The Consultative Committee for Space Data Systems

Recommendation for Space Data System Practices

SYMMETRIC KEY MANAGEMENT

RECOMMENDED PRACTICE

CCSDS 354.0-M-1

MAGENTA BOOK

December 2023

The Consultative Committee for Space Data Systems

Recommendation for Space Data System Practices

SYMMETRIC KEY MANAGEMENT

RECOMMENDED PRACTICE

CCSDS 354.0-M-1

MAGENTA BOOK

December 2023

AUTHORITY

Issue:	Recommended Practice, Issue 1
Date:	December 2023
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* (CCSDS A02.1-Y-4), and the record of Agency participation in the authorization of this document can be obtained from the CCSDS Secretariat at the email address below.

This document is published and maintained by:

CCSDS Secretariat
National Aeronautics and Space Administration
Washington, DC, USA
Email: secretariat@mailman.ccsds.org

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 **Recommendations** and are not in themselves considered binding on any Agency.

CCSDS Recommendations take two forms: **Recommended Standards** that are prescriptive and are the formal vehicles by which CCSDS Agencies create the standards that specify how elements of their space mission support infrastructure shall operate and interoperate with others; and **Recommended Practices** that are more descriptive in nature and are intended to provide general guidance about how to approach a particular problem associated with space mission support. This **Recommended Practice** is issued by, and represents the consensus of, the CCSDS members. Endorsement of this **Recommended Practice** is entirely voluntary and does not imply a commitment by any Agency or organization to implement its recommendations in a prescriptive sense.

No later than five years from its date of issuance, this **Recommended Practice** 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 Practice** is issued, existing CCSDS-related member Practices and implementations are not negated or deemed to be non-CCSDS compatible. It is the responsibility of each member to determine when such Practices or implementations are to be modified. Each member is, however, strongly encouraged to direct planning for its new Practices and implementations towards the later version of the Recommended Practice.

FOREWORD

Through the process of normal evolution, it is expected that expansion, deletion, or modification of this document may occur. This Recommended Practice is therefore subject to CCSDS document management and change control procedures, which are defined in the *Organization and Processes for the Consultative Committee for Space Data Systems* (CCSDS A02.1-Y-4). 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 sent to the CCSDS Secretariat at the email 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 (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 Science Policy Office (BELSPO)/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.
- China Academy of Space Technology (CAST)/China.
- Commonwealth Scientific and Industrial Research Organization (CSIRO)/Australia.
- Danish National Space Center (DNSC)/Denmark.
- Departamento de Ciência e Tecnologia Aeroespacial (DCTA)/Brazil.
- Electronics and Telecommunications Research Institute (ETRI)/Korea.
- Egyptian Space Agency (EgSA)/Egypt.
- 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.
- Hellenic Space Agency (HSA)/Greece.
- Indian Space Research Organization (ISRO)/India.
- Institute of Space Research (IKI)/Russian Federation.
- Korea Aerospace Research Institute (KARI)/Korea.
- Ministry of Communications (MOC)/Israel.
- Mohammed Bin Rashid Space Centre (MBRSC)/United Arab Emirates.
- 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.
- Netherlands Space Office (NSO)/The Netherlands.
- Research Institute for Particle & Nuclear Physics (KFKI)/Hungary.
- Scientific and Technological Research Council of Turkey (TUBITAK)/Turkey.
- South African National Space Agency (SANSA)/Republic of South Africa.
- Space and Upper Atmosphere Research Commission (SUPARCO)/Pakistan.
- Swedish Space Corporation (SSC)/Sweden.
- Swiss Space Office (SSO)/Switzerland.
- United States Geological Survey (USGS)/USA.

DOCUMENT CONTROL

Document	Title	Date	Status
CCSDS 354.0-M-1	Symmetric Key Management, Recommended Practice, Issue 1	December 2023	Original issue

CONTENTS

1 INTRODUCTION

1.1 PURPOSE OF THIS RECOMMENDED PRACTICE

This document recommends standard practices for CCSDS symmetric cryptographic key management. Key management provides the foundation for the secure generation, storage, distribution, use, and destruction of cryptographic keys. In particular, this document recommends types of cryptographic keys, a cryptographic key lifecycle, and abstract symmetric key management procedures for communication security in CCSDS-compliant space missions.

For the cryptographic key types and the cryptographic key lifecycle, a single methodology with several options is recommended. For key distribution procedures to support symmetric key management, a number of high-level procedures are recommended. All or a subset of these procedures can be instantiated into concrete procedures for specific security protocols, such as the SDLS Extended Procedures (reference [B10]).

This Recommended Practice specifies symmetric key management to support communication security cryptographic operations. It does not specify any cryptographic operations for the protection of information or data (those are specified in (reference [B2])). Guidelines on how to combine and integrate symmetric key management with cryptographic operations can be found in *The Application of CCSDS Protocols to Secure Systems* (reference [B3]) and *Security Architecture for Space Data Systems* (reference [B4]).

1.2 SCOPE

The specification contained in this document is recommended for use on space missions with a requirement for symmetric key management. Space missions with requirements for asymmetric or public key cryptosystems are not in the scope of this Recommended Practice. The specifications contained in this document may be employed to support cryptographic protection of any or all mission communications links, such as the forward space link (e.g., telecommand) or the return space link (e.g., telemetry, science data), as well as across the ground data network.

Symmetric key management mechanisms assume the presence of a secure side channel that allows secure distribution of an initial shared secret. The manner in which this initial shared secret is distributed and managed is left for individual agencies or missions to decide. *Space Missions Key Management Concept* (reference [B5]) and *Security Guide for Mission Planners* (reference [B6]) give some indications for mission planners on this topic.

This Recommended Practice requires some information (e.g., cryptographic keys) to be transmitted securely over an unprotected channel. It does not specify how the protection of this information is realized. *CCSDS Cryptographic Algorithms* (reference [B2]) recommends cryptographic algorithms that can be used for this purpose.

The recommended practices in this document are based, in part, on information documented in National Institute of Standards and Technology SP 800-57 (reference [B7] in this document).

1.3 APPLICABILITY

This Recommended Practice is applicable to space missions with a requirement for symmetric key management.

