# Public Comments on SP 800-38E, Recommendation for Block Cipher Modes of Operation: the XTS-AES Mode for Confidentiality on Storage Devices

Comment period: August 6, 2021 - October 1, 2021

On August 6, 2021, NIST's Crypto Publication Review Board initiated a review of SP 800-38E *Recommendation for Block Cipher Modes of Operation: the XTS-AES Mode for Confidentiality on Storage Devices*. This document includes the public comments received during the comment period from August 6, 2021 to October 1, 2021.

More details about this review are available at NIST's Crypto Publication Review Project site.

## LIST OF COMMENTS

## 1. Canadian Centre for Cyber Security (CCCS), September 1, 2021

SP 800-38E is not a self-contained document, but is based on IEEE 1619-2007. This latter standard has been superseded by IEEE 1619-2018, so the updated SP 800-38E should make reference to the updated IEEE 1619-2018.

In particular, here are some noteworthy changes.

- Note that IEEE 1619-2018 specifies that that "The number of 128-b blocks within the data unit shall not exceed 2^20", so the additional requirement on the lengths of the data units referred to in Section 3 and discussed in Section 4 of SP 800-38E is now incorporated in IEEE 1619-2018.
- Clause 7 no longer appears in IEEE standard, so the reference to it (currently in Section 4, page 2) should be removed.
- Section 5.1 of IEEE 1619-2018 now mandates that the total number of 128-bit blocks shall not exceed 2^20, so the note in Section 4 of SP 800-38E regarding this subclause 5.1 should be removed.
- Note that IEEE 1619-2018 mandates that the number of 128-bit blocks in the data unit shall not exceed 2^64 (as opposed to 2^(128)-2 of the previous standard). This is not included in SP 800-38E and might be worth mentioning.

To be consistent with SP 800-38A, B, C, D, the note regarding conformance testing (currently last paragraph of Section 4) should appear in the Authority section.

The following is a useful paper to reference within the document as it settles the question of the security of ciphertext stealing, Matthew V. Ball, Cyril Guyot, James P. Hughes, Luther Martin & Landon Curt Noll (2012) The XTS-AES Disk Encryption Algorithm and the Security of Ciphertext Stealing, Cryptologia, 36:1, 70-79, DOI: 10.1080/01611194.2012.635115

## 2. Center for Cybersecurity Standards, National Security Agency, September 17, 2021

**Comments for SP 800-38E, *Recommendation for Block Cipher Modes of Operation: the XTS-AES Mode for Confidentiality on Storage Devices***

We reviewed this NIST Draft and appreciate this effort and the opportunity to provide the below comments from our SMEs for your consideration:

XTS-AES is approved in SP 800-38E by reference to IEEE Std. 1619-2007. The IEEE standard specifies a key, denoted by *Key*, that is 256 (or 512) bits long; *Key* is then parsed as the concatenation of two AES keys, denoted by *Key_1* and *Key_2*, that are 128 (or 256) bits long.

Misuse of XTS-AES with a class of improper keys results in a security vulnerability. An implementation of XTS-AES that improperly generates *Key* so that *Key_1* = *Key_2* is vulnerable to a chosen ciphertext attack that would defeat the main security assurances that XTS-AES was designed to provide. In particular, by obtaining the decryption of only one chosen ciphertext block in a given data sector, an adversary who does not know the key may be able to manipulate the ciphertext in that sector so that one or more plaintext blocks change to any desired value.

Currently the above security vulnerability is not discussed in SP 800-38E. IEEE Std. 1619-2007 mentions that XTS-AES uses separate keys for tweaking (*Key_2*) and encryption purposes (*Key_1*), but this is relegated to Annex D (in particular, section D.4.3) where it is less likely to be seen by algorithm implementers. Currently the only public guidance that mandates that the two AES keys in XTS-AES be distinct (i.e., *Key_1* ≠ *Key_2*) is Appendix A.9 of *Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program*. However, this guidance may not be widely known. In particular, we are aware of actual XTS-AES instantiations where the same AES key was used for both *Key_1* and *Key_2*. Prior to NIST's publication of SP 800-38E in 2010, public comments strongly endorsed using a single key, citing efficiency reasons and claiming (incorrectly) that "single-key" XTS-AES had been proven secure. This is likely another contributing factor to the perception that using the same key for *Key_1* and *Key_2* is acceptable.

As SP 800-38E is currently under review, this appears to be an appropriate opportunity to include an update in it regarding this vulnerability. We recommend updating SP 800-38E to include discussion about the dangers of using two AES keys, *Key_1* and *Key_2*, in XTS-AES that are equal. At the very least, we suggest pointing to the guidance given in Appendix A.9 of *Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program.*