The Consultative Committee for Space Data Systems

Draft Recommendation for
Space Data System Practices

SYMMETRIC KEY MANAGEMENT

DRAFT RECOMMENDED PRACTICE

CCSDS 354.0-R-1

RED BOOK

June 2018

The Consultative Committee for Space Data Systems

Draft Recommendation for
Space Data System Practices

SYMMETRIC KEY MANAGEMENT

DRAFT RECOMMENDED PRACTICE

CCSDS 354.0-R-1

RED BOOK

June 2018

AUTHORITY

Issue:	Red Book, Issue 1
Date:	June 2018
Location:	Not Applicable

(WHEN THIS RECOMMENDED PRACTICE IS FINALIZED, IT WILL CONTAIN THE FOLLOWING STATEMENT OF AUTHORITY:)

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 e-mail address below.

This document is published and maintained by:

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

STATEMENT OF INTENT

(WHEN THIS RECOMMENDED PRACTICE IS FINALIZED, IT WILL CONTAIN THE FOLLOWING 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 e-mail 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 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.
- Danish National Space Center (DNSC)/Denmark.
- Departamento de Ciência e Tecnologia Aeroespacial (DCTA)/Brazil.
- Electronics and Telecommunications Research Institute (ETRI)/Korea.
- 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.
- 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.
- 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.

PREFACE

This document is a draft CCSDS Recommended Practice. Its 'Red Book' status indicates that the CCSDS believes the document to be technically mature and has released it for formal review by appropriate technical organizations. As such, its technical contents are not stable, and several iterations of it may occur in response to comments received during the review process.

Implementers are cautioned **not** to fabricate any final equipment in accordance with this document's technical content.

DOCUMENT CONTROL

Document	Title	Date	Status
CCSDS 354.0-R-1	Symmetric Key Management, Draft Recommended Practice, Issue 1	June 2018	Current draft

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 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.

This Recommended Practice specifies symmetric key management to support 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 (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.

While the use of security services is encouraged for all missions, the results of a threat/risk analysis and the realities of schedule/cost drivers may reduce or eliminate its need on a mission-by-mission basis.

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

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 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

All definitions used in this Recommended Practice are contained in reference [B8].

1.8 REFERENCES

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

2 OVERVIEW

Cryptography is used to protect 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). It is particularly useful when data transmission or authentication occurs over communication channels for which physical means of protection are often cost-prohibitive or even impossible to achieve. The space link is such a communication channel.

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 to the need to protect only keys and certain metadata (Kerkhoff Principle).

For several reasons (see reference [B5]), symmetric key crypto systems have been proven to be superior to asymmetric crypto systems in classical point-to-point space mission scenarios. This symmetric key recommendation for space missions covers all symmetric key management aspects that are required to successfully support the operation of a secure space link protocol such as the Space Data-Link Layer Security Protocol (reference [B9]). The individual aspects covered by this Recommended Practice are:

- Cryptographic Key Types and Key Hierarchy (3.1): The key types required to successfully operate all aspects of a secure space link protocol are specified, and the hierarchy in which they must be organized is defined.
- Cryptographic Key Lifecycle (3.2): A key lifecycle specification is important to allow an interoperable operation of a 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 shall use only two categories of cryptographic keys:

a) Master Keys; and

b) Session Keys.

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) encryption or authenticated encryption and authorization of specific on-board 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 on-board crypto units is outside the scope of this Recommended Practice.

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 also called static keys or key encryption keys.

3.1.2.3 The crypto period of a Master Key should not exceed one use of the key.

3.1.3 SESSION KEYS

3.1.3.1 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.

NOTES

1 Session Keys are also called traffic-protection keys or traffic-encryption keys.

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

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

3.1.3.3 Session Keys shall not be used for the protection of other Session Keys or information that contains unprotected Session Keys.

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;

f) Compromised 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 during its lifetime.

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

NOTE – Figure 3-1 illustrates the possible key states and transitions as further detailed in the following subsections.