The need for and nature of security services implemented for space missions is determined by the outcome of a threat/risk analysis. Thus they may vary on a mission-by-mission basis.

The main audience of this document is space mission system developers and mission planners.

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 migration 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 dangerous.

The proper management of cryptographic keys is essential to the effective use of cryptography in communication security. Keys are analogous to the combination of a safe. If a safe combination is known to an adversary, the strongest safe provides no security against penetration. Similarly, poor key management may easily compromise strong algorithms. Ultimately, the security of information protected by cryptography directly depends on the strength of the keys, the effectiveness of mechanisms and protocols associated with the keys, and the protection afforded to the keys. All keys need to be protected against unauthorized disclosure. Key Management provides the foundation for the secure generation, storage, distribution, use, and destruction of keys.

This CCSDS Symmetric Key Management Recommended Practice is necessary to support key management operations and use of secure communication channels in space data systems. It enables the communication partners to exchange cryptographic keys, a necessary prerequisite for secure communications. It further specifies exactly the use of these keys to ensure a high level of security and interoperability.

1.5 DOCUMENT STRUCTURE

1.5.1 DOCUMENT ORGANIZATION

Four sections and two 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 symmetric key management recommendations as well as an overview of the document. Section 3 specifies cryptographic key types and hierarchies. Section 4 specifies the Key Management Services.

1.6 NOMENCLATURE

1.6.1 NORMATIVE TEXT

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

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, 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 DEFINITIONS

Most definitions used in this Recommended Practice are contained in reference [B8]. In addition, the following definition is used:

operational lifetime: The period in which a cryptographic key is in Active state and can be used for cryptographic operations.

Initiator: Entity initiating a procedure (proactive participant).

Recipient: Entity reacting to an initiated procedure (reactive participant).

1.8 REFERENCES

This document contains no normative references. Informative references are provided in annex B.

2 OVERVIEW

In a space-link communication security scenario, cryptography is used to protect transmitted information from unauthorized disclosure, to detect modification, and to authenticate the identities of ground or space entities (i.e., to provide confidentiality, integrity, and authenticity). Cryptographic techniques use cryptographic keys that are managed and protected throughout their lifecycles by a key management framework. Well implemented cryptography can reduce the scope of the information management problem from the need to protect large amounts of information or the cryptographic algorithms to the need to protect only keys and certain metadata (Kerckhoff Principle).

Spacecraft are isolated in space and operated fully remotely, only connected to the operator through modulated radio communication channels or optical links. Because of this, the installation of pre-shared information or secrets on board the spacecraft, is an option to reduce the complexity of the key management problem. It removes the advantages of asymmetric key management systems for key exchange between the operator and the spacecraft since there is no longer a need for establishing a key over an insecure medium. Furthermore, symmetric cryptosystems are generally less complex and less computationally expensive than asymmetric cryptosystems. For the above reasons (more details in reference [B5]), symmetric key cryptosystems are generally the preferred solution in the classic point-to-point space mission communication security scenarios. Nevertheless the concrete choice of cryptosystem for a specific mission should always be taken as a consequence of a thorough threat and risk assessment.

This symmetric key recommendation for space missions covers all technical symmetric key management aspects related to communication security that are required to successfully support a secure space link protocol such as the Space Data-Link Layer Security Protocol (reference [B9]). Non-technical aspects such as security governance, certification, and secure operations management are not addressed in this recommended practice. Non-communication security related aspects such as secure data storage, cryptographic key generation, key escrow, key backup, key renewal, and key reuse are not covered by this recommended practice.

The communication security symmetric key management elements specified by this Recommended Practice are:

- Cryptographic Key Types and Key Hierarchy (3.1): The key types required to successfully operate a secure space link protocol are specified, and the hierarchy in which they are to be organized is defined.
- Cryptographic Key Lifecycle (3.2): A key lifecycle specification is important to allow an interoperable operation of a secure space link protocol.
- Key Management Procedures (section 4): These procedures address the management of a cryptographic key management function. A recommendation for such procedures is important since it will allow the definition of a standardized set of key management procedures into service standards, such as application layer services, which are widely used throughout the space business. However, since the concrete implementation of these procedures is very specific to the target security protocol, only an abstract specification is provided as part of this Recommended Practice.

3 KEY TYPES AND KEY LIFECYCLE

3.1 KEY TYPES

3.1.1 GENERAL

All symmetric key management instances that are used in CCSDS missions for the purpose of communication security shall use only two categories of cryptographic keys:

a) Master Keys; and

b) Session Keys.

NOTE – The practical resistance of the key to attack and the key validity are very much mission-dependent and will be chosen based on the outcome of the mission risk assessment (see reference [B13]).

3.1.2 MASTER KEYS

3.1.2.1 Master Keys shall be used for the following purposes:

a) encryption or authenticated encryption of Session Keys for the purpose of Over-The-Air-Rekeying (OTAR) or Session Key generation;

b) authentication, encryption or authenticated encryption and authorization of specific onboard crypto unit commands and procedures.

NOTE – The specification of algorithms and procedures for the protection of Session Keys and for authentication or authenticated encryption of onboard crypto units is outside the scope of this Recommended Practice. This includes recovery procedures.

3.1.2.2 A specific Master Key shall be used for only one of the above purposes during its lifetime.

NOTE – Master Keys are used as static keys, recovery keys, or key encryption keys, depending on their concrete functionality.

3.1.2.3 The operational lifetime of a Master Key should not be exceeded. After the end of the operational lifetime the Master Key should be deactivated.

NOTE – This is considered secure practice, for example, in the case of a Master Key that is used as key encryption key. In some cases (e.g., if a Master Key is used as a recovery key), and if backed up by the mission threat and risk assessment, Master Keys can be used for a longer time.

3.1.3 SESSION KEYS

3.1.3.1 A hierarchy of Session Keys may exist, creating a multi-tiered system.

NOTE – The highest key rank is always the Master Key, but below that an arbitrary number of Session Key ranks may exist.

3.1.3.2 Session Keys shall be used for the following purposes:

a) authentication of information or data to be protected;

b) encryption of information or data to be protected;

c) authenticated encryption of information or data to be protected;

d) encryption or authenticated encryption of lower-tier Session Keys for the purpose of OTAR or Session Key generation.

