Retired Draft

Warning Notice

The attached draft document has been RETIRED. NIST has discontinued additional development of this document, which is provided here in its entirety for historical purposes.

Retired Date April 23, 2012

Original Release Date February 10, 2011

Retired Document

Status	Initial Public Draft (IPD)
Series/Number	NIST Special Publication 800-131C
Title	Transitions: Validating the Transition from FIPS 186-2 to FIPS 186-3
Publication Date	February 2011
Additional Information	The guidance in this draft was moved to FIPS 140-2 Implementation Guidance W.2.

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Special Publication 800-131C

Transitions: Validating the Transition from FIPS 186-2 to FIPS 186-3

Elaine Barker, Allen Roginsky, Randall Easter and Sharon Keller

Computer Security Division
Information Technology Laboratory

C O M P U T E R S E C U R I T Y

February 2011

U.S. Department of Commerce
Gary Locke, Secretary
National Institute of Standards and Technology
Patrick Gallagher, Director

Abstract

Federal Information Processing Standard (FIPS) 186-3 [FIPS 186-3], *Digital Signature Standard*, was approved in June, 2009 to replace FIPS 186-2 [FIPS 186-2]. This transition plan addresses both the cryptographic algorithm validations and the cryptographic module validations that are conducted by the Cryptographic Algorithm Validation Program (CAVP) and the Cryptographic Module Validation Program (CMVP), respectively.

Key Words: Cryptographic Algorithm Validation Program (CAVP), Cryptographic Module Validation Program (CMVP), digital signature standard, validation testing.

Authority

This publication has been developed by the National Institute of Standards and Technology (NIST) in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347.

NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems.

This Recommendation has been prepared for use by federal agencies. It may be used by non-governmental organizations on a voluntary basis and is not subject to copyright. (Attribution would be appreciated by NIST.)

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official.

Conformance testing for implementations of this Recommendation will be conducted within the framework of the Cryptographic Algorithm Validation Program (CAVP) and the Cryptographic Module Validation Program (CMVP). The requirements of this Recommendation are indicated by the word "shall." Some of these requirements may be out-of-scope for CAVP or CMVP validation testing, and thus are the responsibility of entities using, implementing, installing or configuring applications that incorporate this Recommendation.

Table of Contents

Transitions: Validating the Transition from FIPS 186-2 to FIPS 186-3

1 Introduction

Federal Information Processing Standard (FIPS) 186-3 [FIPS 186-3], *Digital Signature Standard*, was approved in June, 2009 to replace FIPS 186-2 [FIPS 186-2]. [FIPS 186-2] specified the Digital Signature Algorithm (DSA) for the generation and verification of digital signatures, and adopted American National Standard (ANS) X9.31 [X9.31] for the generation and verification of digital signatures using the RSA algorithm, and ANS X9.62 [X9.62] for the generation and verification of digital signatures using the Elliptic Curve Digital Signature Algorithm (ECDSA). Two additional techniques for the generation and verification of digital signatures using RSA were approved in FIPS 140-2, Annex A [Annex A]: RSASSA-PKCS1-v1_5 and RSASSA-PSS; both are specified in Public Key Cryptography Standard (PKCS) #1, version 2.1 [PKCS1], *RSA Cryptography Standard*.

[FIPS 186-3] includes the DSA specification from [FIPS 186-2], and adopts the RSA techniques specified in [X9.31] and PKCS #1 [PKCS1] (i.e., RSASSA-PKCS1-v1.5 and RSASSA-PSS) and ECDSA as specified in [X9.62]. [FIPS 186-3] also increases the key lengths allowed for DSA, provides additional requirements for the use of RSA and ECDSA, and includes requirements for obtaining the assurances necessary for valid digital signatures and new methods for generating key pairs and domain parameters. While [FIPS 186-2] contained specifications for random number generators (RNGs), [FIPS 186-3] does not include such specifications, but refers to National Institute of Standards and Technology (NIST) Special Publication (SP) 800-90 [SP 800-90] for obtaining random bits.

This transition plan addresses both the cryptographic algorithm validations and the cryptographic module validations that are conducted by the Cryptographic Algorithm Validation Program (CAVP) and the Cryptographic Module Validation Program (CMVP), respectively.