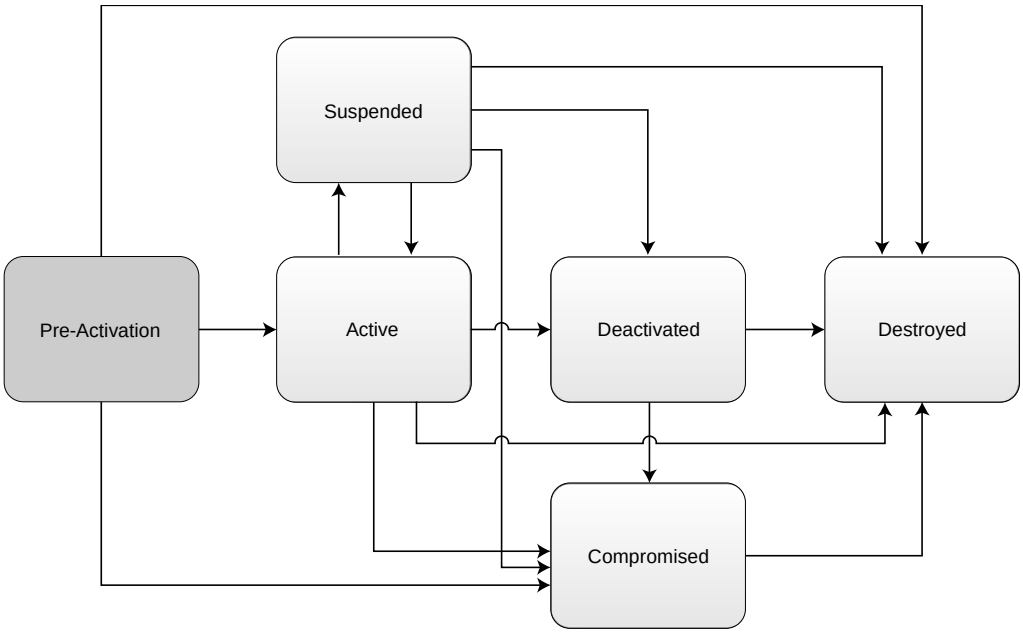

Figure 3-1: Key States and Transitions

NOTE – A detailed description of the states is provided in the CCSDS Informational Report on Symmetric Key Management (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 Master Keys associated with Pre-activation state shall never be communicated over an unprotected communication channel.

3.2.2.1.3 Session Keys associated with Pre-activation state may be communicated over an unprotected communication channel if they are protected under a Master Key.

3.2.2.1.4 Once they have been used to support cryptographic operations for the first time, keys in Pre-activation state shall be transitioned to Active state.

3.2.2.1.5 Key Verification as per 4.3.4 can be executed on keys in Pre-activation state without triggering their transition to Active 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 used to support cryptographic operations for the first time.

NOTE – A cryptographic key that is selected but not yet used operationally may still be associated with Pre-activation state.

3.2.2.2.2 A cryptographic key associated with Pre-activation state shall transition to Compromised state immediately if a corruption of the key is detected.

3.2.2.2.3 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 3.1.2.

3.2.3.2 Transitions from Active State

3.2.3.2.1 A cryptographic key associated with Active state shall transition to Compromised state immediately if a corruption of the key is detected.

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

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

3.2.3.2.4 A cryptographic key associated with Active state may transition to Suspended state.

3.2.3.2.5 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 General

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

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

3.2.4.2 Transitions from Suspended State

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

3.2.4.2.2 A cryptographic key associated with Suspended state shall transition to Compromised state immediately if a corruption of the key is detected.

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

3.2.4.2.4 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 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

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

3.2.5.3 Transitions from Deactivated State

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

3.2.5.3.2 A cryptographic key associated with Deactivated state shall transition to Compromised state immediately if a corruption of the key is detected.

3.2.6 COMPROMISED STATE

3.2.6.1 Overview

The Compromised state is an non-nominal state that refers to all cryptographic keys that have been corrupted (i.e., broken by a malicious attacker) but are still available (i.e., have not yet been destroyed).

