

Received Comments on SP 800-131B

| | |
|-----------------------------------|------|
| David Cornwell, Coact..... | 2, 3 |
| Ashit Vora, Cisco..... | 4 |
| Steve Ratcliffe, ICSA Labs..... | 5 |
| David Cornwell, Coact..... | 6 |
| Stephanie Eckgren, Infogard..... | 7 |
| Jon Geater, Thales Security | 13 |
| Paul Turner, Venafi..... | 14 |
| Mike Grimm, Microsoft..... | 15 |

From: David Cornwell <dcornwell@coact.com>

Date: February 23, 2011

It is mentioned in several places that the Security Policies **shall** reference [SP 800-131A].

Wherever such “**shall**” statements are made in the SP 800-131B, please provide examples of acceptable References in the Security Policies and the level of detail needed to satisfy this requirement.

These examples will prevent the need for Implementation Guidance later and the labs will be able point vendors to these examples and avoid lengthy debates and comment rounds about what is or is not acceptable.

For example, is the following single catch-all statement acceptable in the Security Policy? “See SP 800-131A for details concerning algorithm and key transition dates”.

From: David Cornwell <dcornwell@coact.com>

Date: February 24, 2011

Algorithms and keys used for legacy use will become important as we cross the Transition boundaries. It would be useful to have more legacy use examples and the reasons why they are true.

1. Your example is true because data that was encrypted up until 31st Dec 2015 using two-key Triple DES can continue to be decrypted into the future for legacy use after this time even though encrypt mode is disallowed after this time.
2. A digital signature that was generated using 1024 keys can continue to be verified into the future because signature verification of signatures with 80 bits of security can be verified for legacy use, even though signature generation using 1024 bit keys is disallowed after 31st Dec 2013.
3. A digital signature that was generated using SHA-1 can continue to be verified into the future because this is allowed for legacy use, even though signature generation using SHA-1 is disallowed after Dec 31st 2013.

From: Ashit Vora <asvora@cisco.com>

Date: February 25, 2011

1. SP 800-131B: The transition time for RNG is not clear. This document points to SP 800-131C but the latter document does not have a definitive date. Based on Peer-2-Peer session at RSA conference it seemed that the transition date was December 31, 2013. This needs be clearly listed
2. General comment: The transition date for RNGs is not in line with SP 800-131A. The general understanding was that the validation process timelines will be same as that of 131A and as such vendors have prepared accordingly. Changing this timeline does cause issues with plans already made. We would appreciate it if the timeline mentioned in 131A is maintained.

From: Ratcliffe, Steve <sratliffe@icsalabs.com>

Date: February 28, 2011

Page 7

"Module security policies shall reference [SP 800-131A] for any future end dates that may apply." Interesting statement. Recommend a few examples or point to another doc with examples.

Page 9

Why is this statement in the doc? "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." Is NIST encouraging independent testing?

Comment [ebb1]: Is the surrounding text clear?

SP800-131C

Page 7

Remove the two "[" from:

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.

From: David Cornwell <dcornwell@coact.com>

Date: February 28, 2011

Regarding signature verification for legacy-use in FIPS mode:

Suppose a vendor signs their software or firmware using 1024 bit DSA and continues to use this signed software/firmware for their software/firmware integrity test in 2011 and beyond. Is this allowed under the legacy-use of signature verification for 1024 bit keys or do they have to upgrade to a larger key size?

Comment [ebb2]: Yes? Insert as an example?

Is there a difference between signature verification of data versus signature verification of software/firmware under the software/firmware integrity test?

Comment [ebb3]: No?

From: Stephanie Eckgren <seckgren@infogard.com>

Date: March 24, 2011

| # | Section, Paragraph, or Page | Comment | Suggested Revisions | Rationale for Revisions |
|---|-----------------------------|--|--|--|
| 1 | Title | The term “Algorithm” should be plural. | Change “Transitions: Validation of Transitioning Cryptographic Algorithm and Key Lengths” to “Transitions: Validation of Transitioning Cryptographic Algorithms and Key Lengths” | This will fix the typo. |
| 2 | Section 2.1, Paragraph 7 | This paragraph does not mention what will happen if ALL algorithm certificates are revoked within a module. Will the CMVP revoke the module certificate in this case? | Add the following sentence: “If all algorithm certificates within a module certificate are revoked, then the entire module certificate will be marked as ‘Revoked’”. | This information is missing and is important, especially for very old FIPS certificates. If there are no “FIPS-approved algorithms” left in the module then the module is no longer valid. |
| 3 | Section 2.1, Paragraph 7 | This paragraph states that “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”. Does this mean it will be moved to the “Other algorithms” section on the certificate? | Change the sentence to: “If an algorithm validation is revoked by the CAVP, the module’s validation reference will be moved to the <i>Other algorithms</i> line of the CMVP validation certificate”. | This information is missing and it is important to clarify. |