NOTES

1 Session Keys are also called traffic-protection keys, traffic-encryption keys, or key encryption keys (in the case of protection of lower-tier Session Keys).

2 The specification of algorithms and procedures for authentication, encryption, and authenticated encryption is outside the scope of this Recommended Practice.

3.1.3.3 A specific Session Key shall be used for only one of the above purposes during its lifetime.

3.2 KEY LIFECYCLE

3.2.1 KEY LIFECYCLE STATE MODEL

3.2.1.1 The lifecycle for cryptographic keys is organized as a state model with a number of transition rules. The following states shall be present in the lifecycle for all cryptographic keys:

a) Pre-Activation state;

b) Active state;

c) Suspended state (optional);

d) Deactivated state;

e) Destroyed state.

3.2.1.2 The Suspended state represents a non-mandatory state and may be used by a mission.

3.2.1.3 A cryptographic key shall always be associated with exactly one state at a time during its lifetime.

3.2.1.4 The cycle of a cryptographic key shall start in Pre-Activation state and end in Destroyed state.

NOTE 1 – Figure 3-1 illustrates the possible key states and transitions as further detailed in the following subsections. Blue boxes represent key states, arrows represent transitions (details see 4.2). The red enclosure represents the states and transitions in which a key is considered valid.

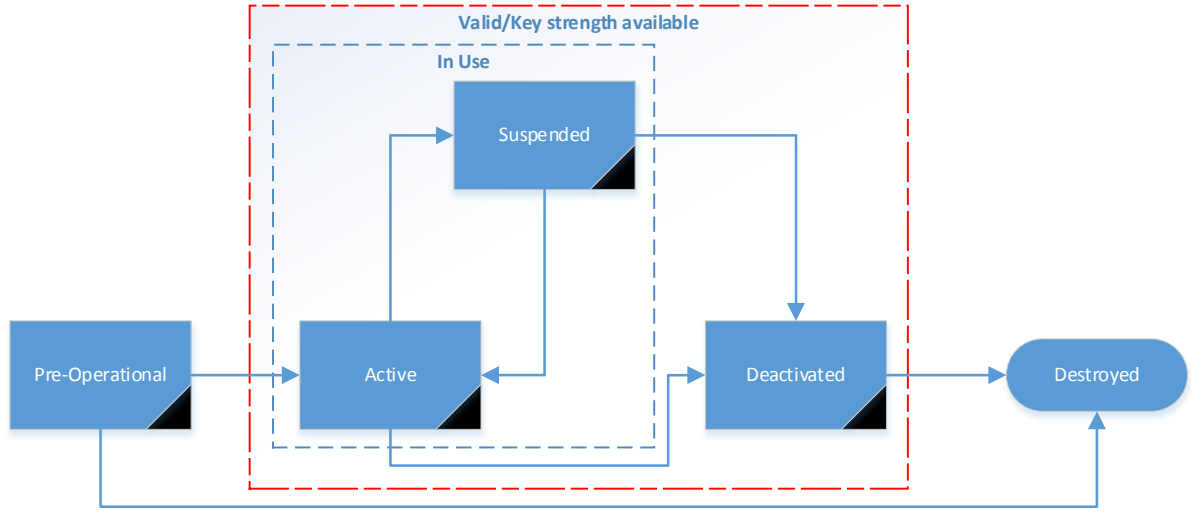

Figure 3-1: Key States and Transitions As Described in 4.2

NOTE 2 – A detailed description of the states is provided in the *Space Missions Key Management Concept* (reference [B5]).

3.2.2 PRE-ACTIVATION STATE

3.2.2.1 General

3.2.2.1.1 Newly generated cryptographic keys shall always be associated with Pre-Activation state.

3.2.2.1.2 If a secure environment cannot be guaranteed for key generation, the newly generated key should immediately transition to Active state.

3.2.2.1.3 Master Keys associated with Pre-Activation state shall always be communicated over a communication channel providing authenticated encryption or equal protection.

NOTE – The security of the Master Keys can also to be ensured with operational processes, for example, the applications of Secure Operating Procedures (SECOPS).

3.2.2.1.4 Session Keys associated with Pre-Activation state may be communicated over an unprotected communication channel if they are protected under a higher-tier Session Key or a Master Key.

3.2.2.1.5 Keys in pre-activation state that are securely distributed after generation shall remain in pre-activation state.

3.2.2.2 Transitions from Pre-Activation State

3.2.2.2.1 A cryptographic key associated with Pre-Activation state shall transition to Active state once it is activated.

NOTES

1 A cryptographic key that is selected but not yet used operationally can still be associated with Pre-Activation state.

2 Activation can happen through the Key Activation Procedure or as part of another procedure (e.g., OTAR).

3.2.2.2.2 A cryptographic key associated with Pre-Activation state may transition directly to Destroyed state.

NOTE – Special care has to be taken concerning the treatment of the last remaining Master Key associated with Pre-Activation state.

3.2.3 ACTIVE STATE

3.2.3.1 General

3.2.3.1.1 Operational lifetime constraints shall apply to all cryptographic keys associated with Active state. A cryptographic key shall start its operational lifetime once it has entered the Active state.

3.2.3.1.2 Only Master Keys associated with Active state may be used to support cryptographic operations as defined in 3.1.2.

3.2.3.1.3 Only Session Keys associated with Active state may be used to support cryptographic operations as defined in 3.1.3.

3.2.3.2 Transitions from Active State

3.2.3.2.1 A cryptographic key associated with Active state shall transition to Deactivated state if it has reached the end of its operational lifetime.

3.2.3.2.2 A cryptographic key associated with Active state shall transition to Deactivated state if a Key Deactivation procedure (see 4.3.2) is issued.

3.2.3.2.3 A cryptographic key associated with Active state may transition to the optional Suspended state, if used.

3.2.3.2.4 A cryptographic key shall transition to Destroyed state once the cryptographic key and all its copies are destroyed.

3.2.4 SUSPENDED STATE

3.2.4.1 Overview

The Suspended state allows for a key to be made non-operational without deactivating it. This means it can be made operational again (which is not possible for a deactivated key). Being suspended does not interrupt the operational lifetime of a key.