2 Validation Testing

2.1 CAVP Validation

The CAVP is transitioning from the validation of cryptographic algorithms and key lengths conforming to FIPS 186-2 to the validation of cryptographic algorithms and key lengths conforming to FIPS 186-3. Some algorithm functions specified in [FIPS 186-2]

will continue to be validated by the CAVP. The transition of the use of particular key lengths for digital signature generation is addressed in SP 800-131A [SP 800-131A], and the validation of algorithms and modules using these key lengths is addressed in SP 800-131B [SP 800-131B].

The CAVP is currently testing the following digital signature-specific functions for both [FIPS 186-2] and [FIPS186-3]; the validation of auxiliary functions (e.g., hash functions and RNGs) is discussed in [SP 800-131B], with reference to [SP 800-131A].

- DSA: domain parameter generation and validation, key pair generation, public key validation, and digital signature generation and validation.
- ECDSA: key pair generation, public key validation, and digital signature generation and verification; only the NIST-recommended curves are used as domain parameters for testing ECDSA.
- RSA: key pair generation, public key validation, and digital signature generation and verification; RSA has no domain parameters.

The parameter sets that can be tested for DSA, ECDSA and RSA are presented in the following table, along with an indication of the applicable standard (FIPS 186-2 or FIPS 186-3). For DSA, the key length is commonly considered to be the value of *L*. For ECDSA, the key length is considered to be the bit length of *n*. For RSA, the key length is considered to be *nlen*, which is the length of the modulus.

<table>
<tr><th rowspan="2">DSA
($L = |p|$, $N = |q|$)</th><th rowspan="2">ECDSA
(q, FR, a, b{, $seed$}, G, n, h)</th><th colspan="2">RSA</th></tr>
<tr><th>Modulus length
($nlen = |n|$)</th><th>Public exponent value (e)</th></tr>
<tr><td>L = 1024, N = 160
Both 186-2 and 186-3</td><td rowspan="6">All NIST-recommended curves

Both 186-2 and 186-3</td><td>$nlen$ = 1024
Both 186-2 and 186-3</td><td rowspan="6">186-2:
e = 3, 17, $2^{16} + 1$

186-3:
$2^{16}+1 \le e < 2^{256}$, where e is odd</td></tr>
<tr><td>L = 2048, N = 224
186-3 only</td><td>$nlen$ = 1536
186-2 only</td></tr>
<tr><td>L = 2048, N = 256
186-3 only</td><td>$nlen$ = 2048
Both 186-2 and 186-3</td></tr>
<tr><td>L = 3072, N = 256
186-3 only</td><td>$nlen$ = 3072
Both 186-2 and 186-3</td></tr>
<tr><td></td><td>$nlen$ = 4096
186-2 only</td></tr>
</table>

The CAVP also provides algorithm validation testing for the random number generators (RNGs) approved via FIPS 140-2, Annex C [Annex C].

2.2 CMVP Validation

The CMVP is transitioning from the validation of cryptographic modules that incorporate digital signature processes as specified in [FIPS 186-2] to modules that incorporate digital signature processes as specified in [FIPS 186-3]. For some digital signature functions specified in [FIPS 186-2] and the RNGs in [Annex C], the CMVP will continue to validate these functions for use in a FIPS 140-2-approved mode of operation.

3 Validation Transition Plan

The validation transition plan is as follows:

1. Conformance to FIPS 186-3:

    a. Effective June 2009 through December 31, 2013: Cryptographic algorithms and modules that conform to [FIPS 186-3] (or parts of [FIPS 186-3) may be submitted for validation by the Cryptographic and Security Testing (CST) Laboratories to the CAVP or CMVP. An example of an implementation that conforms to only part of [FIPS 186-3 might be an implementation that p[erforms key generation but does not perform key pair generation.

    CAVP: Cryptographic algorithm implementations conforming to [FIPS 186-3] or parts of [FIPS 186-3] may be validated by the CAVP, when testing is supported. If CAVP testing is not available, Section A.6 of the *Implementation Guidance for FIPS PUB 140-2 and the CMVP* [IG A.6] addresses vendor affirmation requirements. The testable key lengths are those associated with the parameter sets listed in the above table for [FIPS 186-3]. Only implementations of those testable key lengths that are classified as either acceptable or deprecated in [SP 800-131A] may be validated for domain parameter generation, key pair generation and digital signature generation. Implementations of domain parameter validation, public key validation and digital signature verification may be validated at any testable key length.

