# 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 800-131B |
| **Title** | Transitions: Validation of Transitioning Cryptographic Algorithm and Key Lengths |
| **Publication Date** | February 2011 |
| **Additional Information** | The guidance in this draft was moved to FIPS 140-2 Implementation Guidance W.14. |

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

**NIST Special Publication 800-131B**

# Transitions: Validation of Transitioning Cryptographic Algorithm and Key Lengths

**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

At the start of the 21st century, the National Institute of Standards and Technology (NIST) began the task of providing cryptographic key management guidance, which includes defining and implementing appropriate key management procedures, using algorithms that adequately protect sensitive information, and planning ahead for possible changes in the use of cryptography because of algorithm breaks or the availability of more powerful computing techniques. NIST Special Publication (SP) 800-57, Part 1 was the first document produced in this effort, and includes a general approach for transitioning from one algorithm or key length to another. SP 800-131A provided more specific guidance for transitions to the *use* of stronger cryptographic keys and more robust algorithms. This document (SP 800-131B) is intended to provide more detail about the *validation* of the cryptographic algorithms and cryptographic modules in transition, as specified in SP 800-131A.

**Key Words:** Cryptographic Algorithm Validation Program (CAVP), Cryptographic Module Validation Program (CMVP), 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: Validation of Transitioning Cryptographic Algorithms and Key Lengths

## 1 Background and Purpose

At the beginning of the 21st century, the National Institute of Standards and Technology (NIST) began the task of providing cryptographic key management guidance. This included lessons learned over many years of dealing with key management issues, and attempts to encourage the definition and implementation of appropriate key management procedures, to use algorithms that adequately protect sensitive information, and to plan ahead for possible changes in the use of cryptography because of algorithm breaks or the availability of more powerful computing techniques. The general approach for transitioning from one algorithm or key length to another is addressed in Part 1 of NIST Special Publication (SP) 800-57 [SP 800-57]. SP 800-131A [SP 800-131A] provides a specific transition schedule for using algorithms and key lengths.

This document is intended to provide more detail about the validation of the cryptographic algorithms and cryptographic modules in transition, as specified in [SP 800-131A].

Algorithm testing is conducted under the Cryptographic Algorithm Validation Program (CAVP). Algorithms are incorporated within cryptographic modules where module testing is conducted under the Cryptographic Module Validation Program (CMVP). The CAVP is responsible for validating cryptographic algorithm implementations for conformance to specifications that have been **approved** in Federal Information Processing Standards (FIPS) or NIST Recommendations (published as NIST Special Publications (SP)). The CMVP validates cryptographic modules for conformance to FIPS 140-2 [FIPS 140-2]. To be validated by the CMVP, each module **shall** include an implementation of at least one **approved** algorithm. CAVP and CMVP testing is conducted by independent, National Voluntary Laboratory Accreditation Program (NVLAP)-accredited Cryptographic and Security Testing (CST) laboratories, which submit algorithm and module validation requests containing completed test reports are submitted to the National Institute of Standards and Technology (NIST) and the Communications Security Establishment Canada (CSEC) for validation.

Modules validated by the CMVP for conformance to [FIPS 140-2] are used by Federal agencies for the protection of sensitive unclassified information. With the passage of the Federal Information Security Management Act (FISMA) of 2002, there is no longer a statutory provision to allow for Federal agencies to waive mandatory Federal Information Processing Standards.

# 2 Useful Terms

## 2.1 New Validations, Already Validated Implementations and Revalidations

The CAVP and CMVP, along with the accredited CST laboratories, have been in existence since 1995. Consequently, a large number of implementations have been tested and validated under these programs, and the number of new implementations that are validated continue to increase every year. The CMVP conducts revalidations of already-validated module implementations whenever changes are made to the module implementations or when new operational environments are added to an existing validation. These changes may require the validation of new implementations and/or the retesting of already-validated algorithm implementations.

- *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 Section G.8 of the *Implementation Guidance for FIPS PUB 140-2 and the CMVP* [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 refer to the dates of the CST laboratory's initial submission of a module test report to the CMVP for validation.

  Security policies for new module implementations **shall** include information about any transitions that have already occurred or may occur in the future by a reference to [SP 800-131A].

- *Already-Validated Implementations* are algorithm or module implementations that have already been tested by a CST laboratory and validated by the CAVP or CMVP. The CAVP and CMVP will review these implementations and the underlying algorithm validations for compliance with the new security requirements as stated in [SP 800-131A] when a transition date occurs.