3.2.4.2 General

3.2.4.2.1 The Suspended state represents a non-mandatory (optional) state and may be used by a mission.

3.2.4.2.2 Cryptographic keys associated with Suspended state shall not be used to support cryptographic operations.

3.2.4.3 Transitions from Suspended State

3.2.4.3.1 A cryptographic key associated with Suspended state shall transition to Active state once it is used for cryptographic operations.

3.2.4.3.2 A cryptographic key associated with Suspended state shall transition to Deactivated state if a Key Deactivation procedure for it is issued.

3.2.4.3.3 A cryptographic key shall transition to Destroyed state once the cryptographic key and all its copies are destroyed.

3.2.5 DEACTIVATED STATE

3.2.5.1 Overview

The Deactivated state refers to all cryptographic keys that have reached the end of their operational lifetime (either because their lifetime has expired or it has been manually shortened) but are not yet destroyed. There is no limitation on the amount of time cryptographic keys can spend in Deactivated state.

3.2.5.2 General

3.2.5.2.1 Cryptographic keys associated with Deactivated state shall not be used to support cryptographic operations.

3.2.5.2.2 The continued use of a deactivated key shall be limited to processing of already-protected information.

NOTE – The purpose of this requirement is to guarantee continued access to protected data although the key is deactivated. Deactivated keys can only be used to decrypt formerly encrypted data but not to encrypt/authenticate new data.

3.2.5.3 Transitions from Deactivated State

A cryptographic key associated with Deactivated state shall transition to Destroyed state once the cryptographic key and all its copies are destroyed.

3.2.6 DESTROYED STATE

3.2.6.1 Overview

The Destroyed state refers to all cryptographic keys that have reached the end of their operational lifetimes and have been destroyed. It is not possible to retrieve any data that has been protected under a destroyed key.

3.2.6.2 Recommendation

The Destroyed state shall be the nominal end state of a key.

3.2.7 COMPROMISED KEYS

3.2.7.1 Overview

Cryptographic Keys in any operational state can be declared to be compromised. A cryptographic key that is compromised can no longer be trusted since it is assumed that it is no longer confidential (e.g., because it has been leaked, broken, or otherwise obtained by an unauthorized entity). A compromised or assumed compromised key can still be used for legacy operations as per its current state but should not be used for operational purposes. Compromise is not a state of the key but rather an attribute.

3.2.7.2 Compromised Key Attribute

A cryptographic key in any state may be assigned the attribute ‘compromised’.

3.2.7.3 Use of compromised keys

Cryptographic keys with the attribute ‘compromised’ should be limited to processing of already-protected information.

NOTE – Compromised keys should be handled very similar to deactivated keys. However, sometimes operational use of compromised keys cannot be avoided. In this case the operator needs to make a conscious decision on how to work with the compromised key based on a risk assessment.

4 KEY MANAGEMENT SERVICES

4.1 OVERVIEW

This section specifies a number of key management services that can be used to maintain cryptographic operations. They represent an exhaustive set. Not all of them need to be implemented by a mission requiring key management services, and some of them are even mutually exclusive. The specifications in this section are abstract. The number of keys or Key IDs in a set is a managed parameter.

4.2 SERVICE SPECIFICATIONS

The following key management service procedures may be supported by a symmetric key management system. They are applicable to both Master and Session Keys unless further specified in the list:

a) Key Activation;

b) Key Deactivation;

c) Key Destruction—only applicable to Session Keys;

d) Key Verification;

e) OTAR—only applicable to Session Keys;

f) Zeroize—only applicable to Session Keys;

g) Key Generation (key establishment)—only applicable to Session Keys;

h) Key Suspension; and

i) Key Un-Suspension.

4.3 KEY MANAGEMENT SERVICE PROCEDURES

4.3.1 KEY ACTIVATION

4.3.1.1 Overview

The Key Activation procedure activates a set of keys that are currently in Pre-Activation state. For example, this applies to previously uploaded Session Keys on the spacecraft (Recipient) side. These keys are then assigned the Active state and subsequently can be used for cryptographic operations. This means that the key lifetime has started.

4.3.1.2 Preconditions for the Procedure

The communicating entities shall have an identical set of Session Keys in Pre-Activation state.

4.3.1.3 Procedural Steps

4.3.1.3.1 General

The Key Activation procedure shall include the following mandatory execution steps:

a) Activation of Initiator Session Keys; role: Initiator;

b) Signaling of Key IDs to Be Activated; role: Initiator;

c) Activation of Recipient Session Keys; role: Recipient.

4.3.1.3.2 Activation of Initiator Session Keys

The Activation of Initiator Session Keys step shall:

a) be executed by the Initiator;

b) have the following input: the set of Key IDs of keys to be activated;

c) have the following output: all keys identified by the set of Key IDs in Active state;

d) execute the following: the Session Keys identified by the Key IDs in the set of Key IDs shall be transitioned from Pre-Activation state to Active state.

4.3.1.3.3 Signaling of Keys to Be Activated

The Signaling of Keys to Be Activated step shall:

a) be executed by the Initiator;

b) have the following input: the set of Key IDs of keys to be activated in step 4.3.1.3.2;

c) have the following output: the set of Key IDs of keys to be activated in step 4.3.1.3.2 transmitted to the Recipient;

d) execute the following: a message carrying the set of Key IDs to be activated shall be transmitted to the Recipient.

4.3.1.3.4 Activation of Recipient Session Keys

The Activation of Recipient Session Keys step shall:

a) be executed by the Recipient;

b) have the following input: the set of Key IDs of keys activated in step 4.3.1.3.2 received from the Initiator;

c) have the following output: all keys identified by the set of Key IDs in Active state;

d) execute the following: the Session Keys identified by the Key IDs in the set of Key IDs shall be transitioned from Pre-Activation state to Active state.

4.3.2 KEY DEACTIVATION

4.3.2.1 Overview

The Key Deactivation procedure deactivates a set of Session Keys at both ends of the communication channel. Deactivated keys can only be used to decrypt formerly encrypted data but not to encrypt/authenticate new data,. However, the keys are not (yet) destroyed.

4.3.2.2 Preconditions for the Procedure

The communicating entities shall have an identical set of Session Keys in either Pre-Activation, Active, or Suspended state.

