The Consultative Committee for Space Data Systems

Recommendation for Space Data System Standards

CCSDS CRYPTOGRAPHIC ALGORITHMS

RECOMMENDED STANDARD

CCSDS 352.0-B-1

BLUE BOOK

November 2012

The Consultative Committee for Space Data Systems

Recommendation for Space Data System Standards

CCSDS CRYPTOGRAPHIC ALGORITHMS

RECOMMENDED STANDARD

CCSDS 352.0-B-1

BLUE BOOK

November 2012

AUTHORITY

Issue:	Recommended Standard, Issue 1
Date:	November 2012
Location:	Washington, DC, USA

This document has been approved for publication by the Management Council of the Consultative Committee for Space Data Systems (CCSDS) and represents the consensus technical agreement of the participating CCSDS Member Agencies. The procedure for review and authorization of CCSDS documents is detailed in *Organization and Processes for the Consultative Committee for Space Data Systems*, and the record of Agency participation in the authorization of this document can be obtained from the CCSDS Secretariat at the address below.

This document is published and maintained by:

CCSDS Secretariat
Space Communications and Navigation Office, 7L70
Space Operations Mission Directorate
NASA Headquarters
Washington, DC 20546-0001, USA

STATEMENT OF INTENT

The Consultative Committee for Space Data Systems (CCSDS) is an organization officially established by the management of its members. The Committee meets periodically to address data systems problems that are common to all participants, and to formulate sound technical solutions to these problems. Inasmuch as participation in the CCSDS is completely voluntary, the results of Committee actions are termed **Recommended Standards** and are not considered binding on any Agency.

This **Recommended Standard** is issued by, and represents the consensus of, the CCSDS members. Endorsement of this **Recommendation** is entirely voluntary. Endorsement, however, indicates the following understandings:

- Whenever a member establishes a CCSDS-related **standard**, this **standard** will be in accord with the relevant **Recommended Standard**. Establishing such a **standard** does not preclude other provisions which a member may develop.
- Whenever a member establishes a CCSDS-related **standard**, that member will provide other CCSDS members with the following information:
  - -- The **standard** itself.
  - -- The anticipated date of initial operational capability.
  - -- The anticipated duration of operational service.
- Specific service arrangements shall be made via memoranda of agreement. Neither this **Recommended Standard** nor any ensuing **standard** is a substitute for a memorandum of agreement.

No later than three years from its date of issuance, this **Recommended Standard** will be reviewed by the CCSDS to determine whether it should: (1) remain in effect without change; (2) be changed to reflect the impact of new technologies, new requirements, or new directions; or (3) be retired or canceled.

In those instances when a new version of a **Recommended Standard** is issued, existing CCSDS-related member standards and implementations are not negated or deemed to be non-CCSDS compatible. It is the responsibility of each member to determine when such standards or implementations are to be modified. Each member is, however, strongly encouraged to direct planning for its new standards and implementations towards the later version of the Recommended Standard.

FOREWORD

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CCSDS shall not be held responsible for identifying any or all such patent rights.

Through the process of normal evolution, it is expected that expansion, deletion, or modification of this document may occur. This Recommended Standard is therefore subject to CCSDS document management and change control procedures, which are defined in *Organization and Processes for the Consultative Committee for Space Data Systems* (CCSDS A02.1-Y-3). Current versions of CCSDS documents are maintained at the CCSDS Web site:

http://www.ccsds.org/

Questions relating to the contents or status of this document should be addressed to the CCSDS Secretariat at the address indicated on page i.

At time of publication, the active Member and Observer Agencies of the CCSDS were:

Member Agencies

- Agenzia Spaziale Italiana (ASI)/Italy.
- Canadian Space Agency (CSA)/Canada.
- Centre National d'Etudes Spatiales (CNES)/France.
- China National Space Administration (CNSA)/People's Republic of China.
- Deutsches Zentrum für Luft- und Raumfahrt e.V. (DLR)/Germany.
- European Space Agency (ESA)/Europe.
- Federal Space Agency (FSA)/Russian Federation.
- Instituto Nacional de Pesquisas Espaciais (INPE)/Brazil.
- Japan Aerospace Exploration Agency (JAXA)/Japan.
- National Aeronautics and Space Administration (NASA)/USA.
- UK Space Agency/United Kingdom.

