P1619.1 Authenticated Encryption

Contributed by Administrator
Thursday, 19 July 2007
Last Updated Saturday, 05 April 2014

Standard for Authenticated Encryption with Length Expansion for Storage Devices

(Project 1619.1
September 15, 2006 -- updated June 7, 2007)

Scope: This standard specifies
requirements for cryptographic units that provide encryption and
authentication for data contained within storage media. Full
interchange requires additional specifications (such as compression
algorithms and physical data format) that are beyond the scope of this
standard.

P1619.1 Task Group Chair and Editor: Matt Ball

The IEEE P1619.1 task group has finished developing a standard for encryption and
authentication algorithms suitable for data storage devices that
support expanding blocks. All of these modes using the NIST-approved
AES-256 block cipher. The approved modes are as follows:

- CCM-128-AES-256: Counter mode encryption with cipher block chaining message authentication code.

- GCM-128-AES-256: Galois/Counter mode (counter mode encryption with 128-bit finite field message authentication code)

- CBC-AES-256-HMAC-SHA: Cipher block chaining mode for encryption with key-hash message authentication code using secure hashing algorithm.

- XTS-AES-256-HMAC-SHA: XTS encryption (see P1619) with key-hash message authentication code using secure hashing algorithm.

Project 1619.1 August 11, 2005, with update on September 15, 2006.

In December 2007, IEEE approved P1619.1 as IEEE Std 1619.1-2007. IEEE Std 1619-2007 is now available on-line at the IEEE store.

To purchase from the IEEE Store, follow these instructions:

- Go to http://www.ieee.org/

- Click on 'Shop' at the very top

- Click on the 'Standards' tab

- Click below 'Search Catalog' on the right side

- Click 'New Search'

- Enter '1619' into the Title/Keyword field and click 'Run Search'

- Add the appropriate standards to your Shopping Cart and check-out

For IEEE members, you can use IEEE Xplore (a different way to buy IEEE standards) if you or your company has a subscription to the Digital Library ($35/month).

IEEE 1619: http://ieeexplore.ieee.org/servlet/opac?punumber=4523925

DocumentsHere is the original GCM specification by McGrew and Viega, as referenced by P1619.1.

Errata

This is the informal errata on IEEE Std 1619-2007 based on discussion from the e-mail reflector. For official errata, see the IEEE errata sheets .

Annex C, Doc #6 and 4.6.2 Decryption inputs:

If the cryptographic unit is capable of returning plaintext before validating the MAC, then define the special signal PASS, describe how the host and/or controller receive such a signal, and define limits for the number of host records and bytes of plaintext that the cryptographic unit may return before checking the MAC.

The word “unit” is missing.

Test Vectors

For AES-256-CBC-HMAC-SHA-256 and AES-256-CBC-HMAC-SHA-512, test vector 2 contains the wrong TAG fields. These tags were generated without a CIV field and accordingly are not consistent with the published inputs. Test vector 2 in the standard should read as follows:

KEY 0000000000000000000000000000000000000000000000000000000000000000

HMK 0000000000000000000000000000000000000000000000000000000000000000

HMK 0000000000000000000000000000000000000000000000000000000000000000

AAD 00000000000000000000000000000000

NON N/A

CIV 00000000000000000000000000000000

HMAC-SHA-1

TAG 66040990c7992a2a00d037d0b8631c0db1785897

HMAC-SHA-256

TAG 33ad0a1c607ec03b09e6cd9893680ce210adf300aa1f2660e1b22e10f170f92a

HMAC-SHA-512

TAG bae46cebebbb90409abc5acf7ac21fdb339c01ce15192c52fb9e8aa11a8de9a4

TAG ea15a045f2be245fbb98916a9ae81b353e33b9c42a55380c5158241daeb3c6dd

See http://grouper.ieee.org/groups/1619/email/msg02863.html for additional background information.