3.2.6.2 General

3.2.6.2.1 Cryptographic keys associated with Compromised state shall not be used to support cryptographic operations.

3.2.6.2.2 Cryptographic keys associated with Compromised state should be deactivated.

3.2.6.2.3 The continued use of a compromised 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 known to be compromised. In this case, the entity that uses the information needs to be fully aware of the dangers involved.

3.2.6.3 Transitions from Compromised State

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

3.2.7 DESTROYED STATE

3.2.7.1 Overview

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

3.2.7.2 Recommendation

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

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.

4.2 SERVICE SPECIFICATIONS

The following key management service procedures may be supported, at a minimum, by a symmetric key management system:

a) Key Activation;

b) Key Deactivation;

c) Key Destruction;

d) Key Verification;

e) OTAR;

f) Zeroize;

g) Key Generation (key establishment);

h) Suspend Key;

i) Un-suspend Key.

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 State Activated;

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 activated in Step 4.3.1.3.2;

c) have the following output: the set of Key IDs of keys 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 State Active;

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 such that these keys are assigned to the Deactivated state and can no longer be used for cryptographic operations. 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 revoked 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 Revoked; 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 deactivated in Step 4.3.2.3.2;

c) have the following output: the set of Key IDs of keys 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, Deactivated, or Compromised 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;

NOTE – The number of elements in this set is a managed parameter.

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 sender 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 destroyed in Step 4.3.3.3.2;

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

d) execute the following: a message carrying the set of Key IDs 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.

NOTE – The recipient needs to perform the physical destruction of the keys.

4.3.4 KEY VERIFICATION

4.3.4.1 Overview

The Key Verification procedure allows the verification 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 or static keys associated with Pre-activation state since this would imply a transition to Active state.

4.3.4.2 Preconditions for the Procedure

The communicating entities shall have an identical set of keys in any state except Destroyed or Compromised.

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 to be verified and the Set of Challenges created in Step 4.3.4.3.2;

e) have the following output: Key IDs 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: none;

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. 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 Upload Keys; Role: Initiator;

b) Signaling of Set of Encrypted Upload Keys, Role: Initiator;

c) Processing of Protected Set of Upload Keys; Role: Recipient.

4.3.5.3.2 Protection of Set of Upload Keys

The Protection of Set of Upload Keys step shall

a) be executed by the Initiator;

b) have the following inputs:

   1) set of Upload Keys,

   2) Key ID of the Master Key;

c) have the following outputs:

   1) protected set of Upload 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 Upload Keys:

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

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

4.3.5.3.3 Signaling of Set of Protected Upload Keys

The Signaling of Set of Protected Upload 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 Upload Keys

The Processing of Set of Protected Upload 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: none;

f) execute the following:

1) the Recipient shall perform the authentication and decryption of the Set of Protected upload 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 Upload Key, the Recipient shall store it in Pre-activation state using the indicated Upload Key ID.

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

4.3.6 ZEROIZE

4.3.6.1 Overview

The Zeorize procedure allows the initiator to request the deletion of the entire volatile key store on the Recipient side.

NOTE – In most cases, this only affects the Session Keys, since Master Keys are usually stored in a write protected area of memory.

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. If this is required, extra effort will have to be made.

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.

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 wiping of the key store or not (error case).

4.3.7 KEY GENERATION

4.3.7.1 Overview

Key Generation allows the creation of new Session Keys on the Recipient side on request from 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 a cryptographic generation algorithm and taking the Master Key identified by the Key ID as input parameter.

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: Master 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: Master 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: none;

d) execute the following:

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

2) for Key ID 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 SUSPEND KEY

4.3.8.1 Overview

The Suspend Key procedure allows the initiator to request the suspension of a key on the recipient side. The main purpose of this procedure is to disable a key temporally.

4.3.8.2 Preconditions for the Procedure

Both entities shall have an identical key in Active state.

4.3.8.3 Procedure Steps

4.3.8.3.1 General

The Suspend Key procedure shall incorporate the following mandatory steps:

a) Suspension of the Key; Role: Initiator;

b) Signaling of the Key ID of the Suspended Key; Role: Initiator;

c) Suspension of the Key; Role: Recipient.

