Comments Received on Draft NIST Special Publication (SP) 800-56C Revision 1 (August 2017)
(Comment Period Closed November 2017)

From: g-sakura@ipa.go.jp <g-sakura@ipa.go.jp
Date: 10/31/17, 2:03 AM

Comment Number	Section	Line Number	Comment Type	Comment (including rationale)	Resolution
1	5.1	455-461	T	The minimum length of salt should be clarified, e.g. 112-bit or minimum key length for HMAC.	"non-null" was inserted before "salt", where applicable. Additional text has also been added.
2	5.1	453-509	G, T	The relationship between OtherInfo and L, {IV}, FixedInfo becomes clear in contrast to the previous version of NIST SP 800-56C. NIST SP 800-56B Rev.1 points to NIST SP 800-56C, so the NIST SP 800-56B Rev.1 (especially 5.5 and/or 5.5.2 of NIST SP 800-56B Rev.1) should also be revised to be consistent with NIST SP 800-56C in order to reflect this clarification.	SP 800-56B is currently being revised as requested.