  - The CAVP will review the algorithm validations to determine if a validated algorithm or a key length is disallowed in [SP 800-131A]. If a complete algorithm validation is disallowed, the CAVP will revoke the algorithm validation; revoked references will continue to be available for historical purposes. If only parts of a validation are disallowed (e.g., one of the validated key lengths is disallowed), the disallowed parts of the validation will be annotated as disallowed.

  - Cryptographic module validations reference at least one algorithm implementation. Theses references are to algorithms that have been validated by the CAVP, algorithms for which standards may not have

existed at the time of the CMVP validation, or algorithms for which CAVP validation testing was not available at the time of the module validation. Some algorithms in NIST-Recommendations may appear on a CMVP validation certificate as "non-approved, but allowed for use in a [FIPS 140-2]-approved mode of operation. In addition, the level of specificity found on a module validation-entry has changed over the life of the CMVP program, as standards and testing methods emerged.

The CMVP will review the list of module validations and take the appropriate actions, based on the module's provided algorithm validation references. If an algorithm validation is revoked by the CAVP, the module's validation reference will be removed from the approved line of the CMVP validation certificate. References to revised algorithm validations will remain unchanged; i.e., if only part of the validation is disallowed by the CAVP, the certificate reference will not be revised. 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 sizes utilized by their system are in compliance with the requirements of [SP 800-131A]. All questions regarding the implementation and/or use of any module located on the CMVP module validation lists should first be directed to the appropriate vendor point-of-contact (listed for each entry).

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. However, the CMVP encourages vendors to submit updated Security Policies with appropriate revisions.

Cryptographic modules revalidated under Scenarios 1, 2 and 4 of [IG G.8] will be treated as already-validated implementations.

## 2.2 Terms Used in SP 800-131A

The terms "**acceptable**", "**deprecated**", "**restricted**" and "**legacy use**" are used in [SP 800-131A] to address the use of cryptographic algorithms and key lengths.

- **Acceptable** is used to mean that the algorithm and key length is safe to use; no security risk is currently known.
- **Deprecated** means that the use of the algorithm and key length is allowed, but the user must accept some risk.
- **Restricted** means that the use of the algorithm or key length is deprecated, and there are additional restrictions required to use the algorithm or key length for applying cryptographic protection to data (e.g., encrypting).

- **Legacy-use** means that the algorithm or key length may be used to process already-protected information (e.g., to decrypt ciphertext data or to verify a digital signature) that was protected using an algorithm or key length that has since been deprecated, restricted or disallowed for applying cryptographic protection. For example, from 2011 though 2013, the use of 1024-bit RSA keys to generate a digital signature is deprecated, and is disallowed beginning in 2014. However, digital signatures that were generated using 1024-bit RSA keys prior to 2014 periods may be verified, since digital signature verification is permissible for legacy use.

An algorithm is considered to be disallowed if it is not classified as acceptable, deprecated, restricted or allowed for legacy-use.

## 3 Validation of Cryptographic Algorithms and Cryptographic Modules

[SP 800-131A] addresses the use of cryptographic algorithms and key lengths during given time periods, classifying them as acceptable, deprecated, restricted, legacy-use and disallowed. These classifications affect the validation of new implementations and the status of already-validated implementations.

### 3.1 Acceptable

New algorithm validation submissions and new module implementation submissions will be accepted by the CAVP or CMVP, respectively, through December 31st of the end-year indicated, if an end-year is provided, or with no date restriction if an end-year is not provided. Module security policies **shall** reference [SP 800-131A] for any future end dates that may apply.

Already-validated algorithm or module implementations will remain valid during this period.

No additional requirements are placed on the cryptographic modules revalidated under scenarios 1, 2 and 4 of [IG G.8].

### 3.2 Deprecated

In general, new algorithm validation submissions or new module implementation submissions will be accepted for validation by the CAVP or CMVP, respectively, through December 31st of the end-year for the deprecation period.

Already-validated algorithm and module implementations will remain valid through December 31st of the end-year of the deprecation period.

In the case of the deprecated RNGs, new algorithm validation submissions or new module implementation submissions will only be accepted for validation by the CAVP or CMVP, respectively, through the end of the FIPS 186-2 to FIPS 186-3 transition period (see [SP 800-131C]). For this case, revalidations of module implementations containing deprecated RNGs will be accepted for revalidation by the CMVP until their use is disallowed, as specified in [SP 800-131A].