NOTE – A subset of these Pre-Activation, Active, or Suspended keys is deactivated by this procedure.

4.3.2.3 Procedural Steps

4.3.2.3.1 General

The Key Deactivation procedure shall include the following mandatory execution steps:

a) Deactivation of Initiator Keys; role: Initiator;

b) Signaling of Key IDs to Be Deactivated; role: Initiator;

c) Deactivation of Recipient Keys; role: Recipient.

4.3.2.3.2 Deactivation of Initiator Keys

The Deactivation of Initiator Keys step shall:

a) be executed by the Initiator;

b) have the following input: the set of Key IDs of keys to be deactivated;

c) have the following output: all keys identified by the set of Key IDs in Deactivated state;

d) execute the following: the keys identified by the Key IDs in the set of Key IDs shall be transitioned from Active or Suspended state to Deactivated state.

4.3.2.3.3 Signaling of Keys to Be Deactivated

The Signaling of Keys to Be Deactivated step shall:

a) be executed by the Initiator;

b) have the following input: the set of Key IDs of keys to be deactivated in step 4.3.2.3.2;

c) have the following output: the set of Key IDs of keys to be deactivated in step 4.3.2.3.2 transmitted to the Recipient;

d) execute the following: a message carrying the set of Key IDs to be deactivated shall be transmitted to the Recipient.

4.3.2.3.4 Deactivation of Recipient Session Keys

The Deactivation of Recipient Session Keys step shall:

a) be executed by the Recipient;

b) have the following input: the set of Key IDs of keys deactivated in step 4.3.2.3.2 received from the Initiator;

c) have the following output: all keys identified by the set of Key IDs in Deactivated state;

d) execute the following: the keys identified by the Key IDs in the set of Key IDs shall be transitioned from Pre-Activation, Active, or Suspended state to Deactivated state.

4.3.3 KEY DESTRUCTION

4.3.3.1 Overview

The Key Destruction procedure destroys a set of Session Keys at both ends of the communication channel so that these keys are assigned the Destroyed state and subsequently are not available anymore.

4.3.3.2 Preconditions for the Procedure

Both entities shall have an identical set of Session Keys associated with Pre-Activation, Active, Suspended, or Deactivated state.

NOTE – Nominally, only deactivated keys should get destroyed. The other cases are to be considered exceptional.

4.3.3.3 Procedural Steps

4.3.3.3.1 General

The Key Destruction procedure shall include the following mandatory execution steps:

a) Destruction of Initiator Session Keys; role: Initiator;

b) Signaling of Key IDs to Be Destroyed; role: Initiator;

c) Destruction of Recipient Session Keys; role: Recipient;

4.3.3.3.2 Destruction of Initiator Session Keys

The Destruction of Initiator Session Keys step shall:

a) be executed by the Initiator;

b) have the following input: the set of Key IDs of keys to be destroyed;

c) have the following output: all keys identified by the set of Key IDs in Destroyed state;

d) execute the following: the Session Keys identified by the Key IDs in the set of Key IDs shall be transitioned to Destroyed state.

NOTE – The Initiator also needs to take care of the physical destruction of the keys at this point.

4.3.3.3.3 Signaling of Keys to Be Destroyed

The Signaling of Keys to Be Destroyed step shall:

a) be executed by the Initiator;

b) have the following input: the set of Key IDs of keys to be destroyed in step 4.3.3.3.2;

c) have the following output: the set of Key IDs of keys to be destroyed in step 4.3.3.3.2 transmitted to the Recipient;

d) execute the following: a message carrying the set of Key IDs of keys to be destroyed shall be transmitted to the Recipient.

4.3.3.3.4 Destruction of Recipient Session Keys

The Destruction of Recipient Session Keys step shall:

a) be executed by the Recipient;

b) have the following input: the set of Key IDs of keys destroyed in step 4.3.3.3.2 received from the Initiator;

c) have the following output: all keys identified by the set of Key IDs in Destroyed state;

d) execute the following: the Session Keys identified by the Key IDs in the set of Key IDs shall be transitioned to Destroyed state.

4.3.4 KEY VERIFICATION

4.3.4.1 Overview

The Key Verification procedure allows the verification and validation of a set of active Session Keys at the Recipient. This gives confirmation to the Initiator that the keys are not corrupted or modified and are fully operational. It should be noted that this procedure is not executed for Session Keys or static keys associated with the Pre-Activation state since those keys have not yet started their operational lifetime.

4.3.4.2 Preconditions for the Procedure

The communicating entities shall have an identical set of keys in Active state.

NOTE – A subset of these keys is verified by this procedure.

4.3.4.3 Procedure Steps

4.3.4.3.1 General

The Key Verification procedure shall incorporate the following mandatory steps:

a) Challenge Creation; role: Initiator;

b) Signaling of Challenges and Key IDs to Be Verified; role: Initiator;

c) Computation of Challenge Responses; role: Recipient;

d) Signaling of Challenge Responses; role: Recipient;

e) Response Verification; role: Initiator.

4.3.4.3.2 Challenge Creation

The Challenge Creation step shall:

a) be executed by the Initiator;

b) have the following input: the set of Key IDs of Session Keys to be verified;

c) have the following output: set of Challenges corresponding to the number of keys to be verified;

d) execute the following:

   1) for each key in the set of Key IDs, a Challenge shall be created in the set of Challenges;

   2) each Challenge shall be associated with a Key ID.

NOTE – The specification of the algorithm for the creation of the Challenges is outside the scope of this Recommended Practice.

4.3.4.3.3 Signaling of Challenges and Key IDs to Be Verified

The Signaling of Challenges and Key IDs to Be Verified step shall:

a) be executed by the Initiator;

b) have the following input: the set of Key IDs of keys to be verified and the set of Challenges created in step 4.3.4.3.2;

e) have the following output: Key IDs of keys to be verified and the set of Challenges transmitted to the Recipient;

f) execute the following: a Key Verification shall be created and transmitted to the Recipient.