Observer Agencies

- Austrian Space Agency (ASA)/Austria.
- Belgian Federal Science Policy Office (BFSPO)/Belgium.
- Central Research Institute of Machine Building (TsNIIMash)/Russian Federation.
- China Satellite Launch and Tracking Control General, Beijing Institute of Tracking and Telecommunications Technology (CLTC/BITTT)/China.
- Chinese Academy of Sciences (CAS)/China.
- Chinese Academy of Space Technology (CAST)/China.
- Commonwealth Scientific and Industrial Research Organization (CSIRO)/Australia.
- CSIR Satellite Applications Centre (CSIR)/Republic of South Africa.
- Danish National Space Center (DNSC)/Denmark.
- Departamento de Ciência e Tecnologia Aeroespacial (DCTA)/Brazil.
- European Organization for the Exploitation of Meteorological Satellites (EUMETSAT)/Europe.
- European Telecommunications Satellite Organization (EUTELSAT)/Europe.
- Geo-Informatics and Space Technology Development Agency (GISTDA)/Thailand.
- Hellenic National Space Committee (HNSC)/Greece.
- Indian Space Research Organization (ISRO)/India.
- Institute of Space Research (IKI)/Russian Federation.
- KFKI Research Institute for Particle & Nuclear Physics (KFKI)/Hungary.
- Korea Aerospace Research Institute (KARI)/Korea.
- Ministry of Communications (MOC)/Israel.
- National Institute of Information and Communications Technology (NICT)/Japan.
- National Oceanic and Atmospheric Administration (NOAA)/USA.
- National Space Agency of the Republic of Kazakhstan (NSARK)/Kazakhstan.
- National Space Organization (NSPO)/Chinese Taipei.
- Naval Center for Space Technology (NCST)/USA.
- Scientific and Technological Research Council of Turkey (TUBITAK)/Turkey.
- Space and Upper Atmosphere Research Commission (SUPARCO)/Pakistan.
- Swedish Space Corporation (SSC)/Sweden.
- United States Geological Survey (USGS)/USA.

DOCUMENT CONTROL

Document	Title	Date	Status
CCSDS 352.0-B-1	CCSDS Cryptographic Algorithms, Recommended Standard, Issue 1	November 2012	Original issue

CONTENTS

1 INTRODUCTION

1.1 PURPOSE OF THIS RECOMMENDED STANDARD

This Recommended Standard provides the recommendation for standard CCSDS security algorithms.

A single, symmetric encryption algorithm is recommended for use by all CCSDS missions. In addition, a specific mode of operation for the algorithm is also recommended.

This Recommended Standard provides several alternative authentication/integrity algorithms which may be chosen for use by individual missions depending on their specific mission environments.

This Recommended Standard does not specify how, when, or where these algorithms should be implemented or used. Those specifics are left to the individual mission planners based on the mission security requirements and the results of the mission risk analysis. Suggestions for the use of these algorithms may be found in *The Application of CCSDS Protocols to Secure Systems* (reference [B1]), *Security Architecture for Space Data Systems* (reference [B17]), and *Space Data Link Security Protocol* (reference [B23]).

By using standardized, well-known algorithms, the use of high-quality cryptography and authentication is ensured, the potential rewards of economies of scale through the ability to buy off-the-shelf products is enabled, and the potential for interoperability among missions choosing the same algorithm is assured.

The implementer shall take into account that the use of this Recommended Standard alone does not mitigate all security risks related to confidentiality, integrity, and authentication. An information security risk assessment is necessary to identify additional security risks.

1.2 SCOPE

The algorithms contained in this document are recommended for use on space missions with a requirement for information (e.g., data, voice, and video) confidentiality, authentication, or authenticated confidentiality. The algorithms may be employed on any or all mission communications links such as the forward space link (e.g., telecommand), the return space link (e.g., telemetry, science data), as well as across the ground data network. They could as well be used to ensure confidentiality and authenticity of stored data.