| # | Section, Paragraph, or Page | Comment | Suggested Revisions | Rationale for Revisions |
|---|-----------------------------|--|--|--|
| 4 | Section 2.1, Paragraph 8 | <p>Regarding the statement “the CMVP encourages vendors to submit updated Security Policies with appropriate revisions”. Since Security Policy submission will be “encouraged” but not required, it is important to make a note next to each Security Policy on the FIPS validation page.</p> <p>Those purchasing a module may only look at the Security Policy and they should be warned.</p> | <p>As an example, the CMVP certificate page could list the following next to the Cryptographic Module’s Security Policy:</p> <p style="text-align: center;">Test Implementation (Versions X.Y.Z)</p> <p style="text-align: center;"><i>(When operated in FIPS mode)</i></p> <p style="text-align: center;">Validated to FIPS 140-2</p> <p style="text-align: center;"><u>Security Policy</u> (<i>ALGORITHMS NOT IN SYNC WITH CERTIFICATE</i>)</p> <p style="text-align: center;"><u>Certificate</u></p> | <p>It should be made clear that the Security Policy has not been updated to match the certificate.</p> |
| 5 | Section 2.1, General | <p>Consider moving part of this section to Section 3.5 (Disallowed Algorithms and Key Lengths). All of the statements made about what will happen upon the transition end date should be moved. Section 2.1 should only define a “New Implementation” and “Already Validated Implementation”.</p> | <p>Most of the “Already-Validation Implementations” section should move to Section 3.5. The section should only state that these are the certificates that already exist and those under IG G.8 Scenarios 1, 2, and 4.</p> | <p>The information appears to be out of place and will make more sense under the “Disallowed” section.</p> |

| # | Section, Paragraph, or Page | Comment | Suggested Revisions | Rationale for Revisions |
|---|-----------------------------|--|--|---|
| 6 | Section 3.2, Paragraph 3 | Please clarify this paragraph with respect to “Revalidations”. | Change last sentence to: “The only exception to this case is for modules being submitted under IG G.8 Scenarios 1 through 4. For this case, previously implemented deprecated RNGs will be accepted by the CAVP and CMVP until their use is disallowed as specified in [SP 800-131A]”. | The word “Revalidations” should be specified in terms of IG G.8. |
| 7 | Section 3.3, General | How does the 2-key TDES restriction apply to algorithm certificates? Please add a clarifying sentence. | <p>Consider showing on the algorithm certificates if the restriction applies at the algorithm level and/or at the module level. Some algorithm implementations do allow for $\geq 2^{20}$ blocks per encryption instance. This needs to be restricted.</p> <p>Consider adding a clarifying sentence like: “Depending on the algorithm implementation, the restriction may also apply at the algorithm level. This will be made clear on the algorithm certificate.”</p> | This case needs to be accounted for in the document. Looking at “module” and “algorithm” level restrictions is important. |

| # | Section, Paragraph, or Page | Comment | Suggested Revisions | Rationale for Revisions |
|----|-----------------------------|--|---|--|
| 8 | Section 3.3, Paragraph 4 | The last paragraph is not clear. Please revise. | Remove the first sentence in Paragraph 4 and revise the second sentence. E.g., change the last paragraph to the following: “Already-validated algorithm and module implementations will remain valid through December 31 st of the end-year of the restricted period.” | The first sentence seems out of place and second sentence just refers elsewhere. Instead, an explicit statement should be made here. |
| 9 | Section 3.5, General | It should be clarified that “Disallowed” means “non-Approved”. This is never officially stated. (Similarly, the terms “Acceptable”, “Deprecated”, “Restricted”, and “Legacy-use” should be tied to the term “FIPS Approved”.) | Add a sentence like the following: “An algorithm or key size that is Disallowed is considered FIPS non-Approved and it cannot be used in the FIPS mode of operation.” | This will clarify the meaning and tie the SP 800-131 terms to FIPS terms. |
| 10 | Section 4, General | Use this section to consolidate all of the “Security Policy” statements made throughout this document. | Remove the “Security Policy” statements from Sections 3.1, 3.2, 3.3, 3.4, and 3.5. Instead make the statements in this Section only. | This clarifies and consolidates the “Security Policy” requirements to one section. |

| # | Section, Paragraph, or Page | Comment | Suggested Revisions | Rationale for Revisions |
|----|-----------------------------|--|--|--|
| 11 | Section 4, General | The Security Policy should need to state more than “a reference to SP 800-131 for dates that apply”. | Consider making the Security Policy “shall” requirements stricter. For example, the requirement could be: “Module security policies shall mark each Deprecated, Restricted, and Legacy-use algorithm as such and shall explicitly list the Disallowed date per SP 800-131A”. | This forces Vendors to consciously be aware of which algorithms are going away. This also makes it clear to those purchasing the module. |
| 12 | Section 4, Paragraph 3 | This should be clarified in the terms defined in Section 2.1. “New Implementation” already includes IG G.8 Scenarios 3 and 5. Why is this repeated in the last sentence? | Change the paragraph to: “This documentation requirement applies to all new module implementation submissions made three months after the publication of SP 800-131B.” | There is no need to repeat IG G.8 Scenarios 3 and 5. |