4.3.4.3.4 Computation of Challenge Responses

The Computation of Challenge Responses step shall:

a) be executed by the Recipient;

b) have the following input: Key IDs to be verified and the set of Challenges received from the Initiator;

c) have the following output: the set of Challenge Responses;

d) execute the following: for each key in the set of Key IDs and each associated Challenge in the set of Challenges, a response shall be created in the set of Challenge Responses.

4.3.4.3.5 Signaling of Challenge Responses

The Signaling of Challenge Responses step shall:

a) be executed by the Recipient;

b) have the following input: the set of Key IDs and the set of Challenge Responses created in step 4.3.4.3.2;

c) have the following output: Key IDs and the set of Responses transmitted to the Initiator;

d) execute the following: a Key Verification Response shall be created and transmitted to the Initiator.

4.3.4.3.6 Challenge Response Verification

The Challenge Response Verification step shall:

a) be executed by the Initiator;

b) have the following input: Key IDs and the set of Challenge Responses transmitted to the Recipient;

c) have the following output: verification results associated with each key in the set of Key IDs;

d) execute the following:

   1) for each key in the set of Key IDs and each associated response in the set of Challenge Responses, the challenge shall be computed and compared with the associated challenge in the set of Challenges;

   2) in case of a match, the Session Key shall be verified.

4.3.5 OVER-THE-AIR-REKEYING

4.3.5.1 Overview

OTAR addresses the secure (encrypted and authenticated) transmission of Session Keys over a communication channel from the Initiator to the Recipient for the purposes of rekeying. The implementation of the installation of the keys on the Recipient side is mission specific.

4.3.5.2 Preconditions for the Procedure

4.3.5.2.1 The Initiator shall have available a set of Session Keys in Pre-Activation state.

NOTE – These are the keys that are to be transferred to the Recipient.

4.3.5.2.2 Both entities shall have an identical Master Key in Pre-Activation or Active state.

NOTE – This is the Master Key that will be used to ensure confidentiality of the Session Keys during transmission from the Initiator to the Recipient.

4.3.5.3 Procedure Steps

4.3.5.3.1 General

The OTAR procedure shall incorporate the following mandatory steps:

a) Encryption of Set of Session Keys; role: Initiator;

b) Signaling of Set of Encrypted Session Keys, role: Initiator;

c) Processing of Protected Set of Session Keys; role: Recipient.

4.3.5.3.2 Protection of Set of Session Keys

The Protection of Set of Session Keys step shall:

a) be executed by the Initiator;

b) have the following inputs:

   1) set of Session Keys,

   2) Key ID of the Master Key;

c) have the following outputs:

   1) Protected Set of Session Keys ready for upload, consisting of pairs of Key ID and Key: the whole set needs to be authenticated through a MAC,

   2) Master Key in Active state;

d) execute the following:

   1) the state of the Master Key identified by the Key ID of the Master Key shall be transitioned to Active state if the Master Key is not already in Active state,

   2) authenticated encryption under the selected Master Key shall be applied to the (Key ID, Key) pairs to create the Protected Set of Session Keys:

i) this shall be done using the agreed upon cryptographic algorithm under the Master Key identified by the Master Key ID,

ii) the Initialization Vector and MAC parameters shall be populated accordingly.

4.3.5.3.3 Signaling of Set of Protected Session Keys

The Signaling of Set of Protected Session Keys step shall:

a) be executed by the Initiator;

b) have the following input: Protected Set of Session Keys;

c) have the following output: the Protected Set of Session Keys and the Key ID of the Master Key transmitted to the Recipient;

d) execute the following: a message carrying the Protected Set of Session Keys and the Key ID of the Master Key shall be created and transmitted.

4.3.5.3.4 Processing of Set of Protected Session Keys

The Processing of Set of Protected Session Keys step shall:

a) be executed by the Recipient;

b) have the following input: the Protected Set of Session Keys and the Key ID of the Master Key received from the Initiator;

e) have the following output: set of authenticated and decrypted Session Keys in Pre-Activation state;

f) execute the following:

1) the Recipient shall perform the authentication and decryption of the set of Protected Session Keys using the Initialization Vector and MAC parameters as input to the authentication algorithm execution under the Master Key identified by the Master Key ID;

2) for each decrypted Session Key, the Recipient shall store it in Pre-Activation state using the indicated Session Key ID.

NOTE – This may or may not imply that other keys that are stored at the indicated Session Key ID are overridden. Proper management of the key memory is not the subject of this Recommended Practice and is mission specific.

4.3.6 ZEROIZE

4.3.6.1 Overview

The Zeroize procedure allows the initiator to request the wiping of the Recipient's entire volatile key store. This could become necessary, for example, in the case of suspected corruption of the Recipient's volatile key store. Master Keys are not affected by the Zeroize procedure since they are not stored in the volatile key store. The technical solution for implementation of the Zeroize procedure is outside the scope of this Recommended Practice.

4.3.6.2 Preconditions for the Procedure

This procedure has no pre-conditions.

4.3.6.3 Procedure Steps

4.3.6.3.1 General

The Zeroize procedure shall incorporate the following mandatory steps:

a) Signaling of Zeroize Request; role: Initiator;

b) Wiping of Key Store and Computation of Zeroize Response; role: Recipient;

c) Signaling of Zeroize Response; role: Recipient.

NOTE – The procedure does not result in the wiping of the key store at the Initiator side.

4.3.6.3.2 Signaling of Zeroize Request

The Signaling of Zeroize Request step shall:

a) be executed by the Initiator;

b) have the following input: none;

c) have the following output: Zeroize Request transmitted to the Recipient;

d) execute the following: a message sent to the Recipient with the request for wiping the key store.

4.3.6.3.3 Wiping of Key Store

The Wiping of Key Store step shall:

a) be executed by the Recipient;

b) have the following input: Zeroize Request received from the Initiator;

c) have the following output: Key Store wiped;

d) execute the following: upon reception of the Zeroize Request, the Recipient shall wipe the complete volatile key store memory.

NOTE – The Wiping process is implementation specific according to applicable policy.

4.3.6.3.4 Signaling of Zeroize Response

The Signaling of Zeroize Response step shall:

a) be executed by the Recipient;

b) have the following input: completion of step 4.3.6.3.3;

c) have the following output: Zeroize report transmitted to the Initiator;

d) execute the following: a Zeroize report message is to be generated and sent to the Initiator indicating either a successful or unsuccessful (error case) wiping of the key store.