A symmetric algorithm assumes that all communicating entities possess a shared secret (i.e., a ‘key’) which enables them to encrypt, decrypt, and authenticate information shared among them. The manner in which the shared secret is distributed and managed (key management) is not within the scope of this document. Further information on key management can be found in *Space Missions Key Management Concept* (reference [B22]).

1.3 APPLICABILITY

This Recommended Standard is applicable to all civilian space missions with a requirement for information confidentiality, authentication, and authenticated confidentiality.

While the use of security services is encouraged for all missions, particularly on command links, the results of a risk analysis may reduce or eliminate its need on a mission-by-mission basis.

1.4 RATIONALE

Traditionally, security mechanisms have not been employed on civilian space missions. In recognition of the increased threat, there has been a steady trend towards the integration of security services and mechanisms. For example, ground network infrastructures typically make use of *controlled* or *protected* networks. However, telecommands, telemetry, and science payload data, are still, for the most part, transmitted over unencrypted and unauthenticated Radio Frequency (RF) channels. As the threat environment becomes more hostile, this concept of operation becomes much more susceptible to attacks.

This CCSDS Cryptographic Algorithm Recommended Standard is necessary because of the increasing interconnection of ground networks; the movement towards *joy-sticking* of instruments by principal investigators; the decreasing costs for hardware, potentially allowing cheap *rogue* ground stations to be established; and national trends towards enhancing mission security. These recommended algorithms establish a set of common denominators among all missions for implementing information security services.

1.5 DOCUMENT STRUCTURE

Four sections and three annexes make up this document. Section 1 provides introductory information, definitions, nomenclature, and normative references. Section 2 provides background and rationale for choice of the algorithms. Section 3 describes the encryption algorithm. Section 4 describes the authentication algorithms. Annex A discusses security considerations related to use of symmetric encryption on the space link. Annex B provides informative references. Annex C is a glossary of abbreviations and acronyms used in the document.

1.6 NOMENCLATURE

1.6.1 NORMATIVE TEXT

The following conventions apply for the normative specifications in this Recommended Standard:

a) the words ‘shall’ and ‘must’ imply a binding and verifiable specification;

b) the word ‘should’ implies an optional, but desirable, specification;

c) the word ‘may’ implies an optional specification;

d) the words ‘is’, ‘are’, and ‘will’ imply statements of fact.

NOTE – These conventions do not imply constraints on diction in text that is clearly informative in nature.

1.6.2 INFORMATIVE TEXT

In the normative sections of this document (sections 3 and 4), informative text is set off from the normative specifications either in notes or under one of the following subsection headings:

– Overview;

– Background;

– Rationale;

– Discussion.

1.7 REFERENCES

The following documents contain provisions which, through reference in this text, constitute provisions of this Recommended Standard. At the time of publication, the editions indicated were valid. All documents are subject to revision, and users of this Recommended Standard are encouraged to investigate the possibility of applying the most recent editions of the documents indicated below. The CCSDS Secretariat maintains a register of currently valid CCSDS documents.

[1] *Advanced Encryption Standard (AES).* Federal Information Processing Standards Special Publication 197. Gaithersburg, Maryland: NIST, 2001.

[2] Morris Dworkin. *Recommendation for Block Cipher Modes of Operation: Methods and Techniques.* National Institute of Standards and Technology Special Publication 800-38A. Gaithersburg, Maryland: NIST, 2001.

[3] R. Housley. *Using Advanced Encryption Standard (AES) Counter Mode with IPsec Encapsulating Security Payload (ESP).* RFC 3686. Reston, Virginia: ISOC, January 2004.

[4] Morris Dworkin. *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC.* National Institute of Standards and Technology Special Publication 800-38D. Gaithersburg, Maryland: NIST, November 2007.

[5] J. Viega and D. McGrew. *The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)*. RFC 4106. Reston, Virginia: ISOC, June 2005.

[6] *The Keyed-Hash Message Authentication Code (HMAC)*. Federal Information Processing Standards Publication 198-1. Gaithersburg, Maryland: NIST, July 2008.

