



SP 800-131A Transitions and Related Implementation Guidance

Allen Roginsky
Apostol Vassilev

CMVP NIST
November 2015

Overview of the talk

- Major milestones of the transition
 - SP 800-131A (original and revised)
 - FIPS 186-4
- 112-bit-strong cryptographic keys
- A major change is coming at the end of 2015
- Future transition plans

Why The Transition?

- Security strength of 80 bits was insufficient (the 56-bit strong DES was broken long ago; attacks on the SHA-1 collision resistance property; advances in integer factorization; etc.)
- Some algorithms are not too strong regardless of the key lengths (the non-SP-800-90A RNGs)
- Transition plans first announced in SP 800-57, Part 1 in 2005

Algorithm Status

One of the following:

- **Approved**
- **Acceptable**
- **Deprecated**
- **Restricted** (this category will disappear after 2015)
- **Legacy-use**
- **Disallowed** (all of the algorithms and key sizes not falling into the previous five categories)

Which algorithms are affected?

- **Encryption Algorithms**
 - As of the end of 2010, SKIPJACK encryption is Legacy-use only
 - Until the end of 2015, two-key Triple-DES encryption is Restricted with no more than 2^{20} (plaintext, cyphertext) pairs encrypted under the same key. The encryption strength is estimated at min (112, 120-n) bits when 2^n (plaintext, cyphertext) pairs are available
 - Two-key Triple-DES encryption is Disallowed after 2015.
 - AES and three-key Triple-DES are Acceptable

Which algorithms are affected?

- **Digital Signatures**

- Digital signature generation algorithms with less than 112 bits of encryption strength are Disallowed
- FIPS 186-4 is now in effect
- Signature verification with less than 112 bits of strength is Legacy-use
- SP 800-131A interprets the 112-bit requirement
- An exception: within the scope of the TLS and SSH protocols only, it is “OK” to generate an RSA digital signature using SHA-1. A strong key is still required
- RSA key generation process shall be tested

Which algorithms are affected?

- **Deterministic Random Number Generators**

**As of the end of 2015,
the non-SP-800-90A-
compliant RNGs
become Disallowed
– Retroactively !!!!!**

- **This affects all of the algorithms within a cryptographic module that may rely on an RNG for generation of their keys, nonces, IVs.**

Which algorithms are affected?

- **Key Agreement and Key Transport**
 - Key Agreement and Key Transport algorithms stay Acceptable if
 - Key strength is at least 112 bits and
 - The algorithms are compliant with the appropriate NIST standards: SP 800-56A, SP 800-56B or SP 800-38F
 - As of the end of 2013, the non-compliant Key Agreement and Key Transport (Key Encapsulation) algorithms became Deprecated if key strength was at least 112 bits. Will get Disallowed after 2017.
 - The non-SP-800-38F-compliant key wrapping is Deprecated if compliant with one of the provisions of IG D.9. Will get Disallowed after 2017.
 - All other cases are Disallowed now.

Which algorithms are affected?

- **Other Algorithms**

- Hash Functions
- Message Authentication Codes
- Key Derivations from Other Keys

See SP 800-131A for details

- The transition goes on as scheduled!



FIPS 186-2 to 186-4 Transition

- Beginning in 2014, new implementations are tested for their compliance with FIPS 186-4
 - This applies to domain parameter generation, key pair generation and digital signature generation
 - Signature verification per FIPS 186-2 is Legacy-use
- Beginning in 2014, if the module generates the RSA digital signature keys internally, they shall be generated as shown in FIPS 186-4 and an algorithm validation certificate for RSA key generation shall be obtained by the vendor.



Future Transition Plans

- The 2017 Transition as described in SP 800-131A
- Transition from SP 800-56A to SP 800-56A-rev2
 - At this time, testing can be done only to the original version
 - Vendor affirmation to SP 800-56A-rev2
 - In the future – SP 800-56A-rev2 only
- Transition to the SP 800-90B-compliant NDRNGs

Short Summary

- The non-SP-800-90A random number generators are going away after 2015
- The SP 800-131A transition is on schedule
- Stricter rules regarding the non-Approved algorithms
 - RSA keys must be generated in a compliant manner
 - The RSA, Diffie-Hellman and MQV transitions, as well as the key wrapping transition are scheduled for 2017
 - Key wrapping will need to be compliant with SP 800-38F to be Approved and Acceptable
 - The 100-bit-strength exception for the two-key Triple-DES encryption is going away at the end of 2015