4.3.8.3.2 Suspension of the Key

The Suspension of the Key step shall

a) be executed by the Initiator;

b) have the following input: Key ID of the Key to be suspended;

c) have the following output: Key identified by the Key ID has been transitioned from Active state to Suspended state;

d) execute the following: the Key identified by the Key ID shall be transitioned from Active state to Suspended state.

4.3.8.3.3 Signaling of the Key ID of the Suspended Key

The Signaling of the Key ID of the Suspended Key step shall

a) be executed by the Initiator;

b) have the following input: Key ID of the Key that has been suspended;

c) have the following output: Key ID transmitted to the Recipient;

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

4.3.8.3.4 Suspension of the Key

The Suspension of the Key step shall be

a) executed by the Recipient;

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

c) have the following output: Key identified by the Key ID received from the Initiator has been transitioned from Active state to Suspended state;

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

4.3.9 UN-SUSPEND KEY

4.3.9.1 Overview

The Un-suspend Key procedure allows the initiator to request the un-suspension of a key on the Recipient side. The main purpose of this procedure is to re-enable a temporarily disabled key.

4.3.9.2 Preconditions for the Procedure

Both entities shall have an identical key in Suspended state.

4.3.9.3 Procedure Steps

4.3.9.3.1 General

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

a) Un-suspension of the Key; Role: Initiator;

b) Signaling of the Key ID of the Un-Suspended Key; Role: Initiator;

c) Un-suspension of the Key; Role: Recipient.

4.3.9.3.2 Un-suspension of the Key

The Un-suspension of the Key step shall

a) be executed by the Initiator;

b) have the following input: Key ID of the Key to be un-suspended;

c) have the following output: Key identified by the Key ID has been transitioned from Suspended to Active state.

4.3.9.3.3 Signaling of the Key ID of the Un-Suspended Key

The Signaling of the Key ID of the Un-Suspended Key step shall

a) be executed by the Initiator;

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

c) have the following output: Key ID transmitted to the Recipient;

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

4.3.9.3.4 Un-suspension of the Key

The Un-suspension of the Key step shall

a) be executed by the Recipient;

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

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

f) execute the following: Key identified by the Key ID 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

Where 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 a security protocol such as the Space Data-Link Layer Security Protocol (SDLS) (see reference [B9]).

A1.4 DATA INTEGRITY

Where 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 the Space Data-Link Layer Security Protocol (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 shall 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 [B12].

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 1. Recommendation for Space Data System Standards (Blue Book), CCSDS 352.0-B-1. Washington, D.C.: CCSDS, November 2012.

[B3] *The Application of CCSDS Protocols to Secure Systems*. Issue 2. Report Concerning Space Data System Standards (Green Book), CCSDS 350.0-G-2. Washington, D.C.: CCSDS, January 2006.

[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 1. Report Concerning Space Data System Standards (Green Book), CCSDS 350.7-G-1. Washington, D.C.: CCSDS, October 2011.

[B7] Elaine Barker. *Recommendation for Key Management—Part 1: General*. Revision 4. National Institute of Standards and Technology Special Publication 800-57. Gaithersburg, Maryland: NIST, January 2016.

[B8] *Information Security Glossary of Terms*. Issue 1. Report Concerning Space Data System Standards (Green Book), CCSDS 350.8-G-1. Washington, D.C.: CCSDS, November 2012.

[B9] *Space Data Link Security Protocol*. Issue 1. Recommendation for Space Data System Standards (Blue Book), CCSDS 355.0-B-1. Washington, D.C.: CCSDS, September 2015.

[B10] *Overview of Space Communications Protocols*. Issue 3. Report Concerning Space Data System Standards (Green Book), CCSDS 130.0-G-3. Washington, D.C.: CCSDS, July 2014.

[B11] *Glossary of Key Information Security Terms*. Rev. 1. Edited by Richard Kissel. NIST IR 7298. Gaithersburg, Maryland: NIST, February 2011.

[B12] *Security Threats against Space Missions*. Issue 2. Report Concerning Space Data System Standards (Green Book), CCSDS 350.1-G-2. Washington, D.C.: CCSDS, December 2015.

NOTE – Normative references are listed in 1.8.