[7] Quynh Dang. *Recommendation for Applications Using Approved Hash Algorithms*. National Institute of Standards and Technology Special Publication 800-107. Gaithersburg, Maryland: NIST, February 2009.

[8] *Digital Signature Standard (DSS)*. Federal Information Processing Standards Publication 186-3. Gaithersburg, Maryland: NIST, June 2009.

[9] Morris Dworkin. *Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication*. National Institute of Standards and Technology Special Publication 800-38B. Gaithersburg, Maryland: NIST, May 2005.

[10] *Secure Hash Standard*. Federal Information Processing Standards Publication 180-4. Gaithersburg, Maryland: NIST, March 2012.

[11] *Information Technology—Security Techniques—Authenticated Encryption*. International Standard, ISO/IEC 19772:2009. Geneva: ISO, 2009.

[12] *Information Technology—Security Techniques—Encryption Algorithms—Part 3: Block Ciphers*. International Standard, ISO/IEC 18033-3:2010. 2nd ed. Geneva: ISO, 2010.

NOTE – Annex B contains informative references.

2 OVERVIEW

2.1 GENERAL OVERVIEW

This document contains recommendations for CCSDS cryptographic security algorithms for encryption, authenticated encryption, and authentication. Adoption of standard algorithms which are properly implemented will enable secure interoperability as well as reduce costs for missions utilizing security services. These algorithms are required to provide confidentiality and authentication/integrity protection for mission systems data.

A ground network may support numerous, simultaneous space missions utilizing many support personnel. Likewise, a single ground station may support multiple missions, and several spacecraft might use the same communications frequencies (using spacecraft IDs or Internet Protocol addresses to demultiplex data streams). A single spacecraft might host instruments and experiment packages from various universities, corporations, space agencies, or countries. All of these separate entities may have individual security concerns and may require that their respective data or commands be protected but intermixed with others. The CCSDS cryptographic algorithms can be utilized by the missions to provide the required protections to avoid loss of data or total mission loss.

2.2 ENCRYPTION OVERVIEW

Confidentiality is defined as the *assurance that information is not disclosed to unauthorized entities or processes*. In other words, those who are not authorized are prevented from obtaining information from the protected data. Confidentiality can be accomplished by various physical mechanisms which prevent access to information: locks, guards, or gates. For communications systems, there are essentially two mechanisms: (1) transmission through a physically protected medium (e.g., wire encased in alarmed conduit) and (2) cryptography.

For the CCSDS community, confidentiality must be implemented by cryptography for protection of information between end points that may be located on the ground and in space. In civilian space missions, confidentiality may be employed to ensure non-disclosure of information as it traverses the ground network, as it is transmitted between the ground and the spacecraft, between the spacecraft and the ground, and even on-board a spacecraft.

For human-crewed missions there are concerns regarding the confidentiality of medical information conveyed on-board, across the space link, and over ground communications infrastructures. Similarly, private communications between crew members and their families, such as voice and email, must also be afforded confidentiality.

CCSDS does not mandate at which layer the encryption algorithm is used. As is illustrated in the CCSDS document entitled *The Application of CCSDS Protocols to Secure Systems*, (CCSDS 350.0-G-2, reference [B1]), there are multiple locations within the space communications layering model where an encryption algorithm can be employed. As is pointed out in reference [B1], there is no *single* right answer for positioning and employing encryption. Depending on the system, encryption might be implemented within an

application (e.g., TLS/SSL, reference [B2]). It might be implemented above the Network Layer as with IPSec (references [B3] and [B4]). It might be employed at the Data Link Layer (e.g., Space Data Link Security, reference [B7]) or even at the Physical Layer (e.g., 'bulk encryption'). Or it might be employed simultaneously at multiple layers if that is advantageous to the system (e.g., at both the Network and Application Layers to provide ubiquitous as well as fine-grained security).