    CMVP: Cryptographic modules containing implementations conforming to [FIPS 186-3] or parts of [FIPS 186-3] may be validated by the CMVP if the process has been validated by the CAVP, or if the process is vendor-affirmed under [IG A.6].

    b. Effective January 1, 2014:

    CAVP: Implementations conforming to [FIPS 186-3] that contain testable key lengths that are classified as either acceptable or legacy-use as specified in [SP 800-131A] may be validated.

    CMVP: Cryptographic modules containing implementations conforming to [FIPS 186-3] may be validated by the CMVP if the process has a valid certificate issued by the CAVP, or if the process is vendor-affirmed under [IG A.6].

2. Conformance to FIPS 186-2:
    a. Through December 31, 2013, cryptographic algorithm and module implementations that perform domain parameter generation, key pair generation and digital signature generation as specified in [FIPS 186-2] may be submitted by the CST Laboratories to the CAVP or CMVP for validation.

       CAVP: New algorithm implementations and already-validated, but modified algorithm implementations conforming to [FIPS 186-2] may be submitted for validation for those testable key lengths that are classified as either acceptable, deprecated or legacy-use in [SP 800-131A].

       CMVP: New module implementations and already-validated module implementations containing digital signature processes conforming to [FIPS 186-2] that have a valid certificate issued by the CAVP may be validated or revalidated, as appropriate.

    b. After December 31, 2013, implementations of domain parameter *generation*, key pair *generation* and digital signature *generation* as specified in [FIPS 186-2] for the testable key lengths that are *disallowed* per [SP 800-131A] will not be accepted by the CAVP or CMVP for validation. As time and resources permit, the following additional actions will be taken by the CAVP or CMVP for already-validated implementations of these functions:

       CAVP: An algorithm validation listing for already-validated implementations that contain a testable key length that is disallowed will be annotated to indicate the key length that is disallowed. If an already-validated implementation only supports a testable key length that is disallowed, the algorithm validation will be revoked.

       CMVP: For already-validated modules:
        - If an algorithm validation listing has been annotated to disallow a key length (i.e., only part of a validation is disallowed), the module's CMVP validation certificate will not be changed.
        - If an algorithm validation certificate is revoked by the CAVP, the module's CMVP validation certificate will be updated to remove the algorithm's listing from the approved-algorithms line of the certificate.

    c. After December 31, 2013, cryptographic algorithm and module implementations that perform domain parameter *validation*, public key *validation* and digital signature *verification* as specified in [FIPS 186-2]

using testable key lengths may be submitted by the CST Laboratories to the CAVP or CMVP for validation or revalidation, as appropriate.

d. After December 31, 2013, cryptographic algorithm and module implementations that were validated against [FIPS 186-2] will continue to be valid, subject to the requirements for appropriate security strengths and usage for digital signature generation or verification, as discussed in [SP 800-131A]. For example, the validation of implementations that provide security strengths of 112 bits or more will continue to be valid and operable in a FIPS 140-2-approved mode of operation for the *generation* of digital signatures after the end of the deprecation period specified in [SP 800-131A], but those that provide only 80 bits of security will not be valid or operable in a FIPS 140-2-approved mode of operation beyond the "disallowed" date specified in [SP 800-131A]. However, the *verification* of digital signatures that provided 80 bits of security when generated will continue to be approved for legacy use; therefore, an implementation that verifies digital signatures at a security strength of 80 bits or more will continue to be valid, providing that it **does not** *generate* digital signatures at less than 112 bits of security in a FIPS 140-2 approved mode of operation.

3. Disallowed key lengths: Even though a key length is disallowed for generating digital signatures, interoperability with legacy devices may need to be considered until such devices can be replaced. For example, devices or applications may need to include a disallowed key length for use during a transition period to stronger key lengths. The implementations using these disallowed key lengths should be tested to provide assurance that they are implemented correctly. Previously-validated implementations have already been tested; however, any new implementations should also be tested.

   The testing of new implementations of disallowed key lengths for digital signature generation may be performed by the CST laboratories independently from CAVP validation testing using test tools previously provided for validation testing. The test results should not be submitted to the CAVP for validation.

Appendix A: Definitions

Already-validated implementations:

Already-Validated Implementations are algorithm or module implementations that have already been tested by a CST laboratory and validated by the CAVP and/or CMVP. As time and resources permit, the CAVP and CMVP will review these implementations and the underlying algorithm validations for compliance with [SP 800-131A] when a transition date occurs.

