Informative Note

Date: September 19, 2016

Referenced Publication:

NIST Special Publication 800-135 Revision 1
Recommendation for Existing Application-Specific Key Derivation Functions.
http://dx.doi.org/10.6028/NIST.SP.800-135r1

Issued By: Computer Security Division

SUBJECT: Section 5.3, The Secure Real-time Transport Protocol (SRTP) Key Derivation Function

NOTE:

In RFC 3711, the index was originally a 48-bit value in SRTP or a 32-bit value in SRTCP. Errata ID 3712, released by the IETF at https://www.rfc-editor.org/errata_search.php?rfc=3711&eid=3712, changed the index value in SRTCP to also be a 48-bit value of `000…000||SRTCP_index` (a string of 17 zero-bits concatenated with the 31-bit SRTCP index).

The release of the Errata 3712 does not alter the text of Section 5.3 in NIST SP 800-135 Rev. 1. Key-derivation methods with both the old and the new index values are approved.

ADDITIONAL INFORMATION:

NIST SP 800-135 Revision 1:
http://csrc.nist.gov/publications/PubsSPs.html#800-135