2.3 AUTHENTICATION/INTEGRITY OVERVIEW

2.3.1 GENERAL

Undetected data modification or corruption is a major concern. It could affect the integrity (correctness) of data received either on the ground from the spacecraft or on the spacecraft from the ground (i.e., what was received is exactly what was transmitted or any unauthorized modifications are detected and flagged). Modified or corrupted commands transmitted to the spacecraft could result in catastrophic results such as total mission loss. Modified or corrupted payload data from the spacecraft could result in erratic or wrong science. Modified or corrupted telemetry (e.g., housekeeping or engineering data) might be acted, upon resulting in a catastrophic event (e.g., telemetry indicates incorrect high onboard temperatures resulting in controller actions that could harm the spacecraft). The spacecraft/instrument must have the ability to recognize and discard unauthorized commands.

Authentication algorithms provide the basis for implementing authentication and integrity services. Regardless of where or how the authentication services are applied, an authentication algorithm must be employed. Authentication can be used to uniquely identify a person or an entity. It can also be used to identify a 'role' that a person has taken on (e.g., the controller of instrument X). Or, for example, it can be applied to uniquely identify a workstation or a group of workstations making up a control center. In this way, anything received which is claimed to have been sent from an individual (e.g., John Smith), an individual acting in a role (e.g., John Smith acting as the instrument X controller), or a facility (e.g., the mission control center) can be authenticated as actually having been sent by/from the claimed identity. The receiver is assured that the identity of the source of the data is authentic (e.g., person, place, role) and the data itself has not been altered or modified in transit without authorization or notification.

2.3.2 SYMMETRIC MESSAGE AUTHENTICATION CODES

For environments using symmetric keys (potentially along with symmetric encryption), one of two types of algorithms must be used to provide authentication/integrity: either hash-based or cipher-based.

Hash-based Message Authentication Codes (MAC) algorithms utilize cryptographic hash functions (e.g., SHA-256) and a shared secret (key). The data to be authenticated is concatenated with the shared secret and then the hash algorithm is run over the concatenated

data resulting in a fixed size MAC. The size of the message digest is strictly dependent on the specific hash algorithm used. Regardless of the size of the input data, the hash algorithm will always result in the fixed size MAC.

A cipher-based MAC can be constructed instead of a hash-based MAC. The cipher-based MAC uses a cryptographic algorithm (e.g., AES). The shared secret is used as the cryptographic key for the cryptographic algorithm which provides a MAC as a result. Cipher-based MACs may make better use of available resources when both authentication and confidentiality are required because a single algorithm can be used for both. In addition, cipher-based MACs may be more easily implemented in hardware than hash-based MACs.

2.3.3 DIGITAL SIGNATURE BASED AUTHENTICATION

For environments where public/private key cryptography is available, authentication and integrity may be accomplished using a digital signature algorithm (reference [8]).

The 'signer' (originator) performs a hash over the data to be signed using a hash algorithm (e.g., Secure Hash Algorithm [reference [10]]). The resultant hash word is then encrypted using the signer's private key to create the digital signature.

The receiver of the signed data verifies the signature on the received data to assure that the data came from the claimed entity and has not been modified. To authenticate the signature, the message digest is decrypted using the signer's public key.

The signer's public key can be sent with the data (and separately authenticated via the certificate authority's signature). It might already be cached by the receiver if previously obtained. Or it can be obtained from a public key server if it has been posted. If the message digest decryption is successful, it proves the authenticity of the signer's identity. The hash algorithm is then run on the received data and the resulting hash word is compared to the transmitted, decrypted hash word.

If they are identical, the data integrity is assured. This proves that no unauthorized or accidental modification of the data has occurred while it was in transit and that the data received at the destination is the exact same data as transmitted from the source.

2.4 AUTHENTICATED ENCRYPTION

Authenticated encryption is a cipher mode which provides the simultaneous security services of confidentiality, integrity, and authenticity. Authenticated encryption is also known as Authenticated Encryption with Associated Data (AEAD).

In general, authenticated encryption can be performed by combining an encryption algorithm with an authentication algorithm (e.g., MAC) as long as both are known to be secure against attack. It has been shown that encrypting data and then applying a MAC to the ciphertext implies security against an *adaptive chosen ciphertext attack*.