4.3.7 KEY GENERATION

4.3.7.1 Overview

Key Generation provides the creation of new Recipient side Session Keys at the request of the Initiator. This process is also called Key Establishment. A Master Key is used for the generation of the new Session Keys.

4.3.7.2 Preconditions for the Procedure

Both entities shall have an identical Master Key in Pre-Activation state.

NOTE – This is the Master Key that will be used to ensure the secure generation of the Session Keys at the Recipient.

4.3.7.3 Procedure Steps

4.3.7.3.1 General

The Key Generation procedure shall incorporate the following mandatory steps:

a) Generation of Session Keys; role: Initiator;

b) Signaling of Master Key ID for Session Key Generation; role: Initiator;

c) Generation of Session Keys; role: Recipient.

4.3.7.3.2 Generation of Session Keys

The Generation of Session Keys step shall:

a) be executed by the Initiator;

b) have the following inputs:

   1) set of Key IDs of the Session Keys to be generated,

   2) Key ID of the Master Key;

c) have the following outputs:

   1) set of newly generated Session Keys,

   2) Master Key in Active state;

d) execute the following:

   1) the state of the Master Key identified by the Key ID of the Master Key shall be transitioned to Active state,

   2) for each Key ID in the set of Session Key IDs, the Initiator shall generate a new Session Key using an agreed-upon cryptographic generation algorithm and taking the Master Key identified by the Key ID as input parameter.

   NOTE – The cryptographic algorithm to be used for the generation of keys is outside the scope of this recommendation.

4.3.7.3.2.1 Signaling of Master Key ID for Session Key Generation

The Signaling of Master Key ID for Session Key Generation step shall

a) be executed by the Initiator;

b) have the following input: Key ID of the Master Key used for generation of the Session Keys in step 4.3.7.3.2;

c) have the following output: Key ID of the Master Key and the set of Session Key IDs transmitted to the Recipient;

d) execute the following: a message carrying the Key ID of the Master Key and the set of Session Key IDs shall be created and transmitted.

4.3.7.3.3 Generation of Session Keys

The Generation of Session Keys step shall

a) be executed by the Recipient;

b) have the following input: the Key ID of the Master Key and the set of Session Key IDs received from the Initiator;

c) have the following output: newly generated Session Keys;

d) execute the following:

   1) the Master Key identified by the Key ID shall be transitioned to Active state,

   2) for Key IDs in the set of received Session Key IDs,

      i) the Recipient shall generate a new Session Key using a cryptographic Key Generation algorithm and the Master Key identified by the Key ID of the Master Key as input,

      ii) the new Session Keys shall then be stored in the storage field associated with the respective Key ID from the set of Key IDs.

4.3.8 KEY SUSPENSION

4.3.8.1 Overview

The Key Suspension procedure allows the initiator to request the suspension of a set of keys on the Recipient side. The main purpose of this procedure is to disable a set of keys temporarily.

4.3.8.2 Preconditions for the Procedure

Both entities shall have an identical set of keys in Active state.

4.3.8.3 Procedure Steps

4.3.8.3.1 General

The Key Suspension procedure shall incorporate the following mandatory steps:

a) Suspension of the Set of Keys; role: Initiator;

b) Signaling of the Set of Keys IDs of the Suspended Keys; role: Initiator;

c) Suspension of the Set of Keys; role: Recipient.

4.3.8.3.2 Suspension of the Set of Keys at Initiator Side

The Suspension of the Set of Keys step shall:

a) be executed by the Initiator;

b) have the following input: set of Key IDs of keys to be suspended;

c) have the following output: set of keys identified by the set of Key IDs has been transitioned from Active state to Suspended state;

d) execute the following: the set of keys identified by the set of Key IDs shall be transitioned from Active state to Suspended state.

4.3.8.3.3 Signaling of the Set of Key IDs of the Suspended Set of Keys

The Signaling of the Set of Key IDs of the Suspended Set of Keys step shall:

a) be executed by the Initiator;

b) have the following input: set of Key IDs of the Keys that have been suspended;

c) have the following output: set of Key IDs transmitted to the Recipient;

d) execute the following: a message carrying the set of Key IDs of the Keys to be suspended shall be created and transmitted.

4.3.8.3.4 Suspension of the Set of Keys at Recipient Side

The Suspension of the Set of Keys step shall:

a) be executed by the Recipient;

b) have the following input: set of Key IDs of the set of keys to be suspended received from the Initiator;

c) have the following output: set of keys identified by the set of Key IDs received from the Initiator have been transitioned from Active state to Suspended state;

d) execute the following: the set of keys identified by the set of Key IDs received from the Initiator shall be transitioned from Active state to Suspended state.

4.3.9 KEY UN-SUSPENSION

4.3.9.1 Overview

The Key Un-Suspension procedure allows the Initiator to request the un-suspension of a set of keys on the Recipient side. The main purpose of this procedure is to re-enable a temporarily disabled set of keys.

4.3.9.2 Preconditions for the Procedure

Both entities shall have an identical set of keys in Suspended state.

4.3.9.3 Procedure Steps

4.3.9.3.1 General

The Key Un-Suspension procedure shall incorporate the following mandatory steps:

a) Un-Suspension of the Set of Keys; role: Initiator;

b) Signaling of the Set of Key IDs of the Un-Suspended Keys; role: Initiator;

c) Un-Suspension of the Set of Keys; role: Recipient.

4.3.9.3.2 Un-Suspension of the Set of Keys at Initiator Side

The Un-Suspension of the Set of Keys step shall:

a) be executed by the Initiator;

b) have the following input: set of Key IDs of keys to be un-suspended;

c) have the following output: keys identified by the set of Key IDs have been transitioned from Suspended to Active state.

4.3.9.3.3 Signaling of the Set of Key IDs of the Un-Suspended Keys

The Signaling of the Set of Key IDs of the Un-Suspended Keys step shall:

a) be executed by the Initiator;

b) have the following input: set of Key ID of the keys that have been un-suspended;

c) have the following output: set of Key IDs transmitted to the Recipient;

d) execute the following: a message carrying the set of Key IDs of the keys to be un-suspended shall be created and transmitted.