Module security policies **shall** reference [SP 800-131A] for any disallowed dates that may apply.

## 3.3 Restricted

SP 800-131A only identifies two-key Triple DES as being restricted. The use of two-key Triple DES for applying cryptographic protection (i.e., encryption of plaintext data or wrapping a plaintext key) is restricted when used between January 1, 2011 through December 31, 2015. Note that the computation of a message authentication code is not listed in [SP 800-131A] as restricted during this period.

New algorithm validation submissions and new module implementation submissions of the two-key Triple DES algorithm that encrypt data or wrap a key will be accepted by the CAVP or CMVP, respectively, through December 31, 2015.

Module security policies **shall** reference [SP 800-131A] for the date when two-key Triple DES will no longer be allowed to encrypt data or wrap a key. When an implementation that includes the capability to encrypt data or wrap a key using two-key Triple DES is validated, the cryptographic module's Security Policy **shall** state that a key **shall not** be used to encrypt or wrap more than $2^{20}$ blocks of data or keying material.

The restricted period for encrypting data or wrapping a key using two-key Triple DES ends after December 31st, 2015. However, CAVP testing is currently designed to only determine if the two-key Triple DES algorithm is implemented correctly, not to distinguish between its uses (e.g., encrypting data or wrapping a key). Already-validated two-key Triple DES implementations will be handled by the CAVP and the CMVP as discussed in Section 2.1.

## 3.4 Legacy-Use

The legacy-use classification is intended to allow the processing of already-protected information (e.g., the decryption of information that was encrypted using an algorithm or key length that was acceptable, restricted or deprecated at the time of encryption).

New algorithm validation submissions and new module implementation submissions will be accepted for validation by the CAVP or CMVP, respectively, until disallowed.

Algorithm validations and module validations for already-validated implementations will remain valid.

Example: After December 31st, 2015, two-key Triple DES decryption can be validated, while two-key Triple DES encryption will not (see Disallowed, below).

## 3.5 Disallowed Algorithms and Key Lengths

Section 2.1 discusses the handling of already-validated implementations of algorithms and key lengths that are no longer allowed for their purpose (e.g., the use of SKIPJACK for encryption, or digital signature generation using a disallowed key length). However, even though [SP 800-131A] disallows the use of an algorithm or key length, interoperability with legacy devices and applications that use the disallowed algorithm or key length need to be considered. For example, devices or applications may need to include the disallowed algorithm or key length for use during a transition period to stronger algorithms or key lengths. The implementations of these disallowed algorithms or 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 algorithms, key lengths, or purposes for which an algorithm or key length may be used 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.

New algorithm validation submissions and new module implementation submissions of algorithms and key lengths that are disallowed for their purpose will not be accepted for validation by the CAVP or CMVP.

## 4. Documentation Requirements for CMVP Validations

Vendors of cryptographic modules employing algorithms and key lengths that are subject to the transition requirements in [SP 800-131A] need to address the status of such algorithms and key lengths in the module's Security Policy that is submitted to the CMVP in the cryptographic module's test report. This applies to those algorithms and key lengths that are classified in [SP 800-131A] as either deprecated, restricted, legacy-use or disallowed.

The Security Policy **shall** either include or make a reference to the transition tables available at [URL will be inserted later]. The data in the tables will inform users of the risks associated with using a particular algorithm and a given key length.

This documentation requirement applies to all validation submissions made three months after the publication of SP 800-131B. This requirement also applies to the revalidation submissions, Scenarios 3 and 5 of [IG G.8].

## Appendix A: References

FIPS and SP documents are available at http://csrc.nist.gov/publications/, except for the FIPS 140-2 Implementation Guidance, which is available at http://csrc.nist.gov/groups/STM/cmvp/standards.html#02.


[FIPS 140-2] FIPS 140-2, Security Requirements for Cryptographic Modules, with Change Notices, December 2002.

[IG G.8] Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program, Section G.8, December 2010.

[FIPS 186-2] FIPS 186-2, Digital Signature Standard, January 2000.

[FIPS 186-3] FIPS 186-3, Digital Signature Standard, June 2009.

[SP 800-57] Part 1, Recommendation for Key Management: General, March 2007.

[SP 800-131A] Transitions: Recommendation for the Transitioning of Cryptographic Algorithms and Key Lengths, January 2011.

[SP 800-131C] Transitions: Validating the Transition form FIPS 186-2 to FIPS 186-3, Draft.