In addition, several different authenticated encryption modes have been developed such as Counter Mode with CBC-MAC (CCM), and Galois/Counter Mode (GCM). CCM has become a mandatory component of the IEEE 802.11i standard. GCM has been adopted for use with IEEE 802.1AE, IETF IPsec, SSH, and TLS/SSL.

It has been shown in the security community that the use of encryption by itself without authentication is dangerous (see reference [B6]). As a result of these findings, the use of non-authenticated encryption is highly discouraged for CCSDS missions.

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.

3.3 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 AUTHENTICATION ALGORITHMS

4.1 OVERVIEW

This section specifies message authentication algorithms that can be used by CCSDS depending on mission needs. These algorithms that can be used are:

– hash-based, or

– cipher-based, or

– digital signature-based.

CCSDS missions can use any of these algorithms to provide authentication services.

4.2 CCSDS HASH MESSAGE BASED AUTHENTICATION

4.2.1 GENERAL

The *Keyed Hash Message Authentication Code* as specified in FIPS 198-1 (reference [6]) shall be employed with modifications per this document.

4.2.2 HMAC HASH ALGORITHM

4.2.2.1 CCSDS HMAC implementations shall use SHA as specified in FIPS 180-4 (reference [10]).

4.2.2.2 CCSDS HMAC implementations shall normally use the SHA-256 variant (reference [10]) as illustrated in RFC 6234 (reference [B20]).

4.2.2.3 CCSDS implementations may use alternative hash algorithms such as SHA-224 (reference [10]), SHA-384 (reference [10]), SHA-512 (reference [10]), or RIPEMD-160 (reference [B14]), among others, with the HMAC algorithm.

4.2.2.3.1 The use of alternative hash algorithms shall be agreed upon by the communicating entities a priori or must be signaled to ensure compatibility and interoperability among mission components.

4.2.2.3.2 SHA-1 shall not be used.

NOTE – This is because of recent theoretical attacks against SHA-1 reducing its collision space.

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.

4.3.1.3 The MAC shall be at least 128 bits in length.

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.

4.4.4 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]).

ANNEX A

SECURITY, SANA, AND PATENT CONSIDERATIONS

(INFORMATIVE)

A1 SECURITY CONSIDERATIONS

A1.1 INTRODUCTION

This annex subsection discusses the various aspects of security with respect to cryptographic algorithms used by CCSDS-conformant missions. The two prime services provided by cryptographic algorithms are confidentiality and authentication.

Confidentiality is typically implemented by the use of encryption. Authentication is implemented by either hash-based or cipher-based message authentication codes. It can also be implemented by use of digital signatures.

Encryption uses a cryptographic algorithm by which information is made *opaque*. That is, it is not visible to unauthorized entities. The algorithm operates on *plaintext* information and the resulting output is transformed into *ciphertext* which, without the encryption key, is unreadable to maintain its confidentiality.

Authentication allows a receiver to establish, with assurance, the identity of the sender. Likewise, a receiver is also provided with assurance of data integrity: that the data has not undergone unauthorized modification or alteration in transit without being discovered.

A1.2 SECURITY CONCERNS WITH RESPECT TO THE CCSDS DOCUMENT

This document discusses security mechanisms, symmetric encryption, and authentication, which are used to provide confidentiality and integrity of information. Encryption prevents unauthorized disclosure of information. Therefore a casual observer or an active attacker would not be able to obtain the information. Authentication prevents unauthorized entities from sending information (e.g., commands) or modifying information without authorization.

A1.3 POTENTIAL THREATS AND ATTACK SCENARIOS

If information confidentiality is not provided, information may be disclosed to unauthorized entities. This could result in the loss of sensitive data, proprietary data, or privacy data (e.g., human-crewed mission medical information). As a result, the information might be obtained by an unauthorized eavesdropper listening to an RF transmission, a tap on a landline, or an unauthorized agency insider examining network traffic.

Information could be corrupted intentionally as a result of a malicious attack or unintentionally as a result of transmission errors. If the data has been corrupted for any reason, the receiver must be made aware of it because the integrity and authenticity of the data is suspect. Corrupted commands could result in a catastrophic mission loss. An attacker, aware of command construction principals, could try to inject false commands to the spacecraft in an attempt to take over control if the spacecraft does not employ command authentication.