| # | Section, Paragraph, or Page | Comment | Suggested Revisions | Rationale for Revisions |
|----|-----------------------------|--|---|--|
| 13 | General | <p>What does it mean when the main RNG on a FIPS certificate is no longer “FIPS Approved”? Will the whole certificate be revoked? It seems that if the mechanism for generating keys for all of the other algorithms is revoked, then we have an issue. For example, in 2016 we may have a module that contains a FIPS Approved AES but a non-FIPS Approved RNG. Therefore, the keys being created for that AES algorithm are not “Approved”.</p> <p>The same question also stands for key establishment techniques and other areas where an algorithm for which other algorithms are dependent upon may no longer be “FIPS Approved”.</p> | <p>Add a clarifying statement regarding NIST’s view on this issue in Section 3.5.</p> | <p>This is a major issue that needs to be clarified.</p> |

From: Jon Geater <Jon.Geater@thales-ecurity.com>

Date: March 31, 2011

1. *“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”*

Surely this is the wrong sense? Should this not be “...more than 30%”?

2. *“It is the user’s responsibility to determine that the algorithms and key sizes utilized in their system are in compliance”*

Thank you for this explicit clarification.

From: Paul Turner Paul.Turner@venafi.com

Date: March 31, 2011

It might be helpful to have information about some of the research that has been done on the ability to break algorithms or key lengths. This might help organizations better understand why it is important to transition to longer key lengths or different algorithms. This might be a regularly updated page that included up to date information.

From: Mike Grimm <mgrimm@exchange.microsoft.com>

Date: March 31, 2011

| Section | Page # | Draft Text | Comment |
|---------|--------|--|---|
| --- | | General question on SP 800-131B | When will the CAVP and CVMP begin to update certificates for already-validated implementations as described in section 2.1? |
| --- | | General question on SP 800-131B | <p>Can the CAVP and CVMP contact the vendors prior to updating the certificates for already-validated implementations?</p> <p>This can help avoid errors or potential ambiguity in the revised certificate. At a minimum, the vendor should be notified of that the certificate has changed so the vendor can then update any corresponding product documentation.</p> |
| 2.1 | 5 | “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 | <p>This part is confusing. It seems that “new implementations” is being used here to refer to any implementation that is submitted for revalidation, whether with < 30% changes (IG G.8 scenario 3) or > 30% changes (IG G.8 scenario 5). We suggest revising the text to reflect this better.</p> <p>Proposed replacement: “For cryptographic modules, new implementations refer to cryptographic modules that are either new modules or the revalidation of previously validated modules. 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.”</p> |

| | | | |
|-----|---|--|---|
| | | FIPS PUB 140-2 and the CMVP [IG G.8], validation Scenarios 3 and 5.” | |
| 2.1 | 5 | “Cryptographic module validations reference at least one algorithm implementation. Theses references...” | Typographical error: replace “Theses” with “These”. |
| 2.1 | 6 | 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.[“] | Typo (missing end quotation mark) |
| 2.1 | 6 | “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 | <p>We believe this is likely to lead to confusion among customers. There are many scenarios in which module validation status gets called into question when one algorithm validation is revoked. For instance, an approved algorithm such as AES may use a revoked RNG to generate its keys, or the module may use revoked algorithms in its module integrity check. However, since new validations will not be questionable in this way (due to the new documentation requirements in this document), it seems inadvisable to issue guidance that causes customers to view all validations with a sense of doubt.</p> <p>Would it be possible for NIST and CMVP to specifically flag validations whose status is rendered questionable by such revocation, and to provide a process for vendors to remove the flag by submitting an updated Security Policy that addresses transition issues?</p> |

| | | | |
|-----|---|--|---|
| | | are in compliance with the requirements of [SP 800-131A].” | |
| 2.1 | 6 | <p>“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.”</p> | <p>Can vendors send updated security policy documents directly to the CMVP that are revised as a result of the cryptographic transition instead of sending the updated security policy documents to a Cryptographic and Security Testing lab?</p> |
| | 9 | <p>“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.</p> <p>New algorithm validation</p> | <p>When CAVP no longer performs validation testing for disallowed algorithms, can the corresponding validation testing tools be made available to the general public?</p> <p>Since many vendors may still implement disallowed algorithms for interoperability with legacy devices, making the testing tools publicly available provides the developer with the ability to check their implementation without the additional expense of hiring a cryptographic testing laboratory.</p> <p>We would also appreciate guidance on how to document any such testing in the Security Policy of the module.</p> |

| | | | |
|-----|-----------------------|--|---|
| | | <p>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.”</p> | |
| 3.5 | Page 9, 3rd Paragraph | <p>“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.”</p> | <p>Please clarify whether module submissions that include BOTH acceptable and disallowed algorithms (for interoperability) will or will not be accepted for validation by the CAVP or CMVP.</p> |
| 4. | Page 9 | <p>“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.”</p> | <p>The “[URL will be inserted later]” placeholder refers to transition tables with contents that are unknown to the reader. Is the table currently available elsewhere? If the transition tables are the same as those provided in SP 800-131A, then please include a more tangible document reference.</p> |