The Consultative Committee for Space Data Systems

Draft Recommendation for
Space Data System Standards

CCSDS CRYPTOGRAPHIC ALGORITHMS

DRAFT RECOMMENDED STANDARD

CCSDS 352.0-P-1.1

PINK SHEETS

August 2018

The Consultative Committee for Space Data Systems

Draft Recommendation for
Space Data System Standards

CCSDS CRYPTOGRAPHIC ALGORITHMS

DRAFT RECOMMENDED STANDARD

CCSDS 352.0-P-1.1

PINK SHEETS

August 2018

3 ENCRYPTION ALGORITHMS

3.1 ALGORITHM AND MODE

In order to achieve a minimum baseline all CCSDS missions shall use the Advanced Encryption Standard algorithm (reference [1]) for encryption.

NOTE – The AES algorithm is specified in the National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 197 (reference [1]) and ISO/IEC 18033-3 (reference [12]).

3.2 CRYPTOGRAPHIC KEY SIZE

~~CCSDS implementations shall use a 128-bit key. A larger key size may be chosen for stronger security.~~

~~NOTE AES is key agile and supports key sizes of 128-bits, 192-bits, or 256-bits.~~

3.2.1 Future CCSDS implementations (for missions whose planning begins after the publication of issue 2 of this specification) shall use a 256-bit key.

3.2.2 Existing CCSDS implementations may use a 128-bit key.

3.3 ALGORITHM MODE OF OPERATION

CCSDS implementations shall use Counter Mode (references [2], [3], and [4]). Other modes of operation are allowed but should be carefully considered before use.

3.4 AUTHENTICATED ENCRYPTION

3.4.1 If encryption in combination with data integrity and origin authentication is required, implementations shall use Galois/Counter Mode (GCM) as specified in references [4] and [5] and [11].

3.4.2 The MAC 't' size shall be 128 bits.

NOTE – The cryptographic community has recognized that data encryption without data origin authentication often results in degraded security. As a result, several additional counter modes of operation that provide both encryption and data origin authentication have been specified. These modes are called Authenticated Encryption with Associated Data (AEAD). GCM can provide very high-speed authenticated encryption in hardware as well as in software. It can also be parallelized and pipelined, methods that can be very advantageous in the space community. It also does not require padding with extraneous, throwaway bits.

4.2.3 TRUNCATION ISSUES

4.2.3.1 CCSDS implementations should not truncate the length of the MAC resulting from HMAC.

4.2.3.2 The truncation, if performed, shall be agreed upon a priori by the communicating entities.

NOTE – Because of functional mission constraints (e.g., bandwidth, storage, frame size, packet size), truncation can be performed. HMAC had been specified in FIPS 198a (an earlier version of HMAC) as a ten-step process with the final step performing the truncation of the message authentication code by selecting only the leftmost *t-bits* from the total of *L-bits* generated by the hash algorithm. Truncation is now addressed in NIST Special Publication 800-107 (reference [7]). Truncation results in fewer bits being transmitted over the communications link and therefore reduced authentication algorithm overhead.

4.3 CIPHER-BASED AUTHENTICATION

4.3.1 Except as noted in 4.3.2, the Cipher Based Message Authentication Code (CMAC—reference [9]) shall be used if a cipher-based MAC is employed.

~~**4.3.1.1** CMAC shall use the AES algorithm using any of the following key sizes: 128-bit, 192-bit, or 256-bit.~~

~~**4.3.1.2** CCSDS implementations shall use at least a 128-bit key.~~

4.3.1.1 For future CCSDS implementations (for missions whose planning begins after the publication of issue 2 of this specification), CMAC shall use the AES algorithm using a 256-bit key size.

4.3.1.2 For existing CCSDS implementations, CMAC may use the AES algorithm using any of the following key sizes: 128-bit, 192-bit, or 256-bit.

4.3.2 The Galois Message Authentication Code (GMAC—reference [4]) may be used in place of CMAC when an authenticated encryption implementation is used for authentication only.

4.4 DIGITAL SIGNATURE BASED AUTHENTICATION

4.4.1 Digital Signature Standard (DSS—reference [8]) shall be used when using digital signature technology.

4.4.2 The Rivest-Shamir-Adleman (RSA) Digital Signature Algorithm (PKCS #1 version 2.1 as referred to in reference [8]) should be used.

~~**4.4.3** The RSA Digital Signature Algorithm key length shall be no less than 2048 bits.~~

~~NOTE The Digital Signature Standard (reference [8]) allows three different RSA modulus sizes to be used to construct the RSA public/private keys. The allowed sizes are 1024, 2048, 3072 bits. CCSDS has chosen to use a minimum modulus of 2048 bits.~~

4.4.3 For future CCSDS implementations (for missions whose planning begins after the publication of issue 2 of this specification), the RSA Digital Signature Algorithm key length shall be 4096 bits.

4.4.4 For existing CCSDS implementations, the RSA Digital Signature Algorithm key length may be 2048 bits.

4.4.5 Other DSS-specified algorithms such as the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA—reference [8]) may be used.

NOTES

1 The *Digital Signature Standard* (reference [8]) specifies several algorithms to construct and verify digital signatures: the Digital Signature Algorithm (DSA); the RSA Digital Signature Algorithm; and ECDSA.

2 For spacecraft without the ability to contact a key server to obtain public keys, a public key cache can be pre-loaded prior to launch, or public keys may be uploaded after launch or when additional keys or updated keys need to be loaded. This is probably not an issue for ground systems which are assumed to have robust network communications and access to a Public Key Infrastructure (PKI) or Certificate Authority (CA) (reference [B22]).