If security services are employed by a mission, and the security services onboard do not operate correctly, there could be a total loss of communications if there is no bypass or any means by which to switch to a security bypass mode of operation.

A1.4 CONSEQUENCES OF NOT APPLYING SECURITY TO THE TECHNOLOGY

The unauthorized disclosure of information could result in total mission loss. If spacecraft commands were disclosed to unauthorized entities, unauthorized commands could be sent to the spacecraft. For example, performing an unauthorized thruster burn could result in the loss of a mission.

Unauthorized disclosure might result in the distribution of information to unauthorized entities when it had been agreed that principal investigators would have exclusive use of the information. It might also result in the disclosure of information which could have been for sale rather than given away (e.g., high resolution Earth observation imagery).

If authentication/integrity is not implemented, an attacker could inject false or unauthorized commands into a spacecraft's command chain, potentially taking over control of the spacecraft. This could result in the loss of a mission.

If the integrity of the data is not checked, a legitimate command might be corrupted but possibly still be recognized as a command. A corrupted command might be loaded into the flight computer and executed, resulting in probable damage to the spacecraft.

If corrupted data is sent to the ground (e.g., engineering data) indicating the spacecraft is having problems, a controller might react by sending a command to 'fix' something when in fact there is no problem. For example, corrupted data might indicate a loss of battery charge. A controller might react by pointing the spacecraft towards the sun potentially causing an overcharge or over-temperature situation resulting in spacecraft damage. Likewise, corrupted navigation data would result in incorrect spacecraft pointing which could result in battery discharge and loss of spacecraft power.

A2 SANA CONSIDERATIONS

The recommendations of this document do not require any action from SANA.

A3 PATENT CONSIDERATIONS

All algorithms referenced in this document are in the public domain, and there are no known patents that apply to the recommendations of this document.

ANNEX B

INFORMATIVE REFERENCES

(INFORMATIVE)

[B1] *The Application of CCSDS Protocols to Secure Systems*. Report Concerning Space Data System Standards, CCSDS 350.0-G-2. Green Book. Issue 2. Washington, D.C.: CCSDS, January 2006.

[B2] T. Dierks and E. Rescorla. *The Transport Layer Security (TLS) Protocol*. RFC 4346. Version 1.1. Reston, Virginia: ISOC, April 2006.

[B3] S. Kent and K. Seo. *Security Architecture for the Internet Protocol*. RFC 4301. Reston, Virginia: ISOC, December 2005.

[B4] S. Kent. *IP Encapsulating Security Payload (ESP)*. RFC 4303. Reston, Virginia: ISOC, December 2005.

[B5] C. Madson and R. Glenn. *The Use of HMAC-SHA-1-96 within ESP and AH*. RFC 2404. Reston, Virginia: ISOC, November 1998.

[B6] Steven M. Bellovin. "Problem Areas for the IP Security Protocols." In *Proceedings of the Sixth USENIX Security Symposium (July 22-25, 1996, San Jose, California)*. Berkeley, California: USENIX, 1996.

[B7] Space Data Link Security Concept of Operation. *Draft Report Concerning Space Data System Standards*, CCSDS 350.5-G-0. Draft Green Book. Under development.

[B8] D. McGrew and J. Viega. *The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH*. Reston, Virginia: ISOC, May 2006.

[B9] S. Frankel, R. Glenn, and R. Glenn. *The AES-CBC Cipher Algorithm and Its Use with IPsec*. RFC 3602. Reston, Virginia: ISOC, September 2003.

[B10] James Nechvatal, et al. "Report on the Development of the Advanced Encryption Standard (AES)." *Journal of Research of the National Institute of Standards and Technology* 106, no. 3 (May-June 2001): 511-576.

[B11] *Encryption Algorithm Trade Survey*. Report Concerning Space Data System Standards, CCSDS 350.2-G-1. Green Book. Issue 1. Washington, D.C.: CCSDS, March 2008.

[B12] *PKCS #1 v2.1: RSA Cryptography Standard*. Bedford, Massachusetts: RSA Laboratories, June 2002.

