Comments on Draft SP 800-56B Revision 2:
Recommendation for Pair-Wise Key-Establishment
Using Integer Factorization Cryptography
(comment period closed October 5, 2018)

From: Hamburg, Mike, mhamburg@rambus.com
Date: Friday, July 13, 2018 at 2:17 PM

I'm confused about the following change in Draft SP 800-56B Rev 2. The change listed as #3 in the Notes to Reviewers is stated to be "Additional checks were added … to ensure that p and q are equal to or greater than 2^(nbits/2)." But the actual change is that if p or q >= 2^(nbits/2), then the keypair is invalid. This is the opposite of ensuring that p,q >= 2^(nbits/2). Furthermore, the previous check is that if p or q > 2^(nbits/2) – 1, the keypair is invalid, which is equivalent since p and q are integers.

What's going on here? The spec already sets a different lower bound on p,q, so it's presumably not trying to ensure p,q >= 2^(nbits/2-1).

NIST: Thank you for bringing this to our attention. Note 3 was removed for the remainder of the comment period.

From: Gen'ya SAKURAI, IPA
Date: October 2, 2018

Comment type: G = General; E = Editorial; T = Technical

Comment Number	Section	Line Number	Comment Type	Comment (including rationale)	NIST Response
1	Page ix		E	RSA-KEM-KWS is no longer available, so Figures 6 and 7 should be removed or list of Figures should be regenerated.	Done.
2	3.2 Page 10	29	E	C, C_0, C_1 should be replaced by C, C_U, C_V to be consistent with the content of main body of the standard.	Done.
3	3.2 Page 11	29	E	RSA-KEM-KWS is no longer available, so *KWK* should be removed because there is no reference to *KWK* other than Appendix E: Revisions (Informative).	Done.
4	3.2 Page 13	29	E	The function *S*(*nBits*) is likely to confuse with lower case letter *s* or its misprint, especially in main body of the standard, for example, the statement in line 1073. Please consider using bold face italic ***S***(*nBits*) to	Changed the name of the function to ES.

				distinguish the function from variable *s*.	
5	3.2 Page 13	29	E	RSA-KEM-KWS is no longer available, so SKW should be removed because there is no reference to SKW other than Appendix E: Revisions (Informative).	Done.
6	5.6.3	665	E	HMAC_SHA… should be corrected to as HMAC-SHA… to be consistent with the definition (HMAC-*hash*) in 3.2.	Done.
7	5.6.3	665	E	HMAC_SHA-1) should be HMAC-SHA-1.	Done.
8	6.2.1	738, 739	T	The former signs of inequality (2^((nBits-1)/2) < *p*, 2^((nBits-1)/2) < *q*) should be replaced by (<=, or ≤), to be consistent with Appendix B.3.1 of FIPS 186-4. (The current statements (<) are not consistent with the statements in lines 1095 and 1097.)	Since the lower bound in question is either even integers or not an integer at all, equality should never occur. It is better to keep the strict inequalities as a way of avoiding errors in the understanding or implementation of the generation routines. Equality with that lower bound could have been a consideration in the validity checks performed on recovered factors of an RSA modulus (recovered, e.g., as in Appendix C). When *p* and *q* are "recovered" from *n*, equality with the bound must be a disqualifying event, indicating that the RSA key pair is invalid. (Note: for an invalid RSA pair – or for RSA key pairs that are not generated as in 56B – *nBits* might be odd, making equality with the lower bound possible.)
9	6.4.1.3.3	1255	E	There is extra space " " between "len(" and "e_{pub}".	Done.
10	6.4.1.4.3	1327	E	The full stop (.) between "*dP*" and "*dQ*" should be replaced by comma (,).	Done.

11	7.2.1	1646	E	The last strike-through should be removed.	Done.
12	8.2.3.2	2103	E	For 5th row and Party U column of Figure 7, the $MacTag_V$ should be replaced by $MacTag_V$, (i.e. from roman to italic).	Done.
13	8.3.3.2	2255	E	For 8th row and Party U column of Figure 9, the $MacTag_V$ should be replaced by $MacTag_V$, (i.e. from roman to italic).	Done.
14		2270	E	The subsection numbering "8.3.3.2" should be corrected to as "8.3.3.3".	Done.
15		2273	E	For 8th row and Party U column of Figure 10, the $MacTag_U$ should be replaced by $MacTag_U$, (i.e. from roman to italic).	Done.
16		2288	E	The subsection numbering "8.3.3.3" should be corrected to as "8.3.3.4".	Done.
17		2291	E	As for 4th row and Party V column of Figure 11, $PrivKey_V$ should be replaced by $PrivKey_V$ (i.e. from roman to italic).	Done.
18		2291	T,E	As for 5th row and Party V column of Figure 11, the statement, (Z_V, C_V) = RSASVE.GENERATE($PubKey_V$) ,should be replaced to as (Z_V, C_V) = RSASVE.GENERATE($PubKey_U$) .	Done.
19	9.2.3	2421	E	The *PubKeyV* should be replaced by *PubKeyV*, (i.e. from roman to italic).	Done.
20	9.2.4.2	2459	E	There are two occurrences of “Error! Bookmark not defined.”	Fixed.
21			G,T	It is not clarified in the current draft how to define the targeted security strength for KAS2 scheme. If s_X denotes a security strength of component X in general, should the targeted security strength for KAS2 be defined as either	The approach to implementation/use of key-agreement schemes taken by this document is to first decide on the (targeted) security strength that is needed/desired and then to make decisions/choices

				(min(s_{RBG_V}, s_{Key_U}) + min(s_{RBG_U}, s_{Key_V})) or min(min(s_{RBG_V}, s_{Key_U}), min(s_{RBG_U}, s_{Key_V})) ?	concerning RBGs, key sizes, etc., accordingly. (See the def. of "Targeted Security Strength" on page 8.) The security strengths for specific schemes is out-of-scope for 56B, but the usual way for determining the security strength provided is to set it to the weakest of all the various components.
22	A.1	2956	E	ANS X9.44-2007 (R2017) was reaffirmed in 2017, so may not be withdrawn.	Corrected.