4.3.9.3.4 Un-Suspension of the Set of Keys at Recipient Side

The Un-Suspension of the Set of Keys step shall:

a) be executed by the Recipient;

b) have the following input: set of Key IDs of the keys to be un-suspended received from the Initiator;

e) have the following output: set of keys identified by the set of Key IDs received from the Initiator that has been transitioned from Suspended state to Active state;

f) execute the following: set of keys identified by the set of Key IDs received from the Initiator shall be transitioned from Suspended state to Active state.

ANNEX A

SECURITY

(INFORMATIVE)

A1 SECURITY CONSIDERATIONS

A1.1 INTRODUCTION

Communications security attempts to ensure the confidentiality, integrity, and/or authenticity of transmitted data, as required depending on the threat, the mission security policy(s), and the desire of the mission planners. It is possible for a single data unit to require all three of these security attributes to ensure that the transmitted data is not disclosed, not altered, and not spoofed.

A1.2 SECURITY CONCERNS WITH RESPECT TO THE CCSDS DOCUMENT

Security concerns specific to the Key Management design are addressed in more detail in reference [B5]. Key Management is intended to support cryptographic operations that operate at one or more layers of the protocol stack. In order to function properly, key management needs to employ to use of cryptographic algorithms. CCSDS recommends cryptographic algorithms for this purpose in reference [B3].

A1.3 DATA PRIVACY

As necessary, this Recommended Practice mandates the use of data encryption. This applies in particular to the transmission of Session Keys using the OTAR process (see 4.3.5).

In addition, it is recommended that the confidentiality of the key management messages specified as part of this Recommended Practice be further protected by security protocols such as the Space Data Link Security (SDLS) Protocol (reference [B9]) and the SDLS Extended Procedures (reference [B10]).

A1.4 DATA INTEGRITY

As necessary, this Recommended Practice mandates the use of data integrity mechanisms. This applies in particular to the transmission of Session Keys using the OTAR process (see 4.3.5). In addition, it is recommended that the integrity of the key management messages that are specified as part of this Recommended Practice be further protected by a security protocol such as SDLS.

A1.5 AUTHENTICATION OF COMMUNICATING ENTITIES

In the context of this Recommended Practice, the provision of data integrity (see A1.4) will also allow authentication of the communicating entities.

A1.6 POTENTIAL THREATS AND ATTACK SCENARIOS

Symmetric key management, as specified in this Recommended Practice, constitutes one element in an overall framework of security mechanisms that help to reduce the risk of successful attacks on the communication link between the two entities of a point-to-point communication session. Reference [B3] provides an overview on the complete framework.

Attack scenarios that specifically target the key management process are the following:

- Cryptographic Key Corruption: The attacker gains knowledge of a Session or Master Key. In general, there is no immediate way to uncover this corruption. However, once a key corruption is suspected, the key in question needs to be replaced as soon as practically possible.
- Interception of Key Management Communication: The attacker intercepts messages that are being transmitted as part of the Key Management Services specified in this Recommended Practice with the intention either to obtain knowledge of a specific key (see Cryptographic Key Corruption) or to interfere with the Key Management Service. This Recommended Practice provides specific means for protection of the OTAR key management service. However, it is assumed that all key management communication is protected by a security protocol such as the Space Data-Link Layer Security Protocol.

A1.7 CONSEQUENCES OF NOT APPLYING SECURITY TO THE TECHNOLOGY

The consequences of not applying security to space communication technologies are outlined in detail in reference [B13].

ANNEX B

INFORMATIVE REFERENCES

(INFORMATIVE)

[B1] *Information Technology—Open Systems Interconnection—Basic Reference Model: The Basic Model*. 2nd ed. International Standard, ISO/IEC 7498-1:1994. Geneva: ISO, 1994.

[B2] *CCSDS Cryptographic Algorithms*. Issue 2. Recommendation for Space Data System Standards (Blue Book), CCSDS 352.0-B-2. Washington, D.C.: CCSDS, August 2019.

[B3] *The Application of Security to CCSDS Protocols*. Issue 3. Report Concerning Space Data System Standards (Green Book), CCSDS 350.0-G-3. Washington, D.C.: CCSDS, March 2019.

[B4] *Security Architecture for Space Data Systems*. Issue 1. Recommendation for Space Data System Practices (Magenta Book), CCSDS 351.0-M-1. Washington, D.C.: CCSDS, November 2012.

[B5] *Space Missions Key Management Concept*. Issue 1. Report Concerning Space Data System Standards (Green Book), CCSDS 350.6-G-1. Washington, D.C.: CCSDS, November 2011.

[B6] *Security Guide for Mission Planners*. Issue 2. Report Concerning Space Data System Standards (Green Book), CCSDS 350.7-G-2. Washington, D.C.: CCSDS, April 2019.

[B7] Elaine Barker. *Recommendation for Key Management—Part 1: General*. Revision 5. National Institute of Standards and Technology Special Publication 800-57. Gaithersburg, Maryland: NIST, May 2020.

[B8] *Information Security Glossary of Terms*. Issue 2. Recommendation for Space Data System Practices (Magenta Book), CCSDS 350.8-M-2. Washington, D.C.: CCSDS, February 2020.

[B9] *Space Data Link Security Protocol*. Issue 2. Recommendation for Space Data System Standards (Blue Book), CCSDS 355.0-B-2. Washington, D.C.: CCSDS, July 2022.

[B10] *Space Data Link Security Protocol—Extended Procedures*. Issue 1. Recommendation for Space Data System Standards (Blue Book), CCSDS 355.1-B-1. Washington, D.C.: CCSDS, February 2020.

[B11] *Overview of Space Communications Protocols*. Issue 4. Report Concerning Space Data System Standards (Green Book), CCSDS 130.0-G-4. Washington, D.C.: CCSDS, April 2023.

[B12] *Glossary of Key Information Security Terms*. Rev. 1. Edited by Richard Kissel. NIST IR 7298. Gaithersburg, Maryland: NIST, February 2011.

[B13] *Security Threats against Space Missions*. Issue 3. Report Concerning Space Data System Standards (Green Book), CCSDS 350.1-G-3. Washington, D.C.: CCSDS, February 2022.