- The CAVP will review the algorithm validation to determine if [SP 800-131A] disallows either a part of the validation or the complete validation. If only part of a validation is disallowed (i.e., one of the tested key lengths is no longer allowed), the disallowed key length will be removed from the algorithm-validation list, or annotated as disallowed. If a complete algorithm validation only supports a disallowed key length, the CAVP will revoke the algorithm validation. Revoked or removed references will continue to be available for historical purposes.
- A CMVP-validated cryptographic module is required to include at least one approved cryptographic algorithm implementation that is an algorithm with a CAVP validation, an algorithm for which a standard may not have existed at the time of the CMVP validation, or an algorithm for which CAVP validation testing was not available at the time of the module validation.

  The CMVP will review the list of module validations and take the appropriate actions, based on the module's referenced algorithm validations. If an algorithm validation is revoked by the CAVP, the reference to the module's validation reference to the revoked algorithm validation will be changed to **non-approved**. References to revised algorithm validations will remain unchanged. References to **non-approved** algorithms will be changed only if sufficient information was provided that would allow modification. The information provided at the time of module validation and presented on the validation-list entry may be insufficient to determine whether a module continues to satisfy all of the new security requirements or whether the module's validation continues to be valid. It is the user's responsibility to determine that the algorithms and keys lengths utilized by their system are in compliance with the requirements of SP 800-131A.

  Note: As appropriate, the CMVP will only modify the module validation entry information; the Security Policy provided with each module validation will not be modified.

Approved: FIPS-**approved** or NIST-recommended.

New implementations (from SP 800-131B):

The term "new implementations" refers to the cryptographic algorithms or modules that have not been validated by the CAVP or CMVP, respectively. For algorithm implementations, new implementations are the algorithm implementations that are to be

tested or are currently under test by an accredited CST laboratory for which the algorithm test results will be submitted to the CAVP. For cryptographic modules, new implementations refer to cryptographic modules that are either new modules or the revalidation of modules where less than 30% of security-relevant mechanisms have changed. These modules are either not yet tested, or are currently under test by an accredited CST laboratory for which the test report will be submitted to CMVP under [IG G.8], validation Scenarios 3 and 5. When applied to cryptographic algorithms, the dates in the tables of SP 800-131A refer to the algorithm's validation date that is assigned by the CAVP. When applied to cryptographic modules, the dates in the tables of SP 800-131A refer to the dates of the CST laboratory's initial submission of a module test report to the CMVP for a new module implementation. Security policies for new module implementations **shall** include information about any transitions that may occur in the future by a reference to SP 800-131A.

Appendix B: References

[Annex A] Annex A of [FIPS 140-2]: Approved Security Functions; available at http://csrc.nist.gov/groups/STM/cmvp/standards.html.

[Annex C] Annex C of [FIPS 140-2]: Approved Random Number Generators, http://csrc.nist.gov/groups/STM/cmvp/standards.html.

[FIPS 186-2] Federal Information Processing Standard 186-2, Digital Signature Standard (DSS); January 2000; now withdrawn, but available at http://csrc.nist.gov/publications/PubsFIPSArch.html.

[FIPS 186-3] Federal Information Processing Standard 186-2, Digital Signature Standard (DSS); June 2009; available at http://csrc.nist.gov/publications/PubsFIPS.html.

[IG A.6] and [IG G.8] Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program; December 2010; available at http://csrc.nist.gov/groups/STM/cmvp/standards.html.

[PKCS1] Public Key Cryptography System #1, v2.1, RSA Cryptography System, June 14, 2002.

[SP 800-90] NIST SP 800-90,Recommendation for Random Number Generation Using Deterministic Random Bit Generators; May 2007; available at http://csrc.nist.gov/publications/PubsSPs.html.

[SP 800-131A] NIST SP 800-131A, Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths; January 2011; http://csrc.nist.gov/groups/STM/cmvp/standards.html.

[SP 800-131B] NIST SP 800-131B, Transitions: Validation of Transitioning Cryptographic Algorithms and Key Lengths; [INSERT DATE]; available at [INSERT LINK].

[X9.31] American National Standard (ANS) X9.31-1998, Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA); withdrawn, but available from X9.org.

[X9.62] American National Standard (ANS) X9.62-2005, Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA).