

Draft Recommendation for
Space Data System Standards

|  |
| --- |
| CCSDS NETWORK LAYER SECURITY ADAPTATION PROFILE |

Draft Recommended Standard

CCSDS 000.0-R-0
Red Book

June 2016

AUTHORITY

|  |
| --- |
|  |
|  | Issue: | Red Book, Issue 0 |  |
|  | Date: | June 2016 |  |
|  | Location: | Not Applicable |  |
|  |

**(WHEN THIS RECOMMENDED STANDARD 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 the *Procedures Manual for the Consultative Committee for Space Data Systems*, and the record of Agency participation in the authorization of this document can be obtained from the CCSDS Secretariat at the address below.

This document is published and maintained by:

CCSDS Secretariat

Space Communications and Navigation Office, 7L70

Space Operations Mission Directorate

NASA Headquarters

Washington, DC 20546-0001, USA

FOREWORD

This CCSDS Recommendation is an adaptation of the Internet Engineering Task Force (IETF) Internet Protocol Security (IPsec) for use by CCSDS missions. IPSec supports many options and this adaptation profile has determined which options shall be supported for CCSDS.

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

http://www.ccsds.org/

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

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

Member Agencies

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

Observer Agencies

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

PREFACE

This document is a draft CCSDS Recommended Standard. 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 and Issue** | **Date** | **Status** |
| CCSDS 000.0-R-0 | CCSDS Network Layer Security Adaptation Profile, Draft Recommended Standard, Issue 0 | June 2016 | Current draft |
|  |  |  |  |
|  |  |  |  |

CONTENTS

Section Page

[DOCUMENT CONTROL v](#_Toc453759584)

[CONTENTS vi](#_Toc453759585)

[1 Introduction 1-1](#_Toc453759586)

[1.1 PUrpose 1-1](#_Toc453759587)

[1.2 Scope 1-1](#_Toc453759588)

[1.3 applicability 1-1](#_Toc453759589)

[1.4 rationale 1-1](#_Toc453759590)

[1.5 References 1-1](#_Toc453759591)

[2 Overview 2-1](#_Toc453759592)

[2.1 General concepts 2-1](#_Toc453759593)

[2.2 service overview 2-3](#_Toc453759594)

[3 CCSDS ipsec profile 3-1](#_Toc453759595)

[3.1 GEneral 3-1](#_Toc453759596)

[3.2 Supported protocols 3-1](#_Toc453759597)

[3.3 esp mode 3-1](#_Toc453759598)

[3.4 esp authenticated encryption service 3-1](#_Toc453759599)

[3.5 ESP Integrity service 3-1](#_Toc453759600)

[3.6 ESP non-authenticated encryption 3-1](#_Toc453759601)

[3.7 esp manual key management 3-1](#_Toc453759602)

[3.8 ESP Automatic key management 3-1](#_Toc453759603)

[3.9 esp cipher suite 3-1](#_Toc453759604)

# Introduction

## PUrpose

This CCSDS Recommendation provides the basis for network layer security for missions utilizing the Internet Protocol (IP) including missions encapsulating IP over CCSDS space links (reference [3]).

## Scope

This recommendation specifies the manner in which the Internet Engineering Task Force’s IP Security Protocol (IPsec) will be implemented and used for CCSDS missions.

## applicability

This recommendation applies to any mission using the Internet Protocol and requiring end-to-end confidentiality, authentication, or integrity from the sender to the receiver regardless of the number of intermediate hops between them. It is assumed that connectivity to an IP-based network has been established and the network is available for use.

## rationale

Many missions require security services to protect commanding (command authentication, command confidentiality, command integrity) and payload data (confidentiality, integrity). Missions using the Internet Protocol (IP) may utilize link layer security services such as the Space Data Link Security (SDLS) Protocol (reference [4]) which provides hop-by-hop security between two points (e.g., a ground station and a satellite). If end-to-end security is required as between a principal investigator and a payload instrument onboard a spacecraft through intermediary hops, then the IP Security (IPsec) protocol should be used. This document specifies a CCSDS “profile” of IPsec for use by CCSDS missions.

## References

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

1. IETF; Kent, S; Seo, K; *Security Architecture for the Internet Protocol*; Request for Comments (RFC) 4301; <http://datatracker.ietf.org/doc/rfc4301>; December 2005.
2. IETF; Kent, S; IP Authentication Header; Request for Comments (RFC) 4302; <http://datatracker.ietf.org/doc/rfc432>; December 2005.
3. IETF; Kent, S; *IP Encapsulating Security Payload (ESP)*; Request for Comments (RFC) 4303; <http://datatracker.ietf.org/doc/rfc4303>; December 2005.
4. IETF; Kaufman, C; *Internet Key Exchange (IKEv2) Protocol*; Request for Comments (RFC) 4306; <http://datatracker.ietf.org/doc/rfc4306>; December 2005.
5. CCSDS; CCSDS Cryptographic Algorithms; CCSDSD 352.0-B-1; Blue Book; Issue 1; November 2012.
6. CCSDS; *IP over CCSDS Space Links*; CCSDS 702.1-B-1; Blue Book; Issue 1; September 2012.
7. CCSDS; *Space Data Link Protocol*; TBD (probably should probably be moved to informative references section).
8. CCSDS; *The Application of CCSDS Protocols to Secure Systems*; CCSDS 350.0-G-2; Green Book; Issue 2; January 2006.

# Overview

## General concepts

Many missions require security services such as confidentiality, integrity, and authentication to protect spacecraft commands, software uploads, engineering telemetry, and science payload data.

As can be seen in *The Application of CCSDS Protocols to Secure Systems* (ref [9]), security services may be applied at various protocol layers. If used below the network layer, the security services must be used on a hop-by-hop basis across a link because routing information would not be available for use by the communications devices. Figure 2‑1 illustrates the use of hop-by-hop security across a network.

If used at or above the network layer, security can be provided on an end-to-end basis because the lower layer protocols and routing information remain visible and usable. Figure 2‑2 illustrates the manner in which end-to-end security is used across a network.



2‑1: Illustration of Hop-by-Hop Security Across a Network



2‑2: Illustration of End-to-End Security Across a Network

## service overview

If the Internet Protocol (IP) is used in the flight system to provide internet-like services, then security services can be applied at the network layer in the form of the IP Security (IPsec) protocol (reference [1]). Using IPsec, the security services are applied at the point of data creation and removed at the data consumption end-point. The information is protected on an end-to-end basis regardless of the number of hops or intermediary systems it traverses. Using IPsec, the data is protected by the security services but the underlying CCSDS link protocols and framing are preserved (e.g., using IP over CCSDS encapsulation (ref [7])) requiring no changes to the existing communications infrastructure.

IPsec consists of two protocols: the Authentication Header (AH) and the Encapsulating Security Payload (ESP). AH only provides authentication and integrity services for the security payload and portions of the IP header. AH does not provide confidentiality.

ESP provides confidentiality, integrity, and authentication. ESP can be also be used to provide an authentication-only service with the use of a null encryption algorithm.

CCSDS requires that ESP be the only IPsec protocol supported. AH is not required because ESP can provide an authentication-only service. Section 3 of this document will specify which ESP options are supported and which are not.

# CCSDS ipsec profile

## GEneral

This profile adopts RFC 4301 (ref [1]) and RFC 4303 (ref [3]) except as specified in 3.2 through 3.10, below.

## Supported protocols

For CCSDS implementations, IPsec shall only support ESP (ref [3]).

## esp mode

For CCSDS implementations, IPsec shall only support tunnel mode.

## esp authenticated encryption service

For CCSDS implementations, IPsec shall support a confidentiality and integrity security service (authenticated encryption).

## ESP Integrity service

For CCSDS implementations, IPsec shall support an integrity-only service.

## ESP non-authenticated encryption

For CCSDS implementations, only authenticated encryption shall be used.

## esp manual key management

For CCSDS implementations, IPsec shall support manual key management.

## ESP Automatic key management

For CCSDS implementations, IPsec shall support automated key management as described in RFC 4306 (reference [4]) with an extension to inhibit rekey or to rekey only upon command.

NOTE: this extension is required to ensure that a rekey does not occur during a critical phase of the mission potentially resulting in a system lockout or loss of mission.

## esp cipher suite

For CCSDS implementations, IPsec shall employ the algorithms described in the CCSDS Cryptographic Algorithms recommendations (reference [6]).

1. [ANNEX TITLE]

[EITHER Normative or Informative]

[Annexes contain ancillary information. Normative annexes precede informative annexes. Informative references are placed in an informative annex. See CCSDS A20.0-Y-2, *CCSDS Publications Manual* (Yellow Book, Issue 2, June 2005) for discussion of the kinds of material contained in annexes.]

1. Security

(Informative)
	1. Introduction

This document is entirely concerned with providing security services for CCSDS spacecraft and ground systems. Data transmitted across networks and RF links can be viewed, captured, altered, or forged. The use of the protocols discussed in this document will help prevent those problems from occurring.

* 1. security concerns with respect to the CCSDS document
		1. Data privacy

The use of IPsec, specified in references [1], and [3] provides data privacy through the use of encryption. Without the use of encryption, any data transmitted over ground networks or RF links could be obtained and examined by those not authorized to obtain the data. This might include the upload of spacecraft software, spacecraft commands, spacecraft telemetry, or spacecraft payload/science data.

* + 1. Data integrity

The use of IPsec, specified in references [1] and [3] provides data integrity through the use of integrity check values (hashes). The use of the integrity service provides assurance that the data received is exactly the same as the data transmitted and that there was no corruption or manipulation of the data while it was in transit. This service is critical for software uploads and commands sent to a spacecraft.

* + 1. Authentication of communicating entities

The use of IPsec, specified in references [1] and [3] provides data authentication through the use of integrity check values (hashes). The use of the authentication service provides assurance of the authenticity of the sender of the data. This is service is critical for software uploads and commands sent to a spacecraft.

* + 1. Control of access to resources

The use of IPsec, specified in references [1] and [3] provides control of unauthorized access to data and resources. The use of IPsec encryption only allows authorized entities to access system data and resources.

* + 1. Availability of resources

The use of IPsec, specified in references [1] and [3] provides assurances that data is both authentic and not corrupted or modified. This provides mission managers the assurance that data corruption or forged commands will not be processed and thereby will not result in a mission failure.

* + 1. Auditing of resource usage

The use of IPsec is not directly related to the auditing of resources – only with their protection. However, ground systems can (and should) implement an audit system to capture security-related system events that may either provide real-time alarms in crisis situations or may be reviewed later to help understand when an anomaly arises.

* 1. Potential threats and attack scenarios

Without the use of IPsec, specified in references [1] and [3], CCSDS missions may have their data stolen by unauthorized entities. An attacker may also try to capture transmitted commands and attempt to modify and replay them to the spacecraft. An attacker may try to assume an authorized entity’s identity in order to transmit unauthorized commands which may harm the spacecraft. An attacker may also try to assume an authorized entity’s identity in order to upload unauthorized or corrupted software to a spacecraft.

* 1. Consequences of not applying security to the technology

An attacker may attempt to corrupt, forge data, forge identity, or manipulate data which could result in a catastrophic mission failure.