnold
InfoGard Laboratories	Doug Biggs
MasterCard International.....	Michael Ward
National Institute of Standards and Technology	Elaine Barker
National Security Agency	Mike Boyle
RSA, The Security Division of EMC.....	Steve Schmalz
Security Innovation.....	William Whyte
Voltage Security, Inc.	Terence Spies

ANSI X9.98-2010 (R2017)

Lattice-Based Polynomial Public Key Encryption Algorithm for the Financial Services Industry, Part 1: Key Establishment

1 Scope

This Standard specifies the cryptographic functions for establishing symmetric keys using a lattice-based polynomial public key encryption algorithm and the associated parameters for key generation (see Note 1). The mechanism supported is *key transport*, where one party selects keying material and conveys it to the other party with cryptographic protection. The keying material may consist of one or more individual keys used to provide other cryptographic services outside the scope of this Standard, e.g. data confidentiality, data integrity, or symmetric-key-based key establishment. The standard also specifies key pair generators and corresponding key pair validation methods supporting the key transport schemes (see Note 2).

This standard does not address the distribution of the public and private keys, associated parameters and other keying material. The integrity and authenticity of the public key and its associated parameters is outside the scope of this standard, and are assumed to be securely managed using the appropriate X9 standards. The confidentiality of the private key and its associated parameters is outside the scope of this standard, and are assumed to be securely managed using the appropriate X9 standards.

This version of the Standard is limited to a small number of possible lattice-based polynomial public key establishment schemes and key pair generators and validation methods. Future versions may include additional schemes with different attributes (see Note 3).

NOTE: 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 generation method. A *public-key validation method* determines whether a candidate public key meets those constraints, without knowledge of the private key. Full public-key validation methods are not specified in this version of the Standard, but are expected to be developed in future X9 work.

2 Conformance to this Standard

An implementation may claim conformance with this Standard if it implements at least one key pair generator, public key validation, or key transport scheme in this Standard with at least one approved set of parameters. An implementation claiming conformance with this Standard shall indicate the specific techniques with which conformance is claimed and the parameter sets for which conformance is claimed.

Key pair generators with which conformance may be claimed are: lbp-kgp-3 (see section 11.3.1.1).

Key transport mechanisms with which conformance may be claimed are: kts1-basic (see section 15.2.3) and kts1-receiver-confirmation (see section 15.2.4).

Key pair validation mechanisms with which conformance may be claimed are: kpv3 (see section 13.4.3.1).

Public key validation mechanisms with which conformance may be claimed are described in section 13.4.5.2.

Parameter sets with which conformance may be claimed are: ees401ep1, ees541ep1, ees659ep1, ees449ep1, ees613ep1, ees761ep1, ees677ep1, ees887ep1, ees1087ep1, ees1087ep2, ees1171ep1, ees1499ep1.