From: Calik, Cagdas (IntlAssoc)
To: lightweight-crypto
Subject: checklist and reference implementations
Date: Thursday, January 31, 2019 4:06:19 PM

I’m done reviewing the checklist document. I’ve made changes in the following items (below is the final version):

- If ciphertext fails decryption-verification, plaintext is not returned
- Authenticated encryption and decryption-verification supported by all family members

Regarding the reference implementations and KAT verification, here are the issues we should inform the submitters about:

- Source code does not compile. There are additional .c files but they must be excluded from compilation for the build to succeed.
- Compiler warnings.
- Binary literal prefix. “comet and lotus” source code include this non-standard feature.
- Build platform. SAEAES KAT file is generated on windows, as opposed to the requirement to be generated on the reference linux platform.
- KAT file is in incorrect folder. “comet, limdolen, and lotus” placed their KAT files inside the ‘ref’ folder.
- No output generated when plaintext is empty. SAEAES has this problem.
- Ciphertext collisions found in limdolen by Meltem.

Cagdas