[B13] *PKCS #3: Diffie-Hellman Key-Agreement Standard*. Revised ed. Bedford, Massachusetts: RSA Laboratories, November 1993.

[B14] Hans Dobbertin, Antoon Bosselaers, and Bart Preneel. "RIPEMD-160: A Strengthened Version of RIPEMD." In *Fast Software Encryption: Third International Workshop, Cambridge, UK, February 21 - 23, 1996, Proceedings*, edited by Dieter Gollman, 71-82. Lecture Notes in Computer Science 1039. Berlin: Springer-Verlag, 1996.

[B15] J. Black, et al. "UMAC: Fast and Secure Message Authentication." In *Advances in Cryptology—CRYPTO '99: 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 1999, Proceedings*, edited by Michael Wiener, 216-233. Lecture Notes in Computer Science 1666. Berlin: Springer-Verlag, 1999.

[B16] M. Myers, et al. *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol—OCSP*. RFC 2560. Reston, Virginia: ISOC, June 1999.

[B17] *Security Architecture for Space Data Systems*. Draft Recommendation for Space Data System Practices, CCSDS 351.0-M-0. Draft Magenta Book. Issue 0. Washington, D.C.: CCSDS, September 2012.

[B18] *Security Threats against Space Missions*. Informational Report, CCSDS 350.1-G-. Green Book. Issue 1. Washington, D.C.: CCSDS, October 2006.

[B19] H. Krawczyk, M. Bellar, and M. Bellar. *HMAC: Keyed-Hashing for Message Authentication*. RFC 2104. Reston, Virginia: ISOC, February 1997.

[B20] D. Eastlake III and T. Hansen. *US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)*. RFC 4634. Reston, Virginia: ISOC, May 2011.

[B21] *Information Security Glossary of Terms*. Draft Report Concerning Space Data System Standards, CCSDS 350.8-G-0. Draft Green Book. Issue 0. Washington, D.C.: CCSDS, forthcoming.

[B22] *Space Missions Key Management Concept*. Report Concerning Space Data System Standards, CCSDS 350.6-G-1. Green Book. Issue 1. Washington, D.C.: CCSDS, November 2011.

[B23] *Space Data Link Security Protocol*. Draft Recommendation for Space Data System Standards, CCSDS 355.0-R-2. Red Book. Issue 2. Washington, D.C.: CCSDS, February 2012.

[B24] Nigel Smart, ed. *ECRYPT II Yearly Report on Algorithms and Keysizes (2009-2010)*. Revision 1.0. ICT-2007-216676. N.p.: ECRYPT II, March 2010.

[B25] Mihir Bellare and Chanathip Namprempre. "Authenticated Encryption: Relations among Notions and Analysis of the Generic Composition Paradigm." In *Advances in Cryptology — ASIACRYPT 2000: Proceedings of the 6th International Conference on the Theory and Application of Cryptology and Information Security (December 3–7, 2000, Kyoto, Japan)*, 531-545. Lecture Notes in Computer Science 1976. Berlin, Heidelberg: Springer, 2000.

NOTE – Normative references are listed in 1.7.

ANNEX C

ABBREVIATIONS AND ACRONYMS

(INFORMATIVE)

Term	Meaning
AEAD	Authenticated Encryption with Associated Data
AES	Advanced Encryption Standard
CA	Certificate Authority
CBC-MAC	Cipher Block Chaining Message Authentication Code
CCM	Counter with CBC-MAC
CMAC	Cipher Based Message Authentication Code
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
ECDSA	Elliptic Curve Digital Signature Algorithm
FIPS	Federal Information Processing Standard
GCM	Galois/Counter Mode
GMAC	Galois Message Authentication Code
HMAC	Hash-based Message Authentication Codes
IPsec	Internet Protocol Security
MAC	Message Authentication Code
NIST	National Institute of Standards and Technology
PKI	Public Key Infrastructure
RSA	Rivest-Shamir-Adleman
SHA	Secure Hash Algorithm
SSH	Secure Shell
SSL	Secure Sockets Layer
TLS	Transport Layer Security