ERICSSON

Date: September 30, 2021

Comments on FIPS 198-1: The Keyed-Hash Message Authentication Code (HMAC)

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 FIPS 198-1:

- It would be good to also mention that HMAC can also be used as a pseudorandom function / key-derivation function. This is currently missing. It would also be good if the specification gives a reference to SP 800-56C Rev. 2 as this is likely useful for many readers.

- ”HMAC shall use an Approved cryptographic hash function [FIPS 180-3].”

  I assume this will be updated to [180-4] and [FIPS PUB 202]. It would be good if the specification also gives a reference to KMAC [800-185], which might be a more efficient solution then HMAC-SHA3 in many cases.

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)