ERICSSON

Date: September 30, 2021

Comments on SP 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC

Dear NIST,

Thanks for your continuous efforts to produce well-written open-access security documents. FIPS 198-1, SP 800-22 Rev. 1a, SP 800-38D, SP 800-38E, and SP 800-107 Rev. 1 are all important documents that should be updated.

Please find below our comments on SP 800-38D:

- The “If len(IV) ≠ 96” where the IV is hashed does not seem to be used in practice, provide weaker security, and adds complexity. We suggest that this IV hashing alternative is deprecated.

- Many recent IETF protocols like TLS 1.3 [RFC8446], OSCORE [RFC8613], Encrypted Content-Encoding for HTTP [RFC8188] etc. does not adhere to the IV constructions in 800-38D. The update to 800-38D should allow for IV to be constructed as a 96-bit fixed random number XORed with the invocation field. Such a construction could optionally allow 128-bit randomness where the block counter is also XORed with the fixed random number instead of being concatenated.

- As stated in [1], several of the statements in Appendix C are not correct. SRTP does in general not meet the guidelines. The idea that an attacker does not get side-channel information about successful forgeries is almost always wrong and very dangerous. As GCM with short tags does not seem to be used, we would recommend to just remove Appendix C and forbid short, truncated tags.

  Note that a high-performance software friendly AEAD algorithm like AES-GCM with secure short tags (e.g., 64 bits) would be useful in wireless networks.

  [1] https://eprint.iacr.org/2015/477.pdf

Best Regards,
John Preuß Mattsson,
Senior Specialist, Ericsson

Ericssson AB
Group Function Technology
SE-164 80 Stockholm
SWEDEN
Tel: +46 10 719 00 00
Fax: +46 10 719 95 27
VAT: SE556056625801
Reg no: 556056-6258
Visiting address
Torshamnsgatan